DIPLOMARBEIT

Classical Class Field Theory and Recent Developments

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter Anleitung von
Univ.Prof. Dipl.-Ing. Dr. techn. Michael Drmota

durch
Elisabeth Fink
Albertplatz 4/7
1080 Wien

____________________ ____________________
Datum Unterschrift

Contents

1 Valuation Theory **4**
- 1.1 Introduction . . . 4
- 1.2 Basic Definitions . . . 8
- 1.3 Completion . . . 13
- 1.4 Extensions of Valuations . . . 17
- 1.5 Unramified and Ramified Extensions . . . 25

2 The Local Reciprocity Law **33**
- 2.1 Local Fields . . . 33
- 2.2 The Norm Map . . . 35
- 2.3 The Neukirch Map . . . 42
- 2.4 The Hazewinkel Homomorphism . . . 48
- 2.5 The Local Reciprocity Law . . . 55
- 2.6 The Reciprocity Map . . . 59

3 A Cohomological Approach **62**
- 3.1 Definitions . . . 62
- 3.2 The Local Reciprocity Law . . . 69
- 3.3 The Global Reciprocity Law . . . 72
- 3.4 Deducing Quadratic Reciprocity . . . 75

4 Recent Results in Class Field Theory **78**
- 4.1 Generalizations of the Ground Field . . . 79
- 4.2 Generalizations of the Reciprocity Law . . . 85
- 4.3 The Langlands Conjecture . . . 88
  - 4.3.1 The Local Langlands Correspondence . . . 88
  - 4.3.2 The Global Langlands Correspondence . . . 92
- 4.4 Constructions and Applications . . . 96
  - 4.4.1 Class Field Towers . . . 96
  - 4.4.2 Computations and Applications . . . 99

A Appendix **101**
- A.1 Group Theory . . . 101
  - A.1.1 Definitions and Isomorphism Theorems . . . 101
  - A.1.2 Sylow Theorems and p-Groups . . . 105
- A.2 Ring Theory . . . 108

A.3 Field Theory 111
A.4 Algebraic Number Theory 116
A.5 Topological Groups 119

Chapter 1

Valuation Theory

In this first chapter, we give an introduction to valuation theory. Understanding valuation theory is a crucial step towards understanding class field theory. Most of the terms and theorems stated here are needed later on, as we get to local class field theory. Most parts of this can be found in [Ne2], [Iw] and [FeVo1].

1.1 Introduction

In this section we would like to give a little motivation for the theory we will develop in this text. Therefore, the definition of the p-adic numbers is essential.

Definition 1.1.1. Fix a prime number p. A *p-adic integer* is a formal infinite series

$$a_0 + a_1 p + a_2 p^2 + \cdots ,$$

where $0 \leq a_i < p$, for all $i = 0, 1, 2, \ldots$. The set of all p-adic integers is denoted by $\mathbb{Z}_p$.

This definition seems natural if we consider the fact that every positiv integer $n \in \mathbb{N}$ can be represented as

$$n = a_0 + a_1 p + \cdots + a_n p^n.$$

We see, that the definition above is just the extension of this to the infinite case. Therefore the next proposition is quite obvious to see:

Proposition 1.1.2. *The residue classes of $a \in \mathbb{Z}_p \mod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \mod p^n$$

where $0 \leq a_i < p$ for $i = 0, \ldots, n-1$.

Idea. The proof is straight forward using induction. □

We would now like to define a valuation on the p-adic integers.

Let $a = \frac{b}{c}$, $b, c \in \mathbb{Z}$, be a nonzero rational number. We extract from b and from c as high a power of the prime number p as possible:

$$a = p^m \frac{b'}{c'},\ (b'c', p) = 1, \tag{1.1}$$

and we put

$$|a|_p = \frac{1}{p^m}.$$

$|a|_p$ is called the *p-adic absolute value*. In these terms, the summands $a_0 + a_1 p + a_2 p^2 + \cdots$ form a sequence converging to 0 with respect to $| \ |_p$.
The exponent m in the representation (1.1) of the number a is denoted by $v_p(a)$, and we put formally $v_p(0) = \infty$. This gives the function

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\},$$

which is easily checked to satisfy the properties

1. $v_p(a) = \infty \Leftrightarrow a = 0$,

2. $v_p(ab) = v_p(a) + v_p(b)$,

3. $v_p(a + b) \geq \min (v_p(a), v_p(b))$,

where $x + \infty = \infty, \infty + \infty = \infty$ and $\infty > x$ for all $x \in \mathbb{Z}$. The function v_p is called the *p-adic exponential valuation* of $\mathbb{Q}$. The following fact explains the term exponential:

The p-adic absolute value is given by

$$| \ |_p : \mathbb{Q} \to \mathbb{R}$$

$$a \mapsto |a|_p = p^{-v_p(a)}.$$

Easy observations show that the p-adic absolute value satisfies the conditions of a topological norm on $\mathbb{Q}$.

Remark 1.1.3. *With respect to the redefinition of a valuation in the next section we will omit the term* exponential *here.*

After this little motivation, we would now like to introduce the p-adic numbers.

If we extend the domain of p-adic integers into that of the formal series

$$\sum_{v=-m}^{\infty} a_v p^v = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdots$$

where $m \in \mathbb{Z}$ and $0 \leq a_v < p$. Such series are simply called *p-adic numbers*, denoted by $\mathbb{Q}_p$. It is easy to see that we obain a canonical mapping

$$\mathbb{Q} \to \mathbb{Q}_p$$

as we had one for the integers into the p-adic integers in an obvious way.
We will see later when we discuss the meaning of completeness, that the p-adic numbers are complete with respect to the p-adic valuation.

We now give another definition of the p-adic integers, including projective limits. However, we will not discuss projective limits in detail, but only give enough information about them to define the p-adic integers. For more detailed information about the construction using the projective limit see [Ne2] or [Wi1] or the Appendix.

As we stated above, the residue classes of a p-adic integer $a \mod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented by finite sums. We therefore consider the p-adic integers as a sequence of residue classes

$$\overline{s}_n = s_n \mod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

The terms of such a sequence lie in different rings $\mathbb{Z}/p^n\mathbb{Z}$, but theses are related by the canonical projections

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \cdots$$

and we find

$$\lambda_n(\overline{s}_{n+1}) = \overline{s}_n.$$

In the direct product

$$\prod_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z} = \{(x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{Z}/p\mathbb{Z}\},$$

we now consider all elements $(x_n)_{n\in\mathbb{N}}$ with the property that

$$\lambda_n(x_{n+1}) = x_n \text{ for all } n = 1, 2, \ldots$$

Definition 1.1.4. This set is called the *projective limit* of the rings $\mathbb{Z}/p^n\mathbb{Z}$ and is denoted by $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

In other words we have:

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \lambda_n(x_{n+1}) = x_n, \ \ n = 1, 2, \ldots \right\}.$$

The following proposition shows that the elements in the construction above really are the p-adic integers as defined in the beginning of this section.

Proposition 1.1.5. *Associating to every p-adic integer*

$$f = \sum_{v=0}^{\infty} a_v p^v$$

the sequence $(\overline{s}_n)_{n\in\mathbb{N}}$ of residue classes

$$\overline{s}_n = \sum_{v=0}^{n-1} a_v p^v \mod p^n \in \mathbb{Z}/p^n\mathbb{Z},$$

yields a bijection

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. The proof immediatly follows from the unique represenation of the residue classes of a p-adic integer $a \mod p^n$. □

Due to that proposition, we identify

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

The p-adic integers are a subring of the direct product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ where addition and multiplication are defined componentwise. In this context, $\mathbb{Q}_p$ becomes the quotient field of $\mathbb{Z}_p$.

1.2 Basic Definitions

In this section we will give most of the definitions we will need later and state useful lemmas and propositions about them.

Let G be an abelian totally ordered group and let F be a field. A map $v : F \to G$ with the following properties

1. $v(\alpha) = +\infty \Leftrightarrow \alpha = 0$

2. $v(\alpha \cdot \beta) = v(\alpha) + v(\beta)$

3. $v(\alpha + \beta) \geq \min \{v(\alpha), v(\beta)\}$

is called a *valuation* on F. A field F that allows such a map is said to be a *valuation field*. It is easy to see that the map $v : F^* \to G$ induces a group homomorphism and therefore the image $v(F^*)$ is a totally ordered subgroup of G.

Remark 1.2.1. *In the introduction we saw that this valuation here is an exponential valuation of an absolute value. However, we could also proceed in the following way:*

We start with absolute values, satisfying the conditions:

1. $|x| \geq 0$ *and* $|x| = 0$ *if and only if* $x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Using this theory, we can define an absolute value to be non-archimedian *if* $|n|$ *stays bounded for all* $n \in \mathbb{N}$*. Otherwise it is called* archimedian*.*
We will see later in the theorem of Ostrowski 1.3.5, why we do not use those definitions.

We will now show some really basic properties about valuations which will be used in proofs in the following sections.

Lemma 1.2.2. *If* v *is a valuation on a field* F *we have:*

1. $v(-1) = 0$

2. $v(-\alpha) = v(\alpha)$

3. $v(\alpha^{-1}) = -v(\alpha)$

Proof. It is clear from the fact that v is a group homomorphism that $v(1) = 0$, which is a commonly known property of group homomorphisms. From that and $(-1)^{-1} = (-1)$, which can be shown easily, we get:

$$v(1) = v\left((-1) \cdot (-1)\right) = v(-1) + v(-1) = 0$$

which leads to $v(-1) = -v(-1)$ which can only mean either $char(F) = 2$ or $v(-1) = 0$. But with characteristic 2 we also have $-1 = 1$ from which we obtain $v(-1) = v(1) = 0$.

The second property simply follows from (1):

$$v(-\alpha) = v\left((-1) \cdot \alpha\right) = v(-1) + v(\alpha) = 0 + v(\alpha) = v(\alpha).$$

The third property follows similar.

□

It is easy to verify that if $v(\alpha) \neq v(\beta)$ the last condition on a valuation, the triangle law, is actually equal to $v(\alpha + \beta) = \min\left(v(\alpha), v(\beta)\right)$. That is because if we assume without loss of generality that $v(\alpha) > v(\beta)$, then

$$\begin{aligned} v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\} = v(\beta) = v(\alpha + \beta - \alpha) \geq \\ \geq \min\{v(\alpha + \beta), v(\alpha)\} = v(\alpha + \beta) \end{aligned}$$

and our assumption $v(\alpha) > v(\beta)$ proves the last equality.

Next we define some sets that are essential for our further discussions.

If we define

$$\mathcal{O}_v := \{\alpha \in F : v(\alpha) \geq 0\}$$
$$\mathcal{M}_v := \{\alpha \in F : v(\alpha) > 0\}$$

then it is easy to see that $\mathcal{O}_v$ is a (clearly commutative) ring. We know from Algebra that the set of non-invertible elements of a ring forms an ideal, which is maximal and unique. Therefore, by definiton, the ring $\mathcal{O}_v$ is a local ring. Hence we have a naturally induced field $\mathcal{O}_v/\mathcal{M}_v$, the *residue (class) field*, denoted by $\overline{F}$. This field is denoted throughout this text by $\overline{F}$ as there will not be any confusion with another valuation. The set $U_v = \mathcal{O}_v \setminus \mathcal{M}_v$ is a multiplicative group, the *group of units*. This group obviously has the property $v(\alpha) = 1$ for all $\alpha \in U_v$.

Remark 1.2.3. *1. We saw that the ideal $\mathcal{M}_v$ is unique and maximal. We will therefore sometimes denote it by P when convenient and when the situation allows no confusion.*

2. U_v will sometimes also be denoted by U_K if the valuation cannot be confused. The same holds for the ideal $\mathcal{M}_v$ which will sometimes be denoted as $\mathcal{M}_K$ for the corresponding field. This is useful as we will have different fields later.

3. *The term* residue class field *should not be mixed up with* class field*, a term we will define later and that is something totally different.*

Lemma 1.2.4. *For every $x \in F$ we either have $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$.*

Proof. This is just a simple observation. By lemma 1.2.2 the assertion is exclusive. □

$\mathcal{O}_v$ is called the *ring of integers* or *valuation ring*. This ring is always integrally closed. For if $x \in F$ is integral over $\mathcal{O}_v$, then by definition there is an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_i \in \mathcal{O}_v$ and by assumption $x \notin \mathcal{O}_v$ and by our previous observation we must have $x^{-1} \in \mathcal{O}_v$. But that would imply $x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0(x^{-1})^{n-1} \in \mathcal{O}_v$.

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

$$\mu(\alpha) = s \cdot v(\alpha), \text{ for all } \alpha \in F.$$

Then μ is again a valuation of F. When two valuations v and μ on F 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 μ are *equivalent valuations* of F.

As it is easy to see, that equivalent valuations on a field F induce the same ring of integers and maximal ideal. Therefore, equivalent valuations have the same residue field, along with many other properties as we will see.

In order to get more specific results, we need to add properties to valutaions. We will concentrate on discrete valuation fields.

First of all we call F a *discrete valuation field* if F allows the definition of a non-trival *discrete valuation*. Such a valuation is one that admits a smallest positive value s such that

$$v(F^*) = s\mathbb{Z}.$$

Since $v(F^*)$ is a subgroup of $\mathbb{Z}$, we get a *normalized* valuation $v^* := \frac{1}{s}v$. Hence we can always assume that the map $v : F^* \to \mathbb{Z}$ is surjective by replacing v with its corresponding normalized valuation. By the definition of the corresponding sets this does not change $\mathcal{O}_v$ or $\mathcal{M}_v$ and hence not the residue class field either. When talking about a discrete valuation we will therefore always assume that it is normalized.

Remark 1.2.5. *It is obvious that a field admitting a discrete valuation can never be finite. This seems obvious at this point, but is worth being mentioned as it will be useful later. This, however, will not be a restriction since we will see that the fields we want to study are extensions of $\mathbb{Q}$.*

In terms of our definition of equivalency of valuations this would mean, we regard all the valuations on a field F in equivalency classes and pick the normalized valuation as a representative of each class. An element $\pi \in F$ is called a *prime*, if $v(\pi)$ generates

$v(F^*)$. In the case of a normalized discrete valuation, this simply means $v(\pi) = 1$.

The next lemma gives us a little information about the inner structure of $\mathcal{O}_v$.

Lemma 1.2.6. *Let F be a discrete valuation field, and π be a prime element. Then the ring of integers $\mathcal{O}_v$ is a principal ideal ring, and every proper ideal of $\mathcal{O}_v$ can be written as $\pi^n\mathcal{O}_v$ for some $n \in \mathbb{N}$. In particular, $\mathcal{M}_v = \pi\mathcal{O}_v$. The intersection of all proper ideals of $\mathcal{O}_v$ is the zero ideal.*

Proof. See [FeVo1]. □

As our next result we get a useful representation of an arbitrary element of F, which can also be shown quite easy.

Lemma 1.2.7. *Any element $\alpha \in F$ can be written as $\alpha = \pi^n\epsilon$ for some $n \in \mathbb{Z}, \epsilon \in U_v$ and a prime element π.*

Proof. Let $n = v(\alpha)$. Then $\alpha\pi^{-n} \in U_v$ and $\alpha = \pi^n\epsilon$ for $\epsilon \in U_v$. If $\pi^n\epsilon_1 = \pi^m\epsilon_2$, then $n + v(\epsilon_1) = m + v(\epsilon_2)$. As $\epsilon_1, \epsilon_2 \in U_v$, we deduce $n = m$, $\epsilon_1 = \epsilon_2$. □

A discrete valuation field can be made a metric space in the following way:

Let v be a discrete valuation on a field F. Then for any d such that $0 < d < 1$ the map $d_v : F \times F \to \mathbb{R}$ defined by $d_v(\alpha, \beta) \mapsto d^{v(\alpha-\beta)}$ is a metric on F, inducing a Hausdorff topology.

Remark 1.2.8. *It can be shown quite easy that equivalent valuations of F induce the same topology. We will therefore always assume $v_1 \nsim v_2$ if we demand $v_1 \neq v_2$.*

For every $\alpha \in F$ the sets $\alpha + \pi^n\mathcal{O}_v$ form a base of open neighborhoods of α, since the sets $1 + \pi^n\mathcal{O}_v$ form a base of neighborhoods of $1 \in F$.

Lemma 1.2.9. *The field F is a topological field with the above-defined topology.*

Proof. By the definition of our base of neighborhoods of an element α it suffices the prove that we can find a neighborhood U of (α, β) from the product topology which satisfies $v(x - v) \geq m$ for some $n \in \mathbb{N}$ (since that implies $v(x - y) \in V$ for some neighborhood $V = \alpha + \pi^k\mathcal{O}_v$ of $\alpha = \epsilon\pi^n$, namely any $m \geq \max\{k, n\}$ will do.
This, however, is gained really easy from the triangle law:

1. $v((\alpha - \alpha_0) - (\beta - \beta_0)) = v((\alpha - \beta) - (\alpha_0 - \beta)) \geq \min\{v(\alpha - \alpha_0), v(\beta - \beta_0)\}$ with $(\alpha, \beta) \in V$ which is a neighborhood of (α_0, β_0) and using property (ii) of lemma 1.2.2.

2. $v(\alpha\beta - \alpha_0\beta_0) = v(\alpha\beta - \alpha_0\beta + \alpha_0\beta - \alpha_0\beta_0) = v((\alpha - \alpha_0)\beta + (\beta - \beta_0)\alpha_0) \geq \min\{v(\alpha - \alpha_0) + v(\beta), v(\beta - \beta_0 + v(\alpha)\}$.

3. $v(\alpha^{-1} - \alpha_0^{-1}) = v(\alpha - \alpha_0) - v(\alpha) - v(\alpha_0)$ by adding terms as in the proof of the multiplication.

We therefore obtain the continuity of subtraction, multiplication and division. □

Lemma 1.2.10. *Let τ_1 be definied by a discrete valuation v_1 and τ_2 by v_2. Then $\tau_1 = \tau_2$ holds if and only if $v_1 = v_2$.*

Proof. Given $v_1 = v_2$ it is obvious that $\tau_1 = \tau_2$ holds.
Assume that $\tau_1 = \tau_2 = \tau$. We observe:

$$\alpha^n \to 0 \text{ with } n \to \infty \text{ in } \tau \Leftrightarrow v(\alpha) > 0$$

First, if $v(\alpha) > 0$, then $v(\alpha) \geq 1$, since $v(F) = \mathbb{Z}$. So $v(\alpha) > 0$ obviously means

$$v(\alpha^n) = n \cdot v(\alpha) \geq n \text{ for all } n \in \mathbb{N}$$

and hence $\lim_{n\to\infty}(v(\alpha^n)) = 0$ which gives us $v(\lim_{n\to\infty} \alpha^n) = 0$ since v is easily shown to be continuous. Let us now assume $v(\alpha) \leq 0$. $v(\alpha) = 0$ implies $v(\alpha^n) = 0$ for all $n \in \mathbb{N}$. By the same limit argument as shown above we get $v(0) = 0$ which contraticts the definition of v. If $v(\alpha) < 0$, we apply the limit argument again and get $v(\lim_{n\to\infty} \alpha^n) \leq 0$ which leads to the same contratiction.
Having shown the above we get $v_1(\alpha) > 0$ if and only if $v_2(\alpha) > 0$, since both topologies coincide. Let now π_1 and π_2 be prime elements of v_1 and v_2 respectively.
For an arbitrary prime element π with respect to a valuation v we always have $v(\pi) > 0$ by definition of $\pi \in \mathcal{O}_v$. As mentioned above we therefore obtain $v(\pi) \geq 1$ in the case of a discrete valuation. We conclude $v_1(\pi_2) \geq 1$ and $v_2(\pi_1) \geq 1$.
If $v_2(\pi_1) > 1$ then

$$v_2(\pi_1\pi_2^{-1}) = v_2(\pi_1) + v_2(\pi_2^{-1}) = v_2(\pi_1) - v_2(\pi_2) > 0$$

since $v_2(\pi_2) = 1$. The same holds for $v_1(\pi_2\pi_1^{-1}) > 0$. The latter expression equals $-v_1(\pi_1\pi_2^{-1}) > 0$. This implies $v_2(\pi_1) = 1$ and $v_1(\pi_2) = 1$ for all primes π_1 with respect to v_1 and π_2 with respect to v_2. Since every element $\alpha \in F$ has a representation $\pi^n \cdot \epsilon$ both valuations must coincide. □

Remark 1.2.11. *According to [Ne2] two valuations are equivalent when they define the same topology on F. It can be shown that this is the case when they only differ in a multiplicative factor s. Since we assumed our valuations to be normalized, the only possible factor s is actually 1.*

1.3 Completion

In the last chapter we developed a theory of valuations on a field. Since valuations naturally define a topology on the field F, making it to a metric topolocial space, we can take a look at its completion.

Definition 1.3.1. A sequence $\{\alpha_n\}$ of elements is called a *Cauchy sequence* if for every real c there is n_0 such that $v(\alpha_n - \alpha_m) \geq c$ for $m, n \geq n_0$.

The following lemma shows us, how it is natural to define the completion of a valuation field.

Lemma 1.3.2. *The set A of all Cauchy sequences forms a ring with respect to componentwise addition and mulitiplication. The set of all Cauchy sequences with $\alpha_n \to 0$ forms a maximal ideal M of A. The field A/M is a discrete valuation field with its discrete valuation $\hat{v}$ defined by*

$$\hat{v}((\alpha_n)) = \lim_{n\to\infty} v(\alpha_n)$$

for a Cauchy sequence $\{\alpha_n\}_{n\geq 0}$.

Having shown the above we new define the completion of a field.

Definition 1.3.3. A discrete valuation field F is called a *complete discrete valuation field* if every Cauchy sequence is convergent in F, i.e. there exists

$$\alpha = \lim_{n\to\infty} \{\alpha_n\} \in F$$

with respect to v. A field $\hat{F}$ is called a *completion* of F if it is complete and $\hat{v}|_F = v$ and F is a dense subfield of $\hat{F}$.

Theorem 1.3.4. *Every discrete valuation field F has a completion which is unique up to an isomorphism over F.*

As promised in the previous section, we will now state the theorem of Ostrowski. We will therefore see why we did not use absolute values to define valuations.

Theorem 1.3.5 (Ostrowski)**.** *Let K be a field which is complete with respect to an archimedean valuation $|\ |$. Then there is an isomorphism σ from K onto $\overline{\mathbb{R}}$ or $\mathbb{C}$ satisfying*

$$|a| = |\sigma a|^s \quad \text{for all} \quad a \in K$$

for some fixed $s \in (0, 1]$.

We see that every discrete valuation field has the above defined completion, which is a complete valuation field with respect to $\hat{v}$, the canonical extension of v from F to $\hat{F}$.

Given a sequence $\{\alpha_n\}$ we observe that $v(\alpha_n)$ must become stationary. For $n \geq n_0$ we have $v(\alpha - \alpha_n) > v(\alpha)$ since $\{\alpha - \alpha_n\}$ has to be a null sequence and hence $v(\alpha - \alpha_n)$ tends to $+\infty$ by the definition of a valuation. Therefore we have

$$v(\alpha_n) = \hat{v}(\alpha_n - a + a) = \min\{\hat{v}(\alpha_n - \alpha), \hat{v}(\alpha)\} = \hat{v}(\alpha).$$

From that we get

$$v(F^*) = \hat{v}(F^*)$$

and if v is discrete and normalized, then so is the extension $\hat{v}$. We obtain that if $\{\alpha_{n+1} - \alpha\}$ is a sequence tending to null, then $\{\alpha_n\}$ is a Cauchy sequence. By the same argument we see that an infinite series $\sum_{n=0}^{\infty} \alpha_n$ converges in $\hat{F}$ **if and only if** the sequence of its terms α_n is a nullsequence.

Definition 1.3.6. A field F which is complete with respect to a discrete valuation v and has perfect residue field is called a *local field*.

Remark 1.3.7. *1. A local field is sometimes defined to have finite residue field, not just a perfect one. A perfect field is a field for which every algebraic extension is seperable (as seen in the appendix). As we know from basic Algebra, whence every field of characteristic* 0 *is perfect, but also every finite field. Local fields are sometimes called* local number fields *if they are of characteristic* 0*, or* local functional fields *if they are of positive characteristic.*

2. In Chapter 2 we will mainly assume local fields will to have finite residue fields.

Let us now take a closer look on the topological aspect of the residue fields.

Proposition 1.3.8. *If $\mathcal{O} \subset K$, respective $\hat{\mathcal{O}} \subset \hat{K}$ is the valuation ring of v resp. $\hat{v}$ and if $\mathcal{M}$ resp. $\hat{\mathcal{M}}$ are the maximal ideals then we have*

$$\hat{\mathcal{O}}/\hat{\mathcal{M}} \simeq \mathcal{O}/\mathcal{M}$$

and if v is discrete

$$\hat{\mathcal{O}}/\hat{\mathcal{M}}^n \simeq \mathcal{O}/\mathcal{M}^n \quad for \quad n \geq 1.$$

The next proposition is a nice property of discrete valuation fields, that will be mentioned, but not proved.

In the introduction we identified the ring $\mathbb{Z}_p$ of p-adic integers with the projective limit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Similar to this we have for every $n \in \mathbb{N}$ the canonical homomorphisms

$$\mathcal{O} \to \mathcal{O}/\mathcal{M}^n$$

which together with

$$\mathcal{O}/\mathcal{M} \xleftarrow{\lambda_1} \mathcal{O}/\mathcal{M}^2 \xleftarrow{\lambda_2} \mathcal{O}/\mathcal{M}^3 \xleftarrow{\lambda_3} \cdots$$

gives as a homomorphism $\mathcal{O} \to \varprojlim_n \mathcal{O}/\mathcal{M}^n$ into the projective limit

$$\varprojlim_n \mathcal{O}/\mathcal{M}^n = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathcal{O}/\mathcal{M}^n \;\middle|\; \lambda_n(x_{n+1}) = x_n \right\}.$$

From this and basic properties of projective limits we obtain that the projective limit $\varprojlim_n \mathcal{O}/\mathcal{M}^n$ is a closed subset of the product in the product topology on $\prod_{n=1}^{\infty} \mathcal{O}/\mathcal{M}^n$.

Proposition 1.3.9. *The canonical mapping*

$$\mathcal{O} \to \varprojlim_{n} \mathcal{O}/\mathcal{M}^n$$

is an isomorphism and a homeomorphism. The same is true for the mapping

$$\mathcal{O}^* \to \varprojlim_{n} \mathcal{O}^*/U^{(n)},$$

where $U^{(n)} = 1 + \mathcal{M}_v^n$.

Remark 1.3.10. *The set* $U^{(n)}$*, the* n-th unit group*, will be properly defined and used later.*

We will now state Hensel's lemma. The proof is not that complicated, but rather long and therefore omitted. For the proof see for example either [FeVo1] or [Ne2].

Lemma 1.3.11 (Hensel's Lemma)**.** *Let* F *be a complete discrete valuation field,* $\mathcal{O}$ *its ring of integers and* p *its unique maximal ideal. If a primitive polynomial* $f(x) \in \mathcal{O}[x]$ *admits a factorization*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \mod p$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \overline{F}[x]$*, then* $f(x)$ *admits a factorization*

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}[x]$ *such that* $\deg(g) = \deg(\overline{g})$ *and*

$$g(x) \equiv \overline{g}(x) \mod p \quad \text{and} \quad h(x) \equiv \overline{h}(x) \mod p.$$

Fields that satisfiy the assertion of Hensel's lemma are called *Henselian fields*. The way we stated the lemma we see, local discrete valuation fields are Henselian fields.

Remark 1.3.12. *It can be shown that if a field* F *is a Henselian field with respect to nontrivial valuations* v, $v' : F \to \mathbb{Q}$ *and the topologies induced by* v *and* v' *are not equivalent and* v *is discrete, then* v' *cannot be discrete.*

Example 1.3.13. The polynomial $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$ splits over the residue class field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ into distinct linear factors. If we apply Hensel's lemma we see that $f(x)$ also splits over $\mathbb{Z}_p$. Applying the lemma repeatedly we get a representation of $f(x)$ as the product of distinct linear factors over $\mathbb{Z}_p$. Therefore the field $\mathbb{Q}_p$ of p-adic numbers must contain the $(p-1)$-th roots of unity, denoted by μ_{q-1}. These, together with 0 even form a system of representatives for the residue class field, which is closed under multiplication.

The next lemma is an immediate consequence of Hensel's lemma, but will be useful in the next section to prove the existence of an extension of a valuation.

Lemma 1.3.14. *Let* F *be a complete discrete valuation field and let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

be an irreducible polynomial with coefficients in F*. Then the condition* $v(a_0) \geq 0$ *implies* $v(a_i) \geq 0$ *for* $0 \leq i \leq n-1$.

Proof. By assumption we know that $a_0 \in \mathcal{O}$ and let us assume that j is the maximal integer such that $v(a_j) = \min_{0 \le i \le n-1} v(a_i)$. If $a_j \notin \mathcal{O}$ and therefore $v(a_j) < 0$, then put

$$f_1(x) = a_j^{-1} f(x)$$

$$g_0(x) = x^j + a_j^{-1} a_{j-1} x^{j-1} + \cdots + a_j^{-1} a_0$$

$$h_0(x) = a_j^{-1} x^{n-j} + 1$$

We obviously have $\overline{f}_1(x) = \overline{g}_0(x)\overline{h}_0(x)$ and $\overline{g}_0(x), \overline{h}_0(x)$ are relatively prime. Therefore by Hensel's lemma we conclude that $f_1(x)$ and $f(x)$ are in contradiction to our assumption not irreducible. □

1.4 Extensions of Valuations

In this section we will look at the extension of a field's valuation to an extension of the field. We will first define the *ramification index* e and the *inertia degree* f of a valuation field and an extension of it. Based on that we deduce basic properties about those two numbers.
To state our main theorem of this section, the one about the uniqueness of an extension in a special case, we need to get familiar with the representation of an arbitrary element $x \in L$ in terms of a basis of the extension $[L : F]$. From that we also obtain the familiar equation $e \cdot f = n$, which we know from algebraic number theory.
Some of the proofs in this section will be omitted, because they are rather long and technical but do not really give any additional information.

If we have a discrete valuation field L with a valuation w and L is an extension of a field F, then $v := w|_F$ induces a valuation on the field F. In this context L/F is said to be an extension of valuation fields. Once again $w(L^*)$ is a totally ordered group and $w(F^*)$ a totally ordered subgroup of it.

Definition 1.4.1. The index $w(L^*)/w(F^*)$ is called the *ramification index* $e(L/F, w)$.

Remark 1.4.2. *We will remark later, that the definition known from algebraic number theory can be deduced from the definiton above.*

The ring of integers $\mathcal{O}_v$ is clearly a subring of $\mathcal{O}_w$ and the maximal ideal $\mathcal{M}_v$ is $\mathcal{M}_v = \mathcal{M}_w \cap F = \mathcal{M}_w \cap \mathcal{O}_v$, as we can see from theorem A.2.15 and theorem A.2.16.

From that we obtain

$$\overline{F} = \mathcal{O}_v/\mathcal{M}_v = \mathcal{O}_v/(\mathcal{M}_w \cap \mathcal{O}_v) = (\mathcal{O}_v + \mathcal{M}_w)/\mathcal{M}_w \subset \mathcal{O}_w/\mathcal{M}_w = \overline{L}$$

by using the second isomorphism theorem. We therefore consider the residue field $\overline{F}$ of F to be a subfield of the residue field $\overline{L}$ of L.

Definition 1.4.3. The degree $[\overline{L} : \overline{F}]$ is called the *inertia degree* or *residue degree* $f(L/F, w)$.

Lemma 1.4.4. *Let L be a finite extension of F of degree n. Then*

$$e(w|v)f(w|v) \leq n.$$

Proof. See [Ne2] for a proof of this. □

The following proposition gives us a unique representation of an element $x \in F$ which will be very useful in latter proofs. We therefore need the definition of a *set of representatives* for a valuation field F. Such a set is a set R with:

1. $R \subset \mathcal{O}$, with $\mathcal{O}$ is the ring of integers of F with respect to its valuation

2. $0 \in R$

3. R is mapped bijectively on $\overline{F} = \mathcal{O}/P$ under the canonical map

We can now use that definiton to express our unique represenation of an arbitrary element x of F in a nice way:

Proposition 1.4.5. *1. Each $x \in F$ can uniquely expressed in the form*

$$x = \sum_{-\infty<<n} \theta_n \pi_n, \text{ with } \theta_n \in R.$$

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

$$v(x) = i.$$

2. Let

$$x = \sum \theta_n \pi_n,\ y = \sum \zeta_n \pi_n,\ \theta_n, \zeta_n \in R.$$

Then, for any integer i

$$v(x-y) \geq i \quad \Leftrightarrow \quad \theta_n = \zeta_n \text{ for all } n < i.$$

Proof. See [Iw]. □

Proposition 1.4.6. *Let L be an extension of F and let F, L be complete with respect to discrete valuations v, w. Let $w|v$, $f = f(w|v)$ and $e = e(w|v) < \infty$. Let $\pi_w \in L$ be a prime element with respect to w and $\theta_1, \dots, \theta_f$ elements of $\mathcal{O}_w$ such that their residues form a basis of $\overline{L} = \mathcal{O}_w/P_w$ over $\overline{F} = \mathcal{O}_v/P_v$.*
Then $\{\theta_i \pi_w^j\}$ is a basis of the F-space L and of the $\mathcal{O}_v$-module $\mathcal{O}_w$, with $1 \leq i \leq f$, $0 \leq j \leq e-1$. If $f < \infty$, then L/F is a finite extension of degree $n = ef$.

The next lemma is very helpful in the proof of the main theorem of this section.

Lemma 1.4.7. *Let L be a finite extension of F and w, v their respective valuations and $\overline{L}, \overline{F}$ their residue fields. Let $\omega_1, \dots, \omega_s$ be any finite number of elements in $\overline{L}$ which are linearly independent over $\overline{F}$ and for each $i, 1 \leq i \leq s$ choose an element χ_i in $\mathcal{O}_w$ that belongs to the residue class ω_i in $\overline{L} = \mathcal{O}_w/P$. Fix a prime element π_w of L and let*

$$\nu_{ij} = \chi_i \pi_w^j,\ 1 \leq i \leq s,\ 0 \leq j < e = e(L/F, w).$$

Then we have:

1. *Let*
$$y' = \sum_{i=1}^{s} y_i \chi_i, \text{ with } y_i \in F.$$
Then
$$w(y') = \min\{ev(y_i), 1 \leq i \leq s\}$$
and $\chi_1, \ldots, \chi_s$ are linearly independent over F.

2. *Let*
$$x' = \sum_{i,j} x_{ij} \nu_{ij}, \text{ with } x_{ij} \in F,\ 1 \leq i \leq s,\ 0 \leq j < e.$$
Then
$$w(x') = \min\{ev(x_{ij}) + j,\ 1 \leq i \leq s,\ 0 \leq j < e\}$$
and the elements ν_{ij}, $1 \leq i \leq s$, $0 \leq j < e$, are linearly independent over F.

Proof. See [Iw]. □

The next theorem is an essential statement about the uniqueness of an extension of a valuation in the case of a complete discrete valuation field to a finite extension of it.

Theorem 1.4.8. *Let F be a complete field with respect to a discrete valuation v and L a finite extension of F. Then there is precisely one extension w on L of the valuation v and*
$$w = \frac{1}{f} v \circ N_{L/F} \quad \text{with} \quad f = f(L/F, w).$$
The field L is complete with respect to w.

We will prove this result, since it can be seen very clearly why our extension is defined the way it is. As discussed in previous chapters we do not loose any of the significant properties of a valuation if we assume it to be normalized. We will therefore assume our valuations to be normalized in the following proof.

Proof. We will first constructively prove the existence of an extension and then show that it is unique.

Existence We define $w' = v \circ N_{L/F}$, where $N_{L/F}$ is the regular norm symbol of the extension L/F, then w' is a valuation on L.

(1) It is obvious that $w'(\alpha) = +\infty$ if and only if $\alpha = 0$ because the same property holds for v and $N_{L/F}(\alpha) = 0$ if and only if $\alpha = 0$.

(2) Next we have to show that $w'(\alpha \cdot \beta) = w'(\alpha) + w'(\beta)$. Since we have:

$$w'(\alpha \cdot \beta) = v \circ N_{L/F}(\alpha \cdot \beta) = v(N_{L/F}(\alpha \cdot \beta)) = v(N_{L/F}(\alpha) \cdot N_{L/F}(\beta)) =$$
$$= v(N_{L/F}(\alpha)) + v(N_{L/F}(\beta)) = v \circ N_{L/F}(\alpha) + v \circ N_{L/F}(\beta) = w'(\alpha) \cdot w'(\beta)$$

because of the multiplicativity of the norm symbol and the valuation v.

(3) For the third property we have to show $w'(\alpha + \beta) \geq \min(w'(\alpha), w'(\beta))$. We can, without loss of generality, assume that $w'(\alpha) \geq w'(\beta)$ is true. Then we have:

$$w'(\alpha + \beta) = w'\left(\beta\left(1 + \frac{\alpha}{\beta}\right)\right) = w'(\beta) + w'\left(1 + \frac{\alpha}{\beta}\right)$$

by (2), which we have already proved above. Due to our assumption we have:

$$w'\left(\frac{\alpha}{\beta}\right) = w'(\alpha) - w'(\beta) \geq 0$$

which can easily be seen to be true due to a remark after the definition of a valuation and by assumption. It therefore sufficies to show that $w'(\gamma) \geq 0$ implies $w'(1 + \gamma) \geq 0$. Let now be $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ the monic irreducible polynomial of γ over F. We know about norms from algebraic number theory that $N_{L/F}(\gamma) = \prod \gamma_i$ when $f(x) = \prod (x - \gamma_i)$ for separable extensions. From that we get $(-1)^m a_0 = N_{F(\gamma)/F}(\gamma)$. Let s be the degree of the second extensions, namely $s := |L : F(\gamma)|$. We know from basic norm properties that

$$N_{L/F}(\gamma) = N_{F(\gamma)/F}(N_{L/F(\gamma)}(\gamma))$$

For the inner part $N_{L/F(\gamma)}(\gamma)$ we simply have $N_{L/F(\gamma)}(\gamma) = \gamma^s$ and due to the multiplicativity of the norm symbol $N_{L/F}(\gamma) = N_{F(\gamma)/F}(\gamma)^s$.
From $w'(\gamma) \geq 0$, which is nothing else but $v \circ N_{L/F}(\gamma) \geq 0$, we obtain $v(((-1)^m a_0)^s) \geq 0$, which by the already proved property (2) means nothing else but $v((-1)^{ms}) + s \cdot v(a_0) \geq 0$. From the simple fact $v(1) = 0$ and of course $v(-1) = 0$ we therefore see $v(a_0) \geq 0$.
For norms we know that $N_{L/K}(g(\alpha)) = g(\alpha_1) \cdot \cdots \cdot g(\alpha_d)$ for an element $\alpha \in F$, with α_i being the conjugates of α. From that we obtain that

$$(-1)^m N_{F(\gamma)/F}(1 + \gamma) = (-1)^m f(-1) = (-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_0$$

and hence

$$v(N_{F(\gamma)/F}(1 + \gamma)) \geq 0 \text{ and } v(N_{L/F}(1 + \gamma)) \geq 0$$

since v is a valuation and we can apply property (3) on the last term, which gives us

$$v((-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_0) \geq min(1, a_{m-1}, a_{m-2}, \ldots, a_0)$$

where we already omitted the signs of the terms because of lemma 1.2.2.
But the last term is just what we wanted to show, namely $w'(1 + \gamma) \geq 0$.

In the last three paragraphs we have shown that w' really is a valuation on L.

We will now show, that it indeed is an extension of v.

Let $n = [L : F]$. By basic norm properties, which we already used, we have $w'(\alpha) = n \cdot v(\alpha)$ for $\alpha \in F^*$. Hence, the valuation $\frac{1}{n}w'$ is an extension of v to L. In general we do not have $\frac{1}{n}w'(L^*) = \mathbb{Z}$.
If we want an extension that is again normalized, we need to drop that $w|_F$ is normalized and add an additional factor:
Let $e = e\left(L/F, \frac{1}{n}w'\right)$. In a preceding lemma we saw that e must be finite, since $ef = n$ holds. We know define a new valuation

$$w = \frac{e}{n}w' : L^* \to \mathbb{Q}.$$

The fact that w is again a valuation is really easily shown, since it just differs by a factor from w' which is, as we already proved, a valuation.
We know for any prime element π_w with respect to w that we have

$$w(L^*) = w(\pi_w)\mathbb{Z} = \mathbb{Z}.$$

Therefore $w = \frac{e}{n}v \circ N_{L/F}$ is a discrete valuation on L and an extension of an equivalent the valuation $v'(\alpha) := e \cdot v(\alpha)$ which is equivalent to v and therefore preserves the important properties of a valuation.

In the above section we saw that w really is an extension on L. We will now show that L is a complete valuation field with respect to w.

L is complete Let $\hat{L}$ be the completion of L with respect to w and let $\hat{w}$ be the discrete valuation on $\hat{L}$. If we apply the third isomorphism theorem to the groups $\hat{w}(\hat{L}^*), w(L^*)$ and $v(F^*)$ we see that

$$[\hat{w}(\hat{L}^*) : v(F^*)] = [\hat{w}(\hat{L}^*) : w(L^*)] \cdot [w(L^*) : v(F^*)].$$

This is nothing else but

$$e(\hat{w}|v) = e(\hat{w}|w) \cdot e(w|v)$$

where the latter term $e(\hat{w}|w)$ must be 1 since w is already surjective. We can also explain this by the fact that the only values of $\hat{w}(\hat{L}^*)$ are the ones from $w(L^*)$ plus the limits. As we observed in the previous section after theorem 1.3.5 the sequence of those limits must become stable and therefore cannot have a value other than one that already is in $w(L^*)$.
We therefore define $e(\hat{w}|v) = e(\hat{w}|w) = e$.
We have a very similiar result for the inertia degree, namely

$$f(\hat{w}|v) = f(\hat{w}|w) \cdot f(w|v)$$

where $f(\hat{w}|w) = 1$ because of proposition 1.3.8.
Proposition 1.4.6 implies $[\hat{L} : F] = n$, but lemma 1.4.4 states $ef \leq n = [L : F]$. It easily follows that $L = \hat{L}$, and therefore L must be complete with respect to $w = \frac{1}{f}v \circ N_{L/F}$.

Uniqueness We will now prove that the above defined extension w of v is unique. Let therefore $\tilde{w}$ be another extension of v on L with $\tilde{w}(L^*) = \mathbb{Z}$. Then $\tilde{w}$ is again a discrete valuation and let w_0 be the induced valuation on F, defined by $w_0 = w|_F$.
If we use the basis from proposition 1.4.6 of L over F, we can write each element $\alpha \in L$ as

$$\alpha = \sum_{i,j} \rho_{ij}\theta_i \pi_w^j \text{ with } \rho_{ij}(\alpha) \in F.$$

According to lemma 1.4.7 we have:

$$w(\alpha) = \min_j \left\{ w_0 \left(\sum_i \rho_{ij}(\alpha)\theta_i \right) + j \right\}.$$

From that it can easily be seen that if $\alpha_k \to 0$ as $k \to +\infty$ with respect to the topology induced by w implies $\sum_i \rho_{ij}(\alpha_k)\theta_i \to 0$ as $k \to +\infty$ with respect to w_0 for $0 \leq j \leq e-1$.
On the other hand we have $\tilde{w}(\alpha + \beta) \geq \min\{\tilde{w}(\alpha), \tilde{w}(\beta)\}$ since $\tilde{w}$ is a valuation and therefore

$$\tilde{w}(\alpha) \geq \min_j \left\{ \tilde{w}_0 \left(\sum_i \rho_{ij}(\alpha)\theta_i \right) + j\tilde{w}(\pi_w) \right\}.$$

$\tilde{w}$ and w both are extensions of v on F and must therefore coincide on F, which means we have only *one* topology on F.
As we saw above we have $\sum_i \rho_{ij}(\alpha_k)\theta_i \to 0$ as $k \to +\infty$ with $\theta_{ij} \in F$. From this we obtain that we must have $\alpha_k \to 0$ as $k \to +\infty$ with respect to $\tilde{w}$.
Putting $\alpha_k = \pi_w^k$ we deduce that $\alpha \in \mathcal{M}_w$ implies $\alpha \in \mathcal{M}_{\tilde{w}}$ and $\mathcal{M}_w^i \subset \mathcal{M}_{\tilde{w}}^i$. If $w(\pi_{\tilde{w}}) \leq 0$ then $\pi_w \pi_{\tilde{w}}^k \in \mathcal{M}_w$ for any negative integer k by lemma 1.2.2.
Hence, $\pi_w \pi_{\tilde{w}}^k \in \mathcal{M}_{\tilde{w}}$, which means $\tilde{w}\left(\pi_w \pi_{\tilde{w}}^k\right) > 0$ for any negative integer k. But on the other hand

$$\tilde{w}(\pi_w \pi_{\tilde{w}}^k) = \tilde{w}(\pi_w) + k \cdot \tilde{w}(\pi_{\tilde{w}}) = \tilde{w}(\pi_w) + k$$

for any $k < 0$ which is clearly a contradiction since $\tilde{w}(\pi_w)$ must have a finite integer value by the first property of a valuation.
Therefore we must have $w(\pi_{\tilde{w}}) > 0$ and hence $w(\pi_{\tilde{w}}) \in \mathcal{M}_w$ and $\mathcal{M}_{\tilde{w}}^i \subset \mathcal{M}_w^i$. This shows that the topologies induced by w and $\tilde{w}$ coincide and by lemma 1.2.10 we see that we must have $w = \tilde{w}$.

□

Remark 1.4.9. *We can now see, that the definition of the ramification index which was given above implies the definition known from algebraic number theory.*
Let L be a finite extension of a discrete valuation field F. If v, and hence $w = \frac{1}{n} v \circ N_{L/F}$, is discrete and if $\mathcal{O}_v, \mathcal{M}_v, \pi$ resp. $\mathcal{O}_w, \mathcal{M}_w, \Pi$, are the valuation ring, the maximal ideal and a prime element of F resp. L, then

$$e = (w(\Pi)\mathbb{Z} : v(\pi)\mathbb{Z}),$$

so that $v(\pi) = e \cdot w(\Pi)$ and we find

$$\pi = \epsilon \cdot \Pi^e,$$

for some unit $\epsilon \in \mathbb{O}_w^*$*. From this we deduce the familiar interpretation of the ramification index:* $\mathcal{M}_v\mathcal{O}_w = \pi\mathcal{O}_w = \Pi\mathcal{O}_w = \mathcal{M}_w^e$*, or*

$$\mathcal{M}_v = \mathcal{M}_w^e.$$

We can now easily proof a lemma about the ramification index and the inertia degree:

Lemma 1.4.10. *Let L be a complete extension of F and E one of L with the respective valuations v of F, v' of L and v'' of E. Then we have:*

$$e(E/F, v'') = e(E/L, v'') \cdot e(L/F, v') \text{ and } f(E/F, v'') = f(E/L, v'') \cdot f(L/F, v').$$

Proof. If v'' is an extension of v' as we demand in the lemma, we just saw in the proof of the preceding theorem that $v''|_L = e(E/L, v'') \cdot v'$ and also $v'|_F = e(L/F, v') \cdot v$ holds, but also $v''|_F = e(E/F, v'') \cdot v$.
Hence it is a simple consequence, that we have

$$e(E/F, v'') = e(E/L, v'') \cdot e(L/F, v)$$

As we discussed above we consider the residue field $\overline{F}$ of F to be a subfield of the residue field $\overline{L}$ of L. Of course the same holds for $\overline{L}$ and $\overline{E}$, such that $\overline{L}$ is a subfield of $\overline{E}$. Since we have two extensions $E : L$ and $L : F$, $E : F$ of course is another complete extension with the same property for its residue fields, namely $\overline{F}$ is a subfield of $\overline{E}$.
This shows, that the property of being extensions of each other just drags down to the residue fields. From basic Algebra exercises we see that

$$[\overline{E} : \overline{F}] = [\overline{E} : \overline{L}] \cdot [\overline{L} : \overline{F}]$$

must be true. Which in terms of the inertia degeree is nothing else but $f(E/F, v'') = f(E/L, v'') \cdot f(L/F, v')$.

□

We now discuss the case of any algebraic extension of Henselian fields. The assertion of the preceding theorem is actually also valid for Henselian fields, as we used Hensel's lemma (1.3.11) to prove it. We therefore easily gain the uniqueness of an extension of a valuation on F to a finite extension L and even know how this extension looks like.

Theorem 1.4.11. *Let v be a discrete valuation on a Henselian field F. Then the discrete valuation v, in respect to which F is Henselian, has a unique extension to every finite algebraic extension L of F.*

Proof. The proof is verbatim the same is in the case of a complete field. □

We can also go a little further with Henselian fields.

Theorem 1.4.12. *Let F be a Henselian discrete valuation field and L an algebraic extension of F. Then there is precisely one valuation $w : L^* \to \mathbb{Q}$ (which is not necessarily discrete), such that the restriction $w|_F$ coincides with the discrete valuation v on F. Moreover, L is Henselian with respect to w.*

Remark 1.4.13. *The last assertion of the theorem does not hold if we replace* Henselian *with* complete. *However, in the case of a finite extension we already obtained that L is complete. As we now see, it will still be Henselian in any case.*

Sketch of proof. The first essential step in this proof of this is the way we extend the valuation to L. We already know that we have a unique extension to finite field extensions. Let $w_M : M^* \to \mathbb{Q}$ be that extention for the finite extension $M : F$ with $w_M|_F = v$. We now set:

$$w(\alpha) = w_M(\alpha) \text{ for every } \alpha \in L^* \text{ with } M = F(\alpha).$$

It is easy to verify that w really is an extension and it is straightforward to show it is unique by obtaining a contradiction to the uniqueness on finite field extensions. □

We will now state a corollary that will be used in chapter 2.

Corollary 1.4.14. *Let F be a Henselian discrete valuation field, and let L/F be a finite separable extension. Let v be the valuation on F and w the extension of v to L. Let $e = e(w|v)$ and $f = f(w|v)$, and $\pi_w \in L$ be a prime element with respect to w and $\theta_1, \ldots, \theta_f$ elements of $\mathcal{O}_w$ such that their residues form a basis of $\overline{F}_w$ over $\overline{F}_v$. Then $\theta_i \pi_w^j$ is a basis of the F-space L and of the $\mathcal{O}_v$-module $\mathcal{O}_w$, with $1 \leq i \leq f, 0 \leq j \leq e-1$. In particular, if $e = 1$, then*

$$\mathcal{O}_w = \mathcal{O}_v[\{\theta_i\}], \quad L = F(\{\theta_i\}),$$

and if $f = 1$, then

$$\mathcal{O}_w = \mathcal{O}_v[\pi_w], \quad L = F(\pi_w).$$

Proof. The proof is quite similar to the proof of lemma 1.4.4. □

We now state another corollary, that will give us a little detail on how the extension of a valuation looks like on other embeddings of L over F in F^{alg}. At this point we would like to make the agreement $F^{alg} = L^{alg}$, which will be valid for the entire text.

Corollary 1.4.15. *Let F be a Henselian discrete valuation field, and L/F a finite separable extension. Let w be the discrete valuation on L and $\sigma : L \to F^{alg}$ an embedding over F. Then $w \circ \sigma^{-1}$ is the discrete valuation on σL and*

$$\mathcal{M}_{\sigma L} = \sigma \mathcal{M}_L, \quad \mathcal{O}_{\sigma L} = \sigma \mathcal{O}_L.$$

1.5 Unramified and Ramified Extensions

In this section we define the new properties of extensions to be unramified, tamely ramified or totally ramified. This is important as we could describe an extension of fields by those terms. However, the proof of this would be too long and would need several lemmas, additional to those already given in this section. The fact that we can split up an extension in this way is important in proving the main theorem of local class field theory.

Remark 1.5.1. *At this point we would like to remind of the well known fact that every finite extension is of course algebraic, but not every algebraic extension has to be a finite one.*

Definition 1.5.2. A finite extension L of a Henselian discrete valuation field F is called *unramified* if $\overline{L}/\overline{F}$ is a separable extension of the same degree as L/F, namely

$$[\overline{L} : \overline{F}] = [L : F].$$

A finite extension L/F is called *totally ramified* if $f(L|F) = 1$.

Remark 1.5.3. 1. *Considering our fundamental equation*

$$e(L/F, w) \cdot f(L/F, w) = [L : F]$$

we can see that unramified means nothing else but $e(L/F, w) = 1$ and totally ramified $f(L/F, w) = 1$. We will use this implicitly later.

2. *By our definition an unramified extension is finite. We will extend this definition to infinite extensions later.*

From that definition and lemma 1.4.10 we can now easily see the following lemma:

Lemma 1.5.4. *If $L/F, M/L$ are unramified, then M/F is unramified.*

Sketch of proof: This can be seen with the lemma mentioned above and the transitivity of separability (for which see lemma A.3.24). □

Lemma 1.5.5. *Let F be a discrete valuation field. Then every subextension E/F of an unramified extension L/F is unramified.*

Proof. We have to prove two properties: First, the degree of the extension E/F must be the same as $\overline{E}/\overline{F}$ and $\overline{E}/\overline{F}$ must be separable.
The first fact simply follows from lemma 1.4.10. As we remarked, $e(E/F)$ must be 1 which can be obtained very easily. We know for the separable extension $\overline{L}/\overline{F}$ that every element $\alpha \in \overline{L}$ is separable over F, and therefore any subextension, which can only contain such separable elements, is also separable. □

Remark 1.5.6. *We will add the following definition to give a complete overview of the terminology, but focus on unramified and totally ramified extensions.*

Definition 1.5.7. A finite extension L/F is called *tamely ramified* if $\overline{L}/\overline{F}$ is a separable extension and $p \nmid e(L|F)$ when $p = char(\overline{F}) > 0$.

Before we give any statement about such extensions, we would like to remind of two basic facts that will be used in the following proofs:

(1) If we have an unramified extension L/F, which means $\overline{L}/\overline{F}$ is separable, we can apply the primitive element theorem (A.3.23) which states that we have $\overline{L} = \overline{F}(\theta)$ with $\theta \in L$.

(2) As we discussed earlier, we have a canonical mapping $F \to \overline{F}$, given by $\alpha \mapsto \overline{\alpha}$, where $\overline{\alpha}$ denotes the residue class of α.

We will now state two very useful lemmas which characterize unramified extensions.

Lemma 1.5.8. *Let L/F be an unramified extension, and $\overline{L} = \overline{F}(\theta)$ for some $\theta \in \overline{L}$. Let $\alpha \in \mathcal{O}_L$ be such that $\overline{\alpha} = \theta$.*
Then $L = F(\alpha)$ and L is separable over F, $\mathcal{O}_L = \mathcal{O}_F[\alpha]$. θ is a simple root of the polynomial $\overline{f}(x)$ which is irreducible over $\overline{F}$, where $f(x)$ is the monic irreducible polynomial of α over F.

Proof. We have $\theta \in \overline{L}$ is a root of $\overline{f}(x)$ which can be lifted to $\alpha \in \mathcal{O}_L$. Therefore $\alpha \in \mathcal{O}_L$ is a root of $f(x)$, $f(\alpha) = 0$, and by lemma A.4.12 we have $f(x) \in \mathcal{O}_F[x]$.
Furthermore,

$$[L : F] \geq [F(\alpha) : F] = \deg f(x) = \deg \overline{f}(x) \geq [\overline{F}(\theta) : F] = [L : F]. \tag{1.2}$$

where the latter equality holds because we have an unramified extension. It follows that $L = F(\alpha)$ and θ is a simple root of the irreducible polynomial $\overline{f}(x)$. Therefore, $\overline{f}'(\theta) \neq 0$ and $f'(\alpha) \neq 0$, i.e. α is separable over F. Applying proposition 1.4.6 helps us to see $\mathcal{O}_L = \mathcal{O}_F[\alpha]$.

□

Remark 1.5.9. *For a monic polynomial $f(x) \in F[x]$ for a valuation field F with valuation v we must have* $\deg f(x) = \deg \overline{f}(x)$, *because for any non-trival ideal I we can never have $1 \in I$ and therefore we know $1 \notin \mathcal{M}_v$.*

We will now show the converse of the preceding lemma.

Lemma 1.5.10. *Let $f(x)$ be a monic polynomial over $\mathcal{O}_F$, such that its residue is a monic separable polynomial over $\overline{F}$ and $\overline{f}(x) = g(x)$. Let α be a root of $f(x)$ in F^{alg}, and let $L = F(\alpha)$. Then the extension L/F is unramified and $\overline{L} = \overline{F}(\theta)$ for $\theta = \overline{\alpha}$.*

Proof. Let $f(x) = \prod_{i=1}^{n} f_i(x)$ be the decomposition of $f(x)$ into irreducible monic factors in $F[x]$. By the lemma of Gauss (A.2.19) we must have $f_i(x) \in \mathcal{O}_f[x]$.
Suppose that α is a root of $f_1(x)$. Then $g_1(x) = \overline{f_1}(x)$ is a monic separable polynomial over $\overline{F}$ since we demanded that $\overline{f}(x)$ is a monic separable polynomial. The Henselian property of F implies that $g_1(x)$ is irreducible over F. If it was not, we could find another decomposition of $f_1(x)$ and therefore had a contradiction to $f_1(x)$ is an irreducible factor. By lemma A.4.12 we get $\alpha \in \mathcal{O}_L$. Since we had $\theta = \overline{\alpha} \in \overline{L}$, we obtain $\overline{L} \supset \overline{F}(\theta)$ and

$$\deg f_1(x) = [L : F] \geq [\overline{L} : \overline{F}] \geq [\overline{F}(\theta) : \overline{F}] = \deg g_1(x) = \deg f_1(x).$$

The latter equality holds because of remark 1.5.9.
Thus, $\overline{L} = \overline{F}(\theta)$, and L/F is unramified. □

We will now prove a fact from which we will obtain the extended definiton of an unramified extension to infinite extensions.

Corollary 1.5.11. *If L/F is unramified, M is an algebraic extension of F and M is the discrete valuation field with respect to the extension of the valuation of F, then ML/M is unramified.*

Remark 1.5.12. *In the corollary above we demand M to be a discrete valuation field. In theorem 1.4.12 we stated, that this infinite extension is not always discrete. We will see later that in the case of an unramified extension, this condition is always true, and therefore no limitation.*

In this figure we show graphically what the assertion of the corollary is.

$$\begin{tikzcd}
M \arrow[r, dash] & ML \\
F \arrow[u, dash, "\text{unramified}"'] \arrow[r, dash, "\text{algebraic}"] & M \arrow[u, dash, "\text{unramified}"']
\end{tikzcd}$$

Proof. Let $L = F(\alpha)$ with $\alpha \in \mathcal{O}_L$ and let $f(x)$ be the monic irreducible polynomial of α, which is in $\mathcal{O}_L$ by lemma A.4.12.
If we had $\alpha \in \mathcal{M}_L$ we would obtain:

$$\overline{\alpha} \in \overline{F} \text{ and so } \overline{L} = \overline{F}$$

which would be the trivial extension so we must have $\overline{L} = \overline{F}(\alpha)$ by assuming to have an unramified extension.
It is easy to see that we have $ML = M(\alpha)$ by noting that $L = F(\alpha)$ and $F \subset M$. We denote the irreducible monic polynomial of α over M by $f_1(x)$. By the Henselian property of M we obtain that $\overline{f_1}(x)$ must be a power of an irreducible polynomial over $\overline{M}$. If it would decomposite into at least two relatively prime factors we would gain a decomposition of $f(x)$ over M.
However, $\overline{f_1}(x)$ divides $\overline{f}(x)$, as α is a root of both polynomials and we of course must have $\deg f_1 \leq \deg f$, which drags down to the residue fields. Hence, $f_1(x)$ is irreducible separable over $\overline{M}$ since $f(x)$ is separable. Applying lemma 1.5.10, we conclude that $ML/M = M(\alpha)/M$ is unramified. □

The next corollary is easily obtained from what we have so far.

Corollary 1.5.13. *Let L_1/F and L_2/F be unramified extensions, then L_1L_2/F is unramified.*

Proof. From lemma 1.5.11 we know that L_1L_2/L_1 must be unramified, since L_1/F is an unramified extension and therefore finite by our current definition, hence algebraic. Applying lemma 1.5.4 completes the proof. □

We will now really, as already mention before, extend our definition of unramified extensions to infinite extension of a Henselian discrete valuation field F.

Definition 1.5.14. Let L be an algebraic extension of a Henselian discrete valuation field F. We call L/F *unramified* if L/F, $\overline{L}/\overline{F}$ are separable extensions and $e(w|v) = 1$, where v is the discrete valuation on F, and w is the unique extension of v on L.

Remark 1.5.15. *Lemma 1.5.8 shows that a finite unramified extension is always separable. Therefore the definition above really is an extension of our previous definition in the finite case.*

The assertion of corollary 1.5.13 shows that the composite of all finite unramified extensions of F in a fixed algebraic closure F^{alg} of F is unramified. From theorem 1.4.12 we know that this extension - since we limited it to be in an algebraic closure - is a Henselian valuation field. Since we have $e(L|F) = 1$ for unramified extensions we see that the valuation on L must be discrete - this simply follows from the construction of the extension on finite extensions, where we had:

$$w(\alpha) = \frac{e}{n} \cdot v \circ N_{L/F}(\alpha).$$

This extension is called the *maximal unramified extension* F^{ur} of F.

We know from Galois theory that the essential properties of an unramified extension are invariant under automorphisms. Therefore if L is an unramified extension of a discrete valuation field F, and $\sigma \in \mathrm{Gal}(F^{sep}|F)$, then $\sigma(L)$ is another unramified extension of F. Hence the maximality of F^{ur} implies $\sigma(F^{ur}) = F^{ur}$ for any automorphism of the separable closure F^{sep} (see A.3.17 for the definition) over F. By lemma A.3.25 we see that F^{ur} is Galois over F.

We will now prove a few facts about unramified extensions that we will need later.

Proposition 1.5.16. *Let L/F be an unramified extension and let $\overline{L}/\overline{F}$ be a Galois extension. Then L/F is Galois.*

Proof. It suffices to prove the assertion for finite unramified extensions, since the composite of such Galois extensions is Galois. This can easily be seen from the transitivity of separability and normality.
We therefore assume L/F to be a finite unramified extension with $\overline{L}$ is Galois over $\overline{F}$. Let $\overline{L} = \overline{F}(\theta)$ as in previous proofs and let $g(x)$ be the irreducible monic polynomial of θ over $\overline{F}$. Then

$$g(x) = \prod_{i=1}^{n}(x - \theta_i),$$

with $\theta_i \in \overline{L}$ which are all distinct due to separability. Let us, without loss of generality, assume $\theta_1 = \theta$.
Let $f(x)$ be a monic polynomial over $\mathcal{O}_F$ of the same degree as $g(x)$ and $\overline{f}(x) = g(x)$. The Henselian property 1.3.11 implies

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i),$$

with $\alpha_i \in \mathcal{O}_L, \alpha_i = \theta_i$. Lemma 1.5.8 shows that $L = F(\alpha)$ and we deduce that L/F is Galois. □

We will now show the converse of the preceding proposition, but also a little more about the Galois groups of L/F and $\overline{L}/\overline{F}$.

Proposition 1.5.17. *Let L/F be an unramified Galois extension. Then $\overline{L}/\overline{F}$ is Galois. For an automorphism $\sigma \in \mathrm{Gal}(L/F)$ let $\overline{\sigma}$ be the automorphims in $\mathrm{Gal}(\overline{L}/\overline{F})$ satisfying the relation $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$ for every $\alpha \in \mathcal{O}_L$. Then the map $\sigma \mapsto \overline{\sigma}$ induces an isomorphism of $\mathrm{Gal}(L/F)$ onto $\mathrm{Gal}(\overline{L}/\overline{F})$.*

Proof. We first note that $\overline{\sigma}$ is unique and well defined:

(Uniqueness) If for $\sigma \in \mathrm{Gal}(L/F)$, $\overline{\sigma}_1$,$\overline{\sigma}_2$ were two such automorphism satisfying $\overline{\sigma}_1(\overline{\alpha}) = \overline{\sigma(\alpha)}$ we can easily see that we have

$$\overline{\sigma}_1(\overline{\alpha}) = \overline{\sigma}_2(\overline{\alpha}) \text{ for every } \overline{\alpha} \in \mathcal{O}_L/\mathcal{M}_{\mathcal{L}}$$

which is equivalent to $\overline{\sigma}_1 = \overline{\sigma}_2$.

(Well-defined) Our first observation is, that we have $\sigma(\mathcal{M}_L) = \mathcal{M}_L$. This is because $\mathcal{M}_L$ is the unique maximal ideal and $\sigma(\mathcal{M}_L)$ must be an ideal too, at least including $\mathcal{M}_L$. We now see, that if $\beta \in \mathcal{O}_L$ with $\overline{\beta} = \overline{\alpha}$, then $\sigma(\alpha - \beta) \in \mathcal{M}_L$.
It again suffices to verify the assertion for a finite unramified Galois extension L/F. Let $f(x)$ be the monic irreducible polynomial of α over F and $\theta \in \overline{L}$ such that $\overline{\alpha} = \theta$. By lemma 1.5.8 we saw that $\overline{f(x)}$ is separable. Since all roots of $f(x)$ belong to L, we obtain that all roots of $\overline{f(x)}$ belong to $\overline{L}$ and $\overline{L}/\overline{F}$ is Galois, due to corollary A.3.26.
It is a well known fact that the image of a root $\alpha_i \in L$ of a polynomial $f(x) \in F[x]$ under an automorphism $\sigma \in \mathrm{Gal}(L/F)$ must be another root $\alpha_j \in L$ of the same polynomial. The homomorphism $\mathrm{Gal}(L/F) \to \mathrm{Gal}(\overline{L}/\overline{F})$ defined by $\sigma \mapsto \overline{\sigma}$ as discussed above is surjective because the condition $\overline{\sigma}(\theta) = \theta_i$ implies $\sigma(\alpha) = \alpha_i$ for the root α_i of $f(x)$ with $\alpha_i = \theta_i$. Since $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(\overline{L}/\overline{F})$ are of the same order by the fundamental theorem of Galois theory we conclude

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(\overline{L}/\overline{F}).$$

□

From the above propositions we can now obtain the following corollary about the residue field of the maximal unramified extension F^{ur}.

Corollary 1.5.18. *The residue field $\overline{F^{ur}}$ of F^{ur} coincides with the separable closure $\overline{F}^{sep}$ of $\overline{F}$ and $\mathrm{Gal}(F^{ur}/F) \simeq \mathrm{Gal}(\overline{F}^{sep}/\overline{F})$.*

Proof. We will proceed in two steps, first proving $\overline{F^{ur}} \subseteq \overline{F}^{sep}$ and then the converse.

(1) First we observe that we must have $\overline{F^{ur}} \subseteq \overline{F}^{sep}$ because F^{ur} is unramified over F and therefore separable by definition and we also have $\overline{F^{ur}}$ is separable over $\overline{F}$, and hence $\overline{F^{ur}} \subseteq \overline{F}^{sep}$.

(2) Let θ be in $\overline{F}^{sep}$ and $g(x)$ its monic irreducible polynomial over $\overline{F}$. Let $f(x)$ be a monic irreducible polynomial over $\mathcal{O}_L$ such that $\overline{f}(x) = g(x)$. Then we have a set $\{\alpha_i\}$ of roots of $f(x)$ with $\alpha_i \in \mathcal{O}_L$ for each i and we define $L = F(\{\alpha_i\})$. Since by lemma 1.5.10 L is an unramified extension we must have $L \subset F^{ur}$ and $\theta = \overline{\alpha}_i \in \overline{F^{ur}}$ for a suitable i.

Hence we have: $\overline{F^{ur}} = \overline{F}^{sep}$. □

We finally give a proposition and a corollary of it that are helpful in proving that an abelian extension can be seen as the composite of an unramified extension and a totally ramified extension. This result, however, would require a few more things we cannot state or prove here. For more on this, see [FeVo1].

Proposition 1.5.19. *Let L be an algebraic extension of F and let L be a discrete valuation field. Then $L^{ur} = LF^{ur}$ and $L_0 = L \cap F^{ur}$ is the maximal unramified subextension of F which is contained in L. Moreover, $\overline{L}/\overline{L}_0$ is a purely inseparable extension.*

$$\begin{tikzcd}
F \arrow[r, dash] \arrow[d, dash] & F^{ur} \arrow[r, dash] \arrow[d, dash] & F^{sep} \arrow[d, dash] \\
L \arrow[r, dash] & L^{ur} = LF^{ur} \arrow[r, dash] & L^{sep}
\end{tikzcd}$$

Proof. Lemma 1.5.11 implies $L^{ur} \supseteq LF^{ur}$ since F^{ur} clearly is an unramified extension of F and L an algebraic one by assumption. We therefore obtain $F^{ur}L/L$ is an unramified extension and hence $F^{ur}L \subseteq L^{ur}$. In the preceding section we discussed that we must have $\overline{F} \subseteq \overline{L}$ for an extension L/F. If we apply that here, we get:

$$\overline{LF^{ur}} \supseteq \overline{L} \quad \text{and} \quad \overline{LF^{ur}} \supseteq \overline{F^{ur}} = \overline{F}^{sep}$$

by the preceding corollary 1.5.18. $\overline{LF^{ur}}$ therefore contains the compositum $\overline{LF}^{sep}$, which conincides with $\overline{L}^{sep}$ since L is an algebraic extension of F and we therefore must have $F^{sep} = L^{sep}$ and $\overline{F}^{sep} = \overline{L}^{sep}$ because $\overline{L}/\overline{F}$ is algebraic. We deduce $L^{ur} = LF^{ur}$.
An unramified subextension of F in L is clearly contained in L_0 and L_0/F is unramified due to lemma 1.5.5.
Let $\theta \in \overline{L}$ be separable over $\overline{F}$, and let $g(x)$ be the monic irreducible polynomial of θ over $\overline{F}$. Let $f(x)$ be a monic polynomial with coefficients in $\mathcal{O}_F$ of the same degree as $g(x)$ and $\overline{f}(x) = g(x)$. Then there exists a root $\alpha \in \mathcal{O}_L$ of the polynomial $f(x)$ with $\overline{\alpha} = \theta$ because of the Henselian property. Because of lemma 1.5.10 we see that $F(\alpha)/F$ is unramified. By our choice of θ we have $\theta \in \overline{L}$ and $\alpha \in \mathcal{O}_L \subset L$. Therefore $F(\alpha)$ is an unramified subextension of L/F and therefore contained in L_0, which shows $\alpha \in L_0$ and $\theta \in \overline{L}_0$.
By that we don't have any other separable elements over $\overline{F}$ which are contained in $\overline{L}$ but not in $\overline{L_0}$. Hence L_0 must be the maximal unramified subextension of F which is contained in L.
The construction of our proof also showed that $\overline{L}/\overline{L}_0$ is purely inseparable.

□

The next corollary is an amendment to the proposition above.

Corollary 1.5.20. *Let L be a finite separable extension of a Henselian discrete valuation field F and let $\overline{L}/\overline{F}$ be separable. Then L is a totally ramified extension of $L_0 = L \cap F^{ur}$, L^{ur} is a totally ramified extension of F^{ur} and $[L : L_0] = [L^{ur} : F^{ur}]$.*

Proof. By previous discussions we saw that we must have $f(L|L_0) = 1$ because $f(L_0|F) = n$ and we apply lemma 1.4.10. For the same reason we see that

$$e(L|L_0) = [L : L_0]. \tag{1.3}$$

Lemma 1.4.10 again implies

$$e(L^{ur}|F^{ur}) = e(L^{ur}|F) = e(L^{ur}|L) \cdot e(L|L_0) \cdot e(L_0|F) = e(L|L_0)$$

because we have $e(L^{ur}|L) = 1$ and $e(L_0|F) = 1$ by definiton and the proposition above. By the 2nd isomorphism theorem (A.1.11) we see:

$$L^{ur}/F^{ur} = LF^{ur}/F^{ur} \simeq L/(L \cap F^{ur}) = L/L_0$$

where we just inserted the results of the propositon above and considered our fields to be additive groups. We therefore obtain

$$[L : L_0] = [L^{ur} : F^{ur}]. \tag{1.4}$$

Combining the equations (1.3) and (1.4) gives us $e(L^{ur}|F^{ur}) = [L^{ur} : F^{ur}]$ and therefore by proposition 1.4.6 $f(L^{ur}|F^{ur}) = 1$. But the latter means, L^{ur}/F^{ur} is a totally ramified extension. □

We next regard the case of a finite Galois extension.

Let therefore L be a finite Galois extension of F. First we state a lemma that can easily be deduced from corollary 1.4.15 and will therefore not be proved.

Lemma 1.5.21. *Let L be a finite Galois extension of F. Then $v \circ \sigma = v$ for the discrete valuation v on L and $\sigma \in \mathrm{Gal}(L/F)$. If π is a prime element in L, then $\sigma\pi$ is a prime element and*

$$\sigma\mathcal{O}_L = \mathcal{O}_L, \quad \sigma\mathcal{M}_L = \mathcal{M}_L.$$

The next proposition seems a little long in its assertion, but will be needed when we define the set Frob and the Neukirch homomorphism, which will be needed for the local reciprocity law. We will also give the prove, as it is not long an only relies on already discussed statements.

Proposition 1.5.22. *Let L be a finite Galois extension of F and let L_0/F be the maximal unramified subextension in L/F. Then L_0/F and $\overline{L}_0/\overline{F}$ are Galois. The map $\sigma \to \overline{\sigma}$ defined with*

$$\overline{\sigma}(\overline{\alpha}) = \overline{\sigma\alpha} \quad \text{for every } \alpha \in \mathcal{O}_L$$

induces the surjective homomorphisms $\mathrm{Gal}(L/F) \to \mathrm{Gal}(L_0/F) \to \mathrm{Gal}(\overline{L}_0/\overline{F})$. If, in addition, $\overline{L}/\overline{F}$ is separable, then $\overline{L} = \overline{L}_0$ and $\overline{L}/\overline{F}$ is Galois, and L/L_0 is totally ramified.

The extension L^{ur}/F is Galois and the group $\mathrm{Gal}(L^{ur}/L_0)$ *is isomorphic to* $\mathrm{Gal}(L^{ur}/L) \times \mathrm{Gal}(L^{ur}/F^{ur})$*, and*

$$\mathrm{Gal}(L^{ur}/F^{ur}) \simeq \mathrm{Gal}(L/L_0), \quad \mathrm{Gal}(L^{ur}/L) \simeq \mathrm{Gal}(F^{ur}/L_0).$$

Proof. Let $\sigma \in \mathrm{Gal}(L/F)$. Then corollary 1.4.15 implies that σL_0 is also unramified over F, hence $L_0 = \sigma L_0$, since L_0 was the maximal unramified subextension, which is unique. Further, L_0/F is of course Galois, since it a subextension with a stable intermediate field (see lemma A.3.25). From proposition 1.5.17 we can easily see that the homomorphism $\mathrm{Gal}(L/F) \rightarrow \mathrm{Gal}(\overline{L}_0/\overline{F})$ is surjective. By previous discussions we saw that F^{ur}/F is Galois (we applied the same lemma A.3.25 to see that). Now, L/F is also a Galois extension, and therefore LF^{ur}/F is a Galois extension. We now had $L^{ur} = LF^{ur}$ in proposition 1.5.19. Therefore L^{ur}/F is a Galois extension.

The last assertions can be deduced from Galois theory. The following diagram helps in seeing what we need to show:

$$\begin{tikzcd}
F \arrow[r, dash] & L_0 \arrow[r, dash] \arrow[d, dash] & \mathrm{L} \arrow[d, dash] & \\
 & F^{ur} \arrow[r, dash] & L^{ur} & = L \cdot F^{ur}
\end{tikzcd}$$

Since F^{ur} is the maximal unramified extension and L_0 is an unramified extension, it is clear that we must have $L_0 \subset F^{ur}$. Further:

$$\mathrm{Gal}(L^{ur}/L) \subset \mathrm{Gal}(L^{ur}/L_0) \text{ and } \mathrm{Gal}(L^{ur}/F^{ur}) \subset \mathrm{Gal}(L^{ur}/L_0).$$

We know from proposition 1.5.17, that $L_0 = L \cap F^{ur}$ and therefore those two Galois subgroups above are disjoint. Also, they generate the whole group because of $L^{ur} = L \cdot F^{ur}$. This shows the first isomorphism. The others are quite easy to see.

□

We will now give a little lemma that we will need in the next chapter. However, the proof would need some other lemmas which we will not state here.

Lemma 1.5.23. *Let L be a finite Galois extension of F and $\overline{L}$ a separable extension of $\overline{F}$. If the extension is totally ramified, then* $\mathrm{Gal}(L/F)$ *is soluble.*

Chapter 2

The Local Reciprocity Law

In this chapter, we will state and prove the local reciprocity law. The short first section gives a little extra information on local fields and useful statements about them. In the second section, we define and study the Neukirch map. This map was first introduced by J. Neukirch ([Ne2]) and used by I. Fesenko ([FeVo1]) to combine it with the Hazewinkel map to a proof of the Local Reciprocity Law that allows to see better what we are doing. In section four we actually state and prove the Local Reciprocity Law. In the last section we give the existence theorem, a very important theorem obtained from the Local Reciprocity Law.
This chapter mainly follows an approach by I. Fesenko ([FeVo1]). We are trying to give enough extra information to get an idea of how we proceed, but omit mainly technical lemmas to not blur the sight on things. Most of the parts are, however, purely field arithmetical. This might seem a little too technical in the beginning, but once all the statements are worked through, everything will nicely fit together. This chapter should give an idea of how complicated and how much into detail things get with reciprocity.

2.1 Local Fields

In this section we will prove a few facts about locals fields and discuss their inner structure. However, we will focus on local fields with a finite residue field instead of a perfect one. We will therefore denote the residue field of F by $\overline{F} = \mathbb{F}_q$ in this section (where q is a prime power p^f). The number f is called the *absolute residue degree* of F.

We next gain a decomposition of F^* which will be useful and is actually quite easy to see.

Proposition 2.1.1. *The multiplicative group of a local field F admits the decomposition*

$$F^* = (\pi) \times \mu_{q-1} \times U^{(1)}$$

where π is a prime element, $(\pi) = \{\pi^k | k \in \mathbb{Z}\}, q = |\overline{F}|$ is the number of elements in the residue class field $\overline{F} = \mathcal{O}_v/\mathcal{M}_v$, and $U^{(1)} = 1 + \mathcal{M}_v$ is the group of principal units. *By μ_{q-1} we denote the group of $(q-1)$-th roots of unity.*

Remark 2.1.2. *We defined the group of principal units since we get a nice decomposition of the mulitplicative group of a local field from it. We will later redefine those principal units as $U^{(1)} = 1+\pi\mathcal{O}$, which can easily be seen to be the same. But the second definition will be expanded to higher groups of units, which we will need later.*

Proof. For every $\alpha \in F^*$ we have, due to lemma 1.2.7, a unique representation $\alpha = \epsilon\pi^n$ with $n \in \mathbb{Z}, \epsilon \in \mathcal{O}^*$ such that $F^* = (\pi) \times \mathcal{O}^*$. As we remarked in a previous section, the polynomial $x^{q-1} - 1$ splits into linear factors over F by Hensel's lemma. Therefore $\mathcal{O}^*$ contains the group μ_{q-1} of $(q-1)$-th roots of unity. The canonical homomorphism $\mathcal{O}^* \to \overline{F}^*$ defined by $\alpha \mapsto \alpha \mod \mathcal{M}_v$, obviously has kernel $U^{(1)}$ and maps μ_{q-1} bijectively onto $\overline{F}^*$. Hence $\mathcal{O}^* = \mu_{q-1} \times U^{(1)}$. □

Remark 2.1.3. 1. *The latter result of the proof, namely*

$$\mathcal{O}^* = \mu_{q-1} \times U^{(1)}$$

will be explicitly needed in the following proof and should therefore be mentioned seperately.

2. *We would also like to denote explicitly, that the canonical homomorphism $\mathcal{O}^* \to \overline{F}^*$ defined by $\alpha \mapsto \alpha \mod \mathcal{M}_v$, has kernel $U^{(1)}$. This means, that the set μ_{q-1} of (q-1)-th roots of unity forms, together with 0, a complete set of representatives of $\overline{F}^*$ in $\mathcal{O}_v$.*

The next result is a very specific characterization of local fields. Althought the proof is not that complicated it is rather lengthly and will therefore be omitted here.

Proposition 2.1.4. *The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$*[1].

Proof. See [Ne2, Chapter II, section 5]. □

With this result, we can get a better decomposition of F^* for local fields with finite residue field.

Proposition 2.1.5. *Let F be a local field and $q = p^f$ the number of elements in the residue class field. Then the following hold:*

1. *If F has characteristic 0, then one has (both algebraically and topologically)*

$$F^* \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

where $a \geq 0$ and $d = [F : \mathbb{Q}_p]$.

2. *If F has characteristic p, then one has (both algebraically and topologically)*

$$F^* \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$

Proof. See [Ne2, Chapter 2]. □

[1] For a field K we denote the formal power series over t with $K[[t]]$. $K[[t]]$ is an integral domain and we denote its quotient field with $K((t))$. This field is called the field of *Laurent series* over K.

2.2 The Norm Map

In this section we regard the norm map for a finite field extension. We will obtain a few useful commutative diagrams that will be used later. The proofs of this section are rather technical, but give a lot of extra information on local field arithmetic.

We will now see that F^{ur}/F is a Galois extension and that the Galois group $\mathrm{Gal}(F^{ur}/F)$ is cyclic and generated by an element called the *Frobenius automorphism.*

Proposition 2.2.1. *For every $n \geq 1$ there exists a unique unramified extension L of F of degree n: $L = F(\mu_{q^n-1})$. The extension L/F is cyclic and the maximal unramified extension F^{ur} of F is a Galois extension.* $\mathrm{Gal}(F^{ur}/F)$ *is isomorphic to $\hat{\mathbb{Z}}$ and topologically generated by an automorphism φ_F, such that*

$$\varphi_F(\alpha) \equiv \alpha^q \mod \mathcal{M}_{F^{ur}} \qquad \text{for } \alpha \in \mathcal{O}_{F^{ur}}.$$

The automorphism φ_F is called the Frobenius auotmorphism *of F.*

Proof. As we discussed above in proposition 2.1.1, F contains the group μ_{q-1} of $(q-1)$th roots of unity. This group is the set of nonzero multiplicative representatives of $\overline{F}$ in $\mathcal{O}$ as we showed in example 1.3.13. As we remarked in 2.1.3, the proof of the preceding proposition implies that the unit group $U_F = \mathcal{O}^*$ is isomorphic to $\mu_{q-1} \times U^{(1)}$. By that we see that μ_{q-1} is in $\overline{F}$ and F and therefore does not change if we regard $\overline{F}$ instead of F or vice-a-versa.
The field $\overline{F} = \mathbb{F}_q$ has the unique extension $\mathbb{F}_{q^n}$ of degree n, which is, as we know from basic algebra, cyclic over $\mathbb{F}_q$. (A cyclic group of order n is clearly isomorphic to $\mathbb{Z}/n\mathbb{Z}$). By lemma 1.5.8 and proposition 1.5.16 we see that there must be a unique unramified Galois extension L of degree n. Namely, if we demand $\overline{L}$ to be $\mathbb{F}_{q^n}$ we have $\overline{L} = \overline{F}(\mu_{q^n-1})$. We see by the discussion above and lemma 1.5.8, that we must have $L = F(\mu_{q^n-1})$. Because of proposition 1.5.16 it is a Galois extension.
Now let E be an unramified extension of F and $\alpha \in E$. Then $F(\alpha)/F$ is of finite degree. Therefore, F^{ur} is contained in the union of all finite unramified extensions of F. We have

$$\mathrm{Gal}(F^{ur}/F) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Z}/n\mathbb{Z}) \cong \hat{\mathbb{Z}}.$$

The first isomorphism holds because of proposition A.5.10.
We can see in [FrJa] that $\mathrm{Gal}(\mathbb{F}_q^{sep}/\mathbb{F}_q)$ is topologically generated by the automorphism σ such that $\sigma(a) = a^q$ for $a \in \mathbb{F}_q^{sep}$. Hence, $\mathrm{Gal}(F^{ur}/F)$ is topogically generated by the Frobenius automorphism φ_F.

□

We will now go a little deeper into the norm map and will obtain very useful lemmas. Those will help proving the main theorem of local class field theory.

This first lemma is just a useful tool for proving the others. The proof is quite straight forward and will therefore be omitted.

Lemma 2.2.2. *Let L/F be a separable extension of prime degree n and $\gamma \in \mathcal{M}_L$. Then*

$$N_{L/F}(1+\gamma) = 1 + N_{L/F}(\gamma) + \mathrm{Tr}_{L/F}(\gamma) + \mathrm{Tr}_{L/F}(\delta)$$

with some $\delta \in \mathcal{O}_L$ such that $v_L(\delta) \geq 2v_L(\gamma)$.

The next statement is helpful in understanding the following proposition and the commutative diagrams at the end of this section. But first we need a definition.

Definition 2.2.3. The group $1 + \pi\mathcal{O}$ is called the *group of principal units* U_1 and its elements are called *principal units*. We would also like to introduce higher groups of units as follows:

$$U_i = 1 + \pi^i\mathcal{O} \quad \text{for} \quad i \geq 1.$$

Remark 2.2.4. *We already used the group of principal units in the proposition before remark 2.1.2. But as we remarked in that remark we now redefined this group in a way that allows the definition of higher groups of units as well. Therefore we now denote this group by U_i instead of $U^{(i)}$.*

We can now state a first proposition using those definitions. The proof is quite easy to see once it is written down, but we will give it anyway to see what is going on.

Proposition 2.2.5. *Let F be a discrete valuation field. Then:*

1. *The choice of a prime element π $(1 \in \mathbb{Z} \to \pi \in F^*)$ splits the exact sequence*

$$1 \to U_F \to F^* \xrightarrow{v} \mathbb{Z} \to 0.$$

The group F^* is isomorphic to $U_F \times \mathbb{Z}$.

2. *The canonical map $\mathcal{O} \to \mathcal{O}/\mathcal{M} = \overline{F}$ induces the surjective homomorphism*

$$\lambda_0 : U_F \to \overline{F}^*, \quad \epsilon \mapsto \overline{\epsilon}.$$

λ_0 maps U/U_1 isomorphically onto $\overline{F}^*$.

3. *The map*

$$\lambda_i : U_i \to \overline{F}, \qquad 1 + \alpha\pi^i \mapsto \overline{\alpha}$$

for $\alpha \in \mathcal{O}$ induces the isomorphism λ_i of U_i/U_{i+1} onto $\overline{F}$ for $i \geq 1$.

Proof. We proceed proving the proposition in the three steps as we stated it.

(1) The first statement follows easily from the uniqueness of the representation $\alpha = \epsilon\pi^i$ with $\alpha \in F^*, \epsilon$ a unit and π a prime element in F. We would like to remind again that we had the agreement to regard all our valautions to be normalized, which gives us the surjectivity. The injectivity of from $U_F \to F^*$ should be very clear.

(2) The kernel of λ_0 coincides with U_1 and λ_0 is of course surjective.

(3) The induced map $U_i/U_{i+1} \to \overline{F}$ is a homomorphism, since we have

$$(1+\alpha_1\pi^i)(1+\alpha_2\pi^i) = 1 + (\alpha_1+\alpha_2)\pi^i + \alpha_1\alpha_2\pi^{2i}.$$

From this we see that the last term, with π^{2i} will be eliminated when we factor by U_{i+1} since we had $i \geq 1$. By the definition of our map λ_i we can easily see the homomorphism property. Finally, if two such elements $(1+\alpha_1\pi^i), (1+\alpha_2\pi^i)$ are mapped into the same class of $\overline{F}$, we must have $\alpha_1 = \epsilon_1\pi^{i_1}, \alpha_2 = \epsilon_2\pi^{i_2}$ and without loss of generality $i_1 > i_2$ with no equality allowed and therefore those two elements are in the same class of U_i/U_{i+1}.

□

We can now proceed to the first proposition.

Proposition 2.2.6. *Let L/F be an unramified extension of degree n. Then a prime element π_F in F is a prime element in L. Let $U_{i,L} = 1 + \pi_F^i\mathcal{O}_L$, $U_{i,F} = 1 + \pi_F^i\mathcal{O}_F$ and let $\lambda_{i,L}, \lambda_{i,F}$, $(i \geq 0)$, be as follows:*

$$\lambda_i : U_i \to \overline{F}, \qquad 1 + \alpha\pi^i \mapsto \overline{\alpha}$$

for $\alpha \in \mathcal{O}$ and with $\pi = \pi_F$ for both fields F and L. And let

$$\lambda_0 : U \to \overline{F}^*, \qquad \epsilon \mapsto \overline{\epsilon}.$$

Then the following diagrams are commutative:

$$\begin{tikzcd} L^* \arrow[r, "v_L"] \arrow[d, "N_{L/F}"'] & \mathbb{Z} \arrow[d, "\times n"] \\ F^* \arrow[r, "v_F"] & \mathbb{Z} \end{tikzcd} \qquad \begin{tikzcd} U_L \arrow[r, "\lambda_{0,L}"] \arrow[d, "N_{L/F}"'] & \overline{L}^* \arrow[d, "N_{\overline{L}/\overline{F}}"] \\ U_F \arrow[r, "\lambda_{0,F}"] & \overline{F}^* \end{tikzcd}$$

$$\begin{tikzcd} U_{i,L} \arrow[r, "\lambda_{i,L}"] \arrow[d, "N_{L/F}"'] & \overline{L} \arrow[d, "\mathrm{Tr}_{\overline{L}/\overline{F}}"] \\ U_{i,F} \arrow[r, "\lambda_{i,F}"] & \overline{F} \end{tikzcd}$$

Proof. First we would like to prove the first fact, namely that a prime element π_F of F is also a prime element of L. By the definition of unramified we have $e = e(L/F) = 1$. But this means, the index of $w_0(F^*)$ in $w(L^*)$ is one. From this we deduce that the valuation of an element generating the whole group $w_0(F^*) = w(L^*)$ cannot change by going from w to w_0.

The first commutativity is a simple result of the construction of v_L as an extension of v_F. Due to proposition 1.5.17 we have: $\overline{N_{L/F}(\alpha)} = N_{\overline{L}/\overline{F}}(\overline{\alpha})$ for $\alpha \in \mathcal{O}_L$. This shows the commutivity of the second diagram.
The preceding lemma 2.2.2 shows that

$$N_{L/F}(1 + \theta\pi_F^i) = 1 + (\mathrm{Tr}_{L/F}\theta)\pi_F^i + (N_{L/F}\theta)\pi_F^{pi} + \mathrm{Tr}_{L/F}(\delta)$$

with $v_L(\delta) \geq 2i$ and, consequently, $v_F\mathrm{Tr}_{L/F}(\delta) \geq 2i$. Thus, we get

$$N_{L/F}(1 + \theta\pi_F^i) \equiv 1 + (\mathrm{Tr}_{L/F}\theta)\pi_F^i \mod \pi_F^{i+1}$$

and the commutativity of the third diagram. □

As our next step, we will prove a very similiar result for totally and ramified Galois extensions. This however is a bit more complicated and needs some preliminary work.

Let L/F be a totally ramified Galois extension of degree $p = \mathrm{char}(\overline{F}) > 0$. Then corollary 1.4.14 shows that $\mathcal{O}_L = \mathcal{O}_F[\pi_L]$, $L = F(\pi_L)$ for a prime element π_L in L, and $\overline{L} = \overline{F}$. Let σ be a generator of $\mathrm{Gal}(L/F)$, then $\frac{\sigma(\pi_L)}{\pi_L} \in U_L$. We can therefore write

$$\frac{\sigma(\pi_L)}{\pi_L} = \theta\epsilon \quad \text{with} \quad \theta \in U_F, \;\; \epsilon \in 1 + \mathcal{M}_L$$

because of the assertion of corollary 1.4.14 and $\overline{L} = \overline{F}$. Then

$$\sigma^2(\pi_L) = \sigma\left(\frac{\sigma(\pi_L)}{\pi_L} \cdot \pi_L\right) = \sigma(\pi_L \cdot \theta\epsilon) = \sigma(\pi_L) \cdot \sigma(\theta\epsilon)$$

and therefore

$$\frac{\sigma^2(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L}\sigma(\theta\epsilon) = \theta\epsilon \cdot \sigma(\theta\epsilon) = \theta^2\epsilon \cdot \sigma(\epsilon)$$

because $\theta \in U_F \subset F$.
We now repeat this step p times. Since we chose σ to be a generator of the Galois group $\mathrm{Gal}(L/F)$, σ^p must be the identity map due to the main theorem of Galois theory (A.3.27).

$$1 = \frac{\sigma^p(\pi_L)}{\pi_L} = \theta^p\epsilon \cdot \sigma(\epsilon) \cdot \dots \cdot \sigma^{p-1}(\epsilon).$$

This shows that $\theta^p \in 1+\mathcal{M}_L$ because everything else on the right side is and 1 is because $v(0) = \infty$, hence $0 \in \mathcal{M}_L$. We also obtain $\theta \in \mathcal{M}_F$, because raising to the p-th power is an injective homomorphism of $\overline{F}$. Thus we obtain $\frac{\sigma(\pi_L)}{\pi_L} \in 1 + \mathcal{M}_L$. Put

$$\frac{\sigma(\pi_L)}{\pi_L} = 1 + \eta\pi_L^s \quad \text{with} \quad \eta \in U_L, \;\; s = s(L|F) \geq 1. \tag{2.1}$$

Remark 2.2.7. *In the above proof $s = s(L|F)$ is a uniquely determined integer which is the same or all primes π_L in L with $L = F(\pi_L)$. This justifies the notation $s(L|F)$.*

Proposition 2.2.8. *Let $[a]$ denote the maximal integer less or equal to a. For an integer $i \geq 0$ put $j(i) = s + 1 + [\frac{i-1-s}{p}]$. Then*

$$\mathrm{Tr}_{L/F}\left(\pi_L^i \mathcal{O}_L\right) = \pi_F^{j(i)} \mathcal{O}_F.$$

The proof of this proposition is quite technical and would need another lemma and will therefore be omitted.

Proposition 2.2.9. *Let L/F be a totally ramified Galois extension of degree $p = \mathrm{char}(\overline{F}) > 0$. Let π_L be a prime element in L. Then $\pi_F = N_{L/F}\pi_L$ is a prime element in F. Let $U_{i,L} = 1 + \pi_L^i \mathcal{O}_L, U_{i,F} = 1 + \pi_F^i \mathcal{O}_F$ and let $\lambda_{i,L}, \lambda_{i,F}$ be as in proposition 2.2.6, for $\pi = \pi_L$ and $\pi = \pi_F$. Then the following diagrams are commutative:*

$$\begin{tikzcd}
L^* \arrow[r, "v_L"] \arrow[d, "N_{L/F}"'] & \mathbb{Z} \arrow[d, "id"] \\
F^* \arrow[r, "v_F"] & \mathbb{Z}
\end{tikzcd}
\qquad
\begin{tikzcd}
U_L \arrow[r, "\lambda_{0,L}"] \arrow[d, "N_{L/F}"'] & \overline{L}^* \arrow[d, "\uparrow p"] \\
U_F \arrow[r, "\lambda_{0,F}"] & \overline{F}^*
\end{tikzcd}$$

$$\begin{tikzcd}
U_{i,L} \arrow[r, "\lambda_{i,L}"] \arrow[d, "N_{L/F}"'] & \overline{L} = \overline{F} \arrow[d, "\uparrow p"] \\
U_{i,F} \arrow[r, "\lambda_{i,F}"] & \overline{F}
\end{tikzcd}
\quad \text{if } \ 1 \leq i < s.$$

$$\begin{tikzcd}
U_{s,L} \arrow[r, "\lambda_{s,L}"] \arrow[d, "N_{L/F}"'] & \overline{L} = \overline{F} \arrow[d, "\overline{\theta} \mapsto \overline{\theta}^p - \overline{\eta}^{p-1}\overline{\theta}"] \\
U_{s,F} \arrow[r, "\lambda_{s,F}"] & \overline{F}
\end{tikzcd}$$

$$\begin{tikzcd}
U_{s+pi,L} \arrow[r, "\lambda_{s+pi,L}"] \arrow[d, "N_{L/F}"'] & \overline{L} = \overline{F} \arrow[d, "\times(-\overline{\eta}^{p-1})"] \\
U_{s+i,F} \arrow[r, "\lambda_{s+i,F}"] & \overline{F}
\end{tikzcd}
\quad \text{if } \ i > 0.$$

Moreover, $N_{L/F}(U_{s+i,L}) = N_{L/F}(U_{s+i+1,L})$ for $i > 0, p \nmid i$.

Proof. The commutativity of the first and the second diagrams can be verified similarly to the proof of proposition 2.2.6. In order to look at the remaining diagrams, put $\epsilon = 1 + \theta\pi_L^i$ with $\theta \in U_L$. Then by lemma 2.2.2, we get

$$N_{L/F}\epsilon = 1 + N_{L/F}(\theta)\pi_F^i + \mathrm{Tr}_{L/F}(\theta\pi_L^i) + \mathrm{Tr}_{L/F}(\theta\delta) \tag{2.2}$$

with $v_L(\delta) \geq 2i$. The previous proposition implies that

$$v_F(\mathrm{Tr}_{L/F}(\pi_L^i)) \geq s + 1 + \left[\frac{i-1-s}{p}\right], \quad v_F(\mathrm{Tr}_{L/F}(\delta) \geq s + 1 + \left[\frac{2i-1-s}{p}\right]$$

and for $i < s$

$$v_F(\mathrm{Tr}_{L/F}(\pi_L^i)) \geq i + 1, \quad v_F(\mathrm{Tr}_{L/F}(\delta)) \geq i + 1.$$

Therefore we see that in equation 2.2 the last two terms could be added to the second term in the unique represenation. Since those terms have a valuation greater or equal to i, it will still remain in the same residue class. Therefore, the third diagram is commutative.

Further, using equation 2.1 and lemma 2.2.2, one can write

$$1 = N_{L/F}\left(\frac{\sigma(\pi_L)}{\pi_L}\right) \equiv 1 + N_{L/F}(\eta)\pi_F^s + \mathrm{Tr}_{L/F}(\eta\pi_L^s) \mod \pi_F^{s+1}.$$

with $\eta \in U_L$.

We deduce that

$$\mathrm{Tr}_{L/F}(\eta\pi_L^s) \equiv -N_{L/F}(\eta)\pi_F^s \mod \pi_F^{s+1}.$$

Since $N_{L/F}(\eta) \equiv \eta^p \mod \pi_L$ in view of $U_L \subset U_F U_{1,L}$ (which would be seen relatively easy), we conclude that

$$N_{L/F}(1 + \theta\eta\pi_L^s) - 1 - \eta^p\pi_F^s(\theta^p - \theta) \in \pi_L^{ps+1}\theta\mathcal{O}_L$$

for $\theta \in \mathcal{O}_F$. This implies the commutativity of the forth (putting $\theta \in \mathcal{O}_F$) and the fifth (when $\theta \in \pi_F^i\mathcal{O}_F$) diagram.

To prove the last assertion, we assume $p \nmid i, \theta \in \mathcal{O}_F$, then

$$\frac{\sigma(1 + \theta\pi_L^i)}{1 + \theta\pi_L^i} \equiv 1 + \theta\eta\pi_L^{i+s} \mod \pi_L^{i+s+1}.$$

This means that $N_{L/F}(1+i\theta\eta\pi_L^{i+s}) \in N_{L/F}U_{s+i+1,L}$ and $N_{L/F}(U_{s+i,L}) = N_{L/F}(U_{s+i+1,L})$. □

We now develop a bit more theory on the norm map that we will refer to later.

First we have a closer look at the norm group $N_{L/F}(L^*)$ for a finite extension L of F. Remember that we chose to local fields to have a finite residue field which we denoted by $\overline{F} = \mathbb{F}_q$ for F and $\overline{L} = \mathbb{F}_{q'}$ for L respectively.

First we regard

$$N_{\mathbb{F}_{q'}/\mathbb{F}_q} : \mathbb{F}_{q'}^* \to \mathbb{F}_q^*.$$

This map is surjective, when we have $\mathbb{F}_{q'} \supset \mathbb{F}_q$ which could be shown as an exercise. We now have look at the diagrams one and two of proposition 2.2.6. Since we proved in propostion 2.2.5 that the maps λ_i are surjective (and also λ_0) it follows from the surjectivity of $N_{\overline{L}/\overline{F}}$ that $N_{L/F}$ must also be surjective.

We therefore obtain $N_{L/F}U_L = U_F$ in the case of an unramified extension L/F. Further, the first diagram of 2.2.6 implies that

$$N_{L/F}L^* = (\pi^n) \times U_F$$

where π is a prime element in F and $n = [L : F]$ the degree of the finite extension L/F. From that representation we can observe particularly that $F^*/N_{L/F}L^*$ is a cyclic group of order n in this case of an unramified extension.

Remark 2.2.10. *We are particularly interested in this factor group $F^*/N_{L/F}L^*$, as it occurs in the local reciprocity law.*

Conversely we see that every subgroup of finite index in F^* that contains with U_F must coincide with the norm group $N_{L/F}L^*$ for a suitable unramified extension L/F.

2.3 The Neukirch Map

In this section we will follow an approach by I. Fesenko and S. Vostokov ([FeVo2]) which can also partly be found in [Ne1]. We will define and explain the Neukirch map, which is an essential step for proving the local reciprocity law. We therefore assume F to be a local field with finite residue field.

First we define the set $\mathrm{Frob}(L/F)$.

Let L be a finite Galois extension of F. According to proposition 1.5.19 we have $L^{ur} = LF^{ur}$.

Definition 2.3.1. We define

$$\mathrm{Frob}(L/F) = \{\tilde{\sigma} \in \mathrm{Gal}(L^{ur}/F) : \tilde{\sigma}|_{F^{ur}} \text{ is a positive integer power of } \varphi_F\}.$$

In propostion 2.2.1 we saw that $\mathrm{Gal}(F^{ur}/F) \simeq \hat{\mathbb{Z}}$ and is topolically generated by an element φ_F. It therefore consists of $\hat{\mathbb{Z}}$-powers of φ_F.

We will now gain a few properties about the set we defined above.

Proposition 2.3.2. 1. *The set* $\mathrm{Frob}(L/F)$ *is closed with respect to multiplication, but it is not closed with respect to inversion and* $1 \notin \mathrm{Frob}(L/F)$.

2. *The fixed field* Σ *of* $\tilde{\sigma} \in \mathrm{Frob}(L/F)$ *is of finite degree over* F, $\Sigma^{ur} = L^{ur}$, *and* $\tilde{\sigma}$ *is the Frobenius automorphism of* Σ.

3. *Thus, the set* $\mathrm{Frob}(L/F)$ *consists of the Frobenius automorphisms* φ_Σ *of finite extensions* Σ *of* F *in* L^{ur} *with* $\mathrm{Gal}(L^{ur}/\Sigma) \simeq \hat{\mathbb{Z}}$.

4. *The map* $\mathrm{Frob}(L/F) \longrightarrow \mathrm{Gal}(L/F)$, $\tilde{\sigma} \mapsto \tilde{\sigma}|_L$ *is surjective.*

This proof goes into the theory of profinite groups. Whenever this would be the necessary, we will only give a sketch of those steps or statements without further explaination.

Proof. The first assertion can be verified very easily.
We know from the general main theorem of Galois theory, that Σ must be an intermediate field of L^{ur}/F. Since we have $F \subset \Sigma \subset L^{ur}$ we deduce that $F^{ur} \subset \Sigma^{ur} \subset L^{ur}$. By definition $\tilde{\sigma}$ is a positive integer power of φ_F.
The Galois group of L^{ur}/Σ is topologically generated by $\tilde{\sigma}$. This can be seen considered that we have $L^{ur} = LF^{ur}$. We know that $\mathrm{Gal}(F^{ur}/F)$ is topologically generated by an element φ_F and isomorphic to $\hat{\mathbb{Z}}$. The same holds for L^{ur}/L. We therefore obtain, that $\mathrm{Gal}(L^{ur}/\Sigma)$ is isomorphic to $\hat{\mathbb{Z}}$. Having that property means, it does not have any nontrivial closed subgroups of finite order.
The group $\mathrm{Gal}(L^{ur}/F^{ur})$ is finite, since again we have $L^{ur} = LF^{ur}$. Therefore the group $\mathrm{Gal}(L^{ur}/\Sigma^{ur})$, being a subgroup of the finite group $\mathrm{Gal}(L^{ur}/F^{ur})$ should be trivial. So

$$L^{ur} = \Sigma^{ur}. \tag{2.3}$$

We now proceed with showing that Σ is a finite extension of F. Put $\Sigma_0 = \Sigma \cap F^{ur}$. This can be seen the fixed field of $\varphi_{F^{ur}} = \varphi_F^m$ with m being the positive integer power from the definition of $\text{Frob}(L/F)$. Therefore $[\Sigma_0 : F] = m$ is finite.
From corollary 1.5.20 we see really easily that

$$[\Sigma : \Sigma_0] = [\Sigma^{ur} : F^{ur}] = [L^{ur} : F^{ur}] = [L : L_0]$$

with $L_0 = L \cap F^{ur}$, is finite.
Thus, Σ/F, being the composite of Σ_0/F and Σ/Σ_0, is finite.

Now, since $L^{ur} = \Sigma^{ur}$, $\tilde{\sigma}$ is a power of φ_Σ. Further, $\varphi_{\Sigma|\Sigma_0} = \varphi_F^{[\Sigma_0:F]}|_{\Sigma_0} = \varphi_F^m|\Sigma_0 = \tilde{\sigma}|_{\Sigma_0}$. Therefore, $\tilde{\sigma} = \varphi_\Sigma$. Certainly, the Frobenius automorphism φ_Σ of a finite extension Σ of F in L^{ur} with $\text{Gal}(\Sigma^{ur}/\Sigma) = \text{Gal}(L^{ur}/\Sigma) \simeq \hat{\mathbb{Z}}$ as we saw above, belongs to $\text{Frob}(L/F)$.

Denote by $\tilde{\varphi}$ an extension in $\text{Gal}(L^{ur}/F)$ of φ_F. Let $\sigma \in \text{Gal}(L/F)$, then $\sigma|_{L_0}$ is equal to φ_F^n for some positive integer n. Hence $\sigma^{-1}\tilde{\varphi}^n|L$ acts trivially on L_0, and so $\tau = \sigma\tilde{\varphi}^{-n}|L$ belongs to $\text{Gal}(L/L_0)$. Let $\tilde{\tau} \in \text{Gal}(L^{ur}/F^{ur})$ be such that $\tilde{\tau}|L = \tau$. That is possible because of proposition 1.5.19. Then for $\tilde{\sigma} = \tilde{\tau}\tilde{\sigma}^n$ we deduce that $\tilde{\sigma}|_{F^{ur}} = \varphi_F^n$ and $\tilde{\varphi}|_L = \tau\tilde{\varphi}^n|_L = \sigma$. Then the element $\tilde{\sigma} \in \text{Frob}(L/F)$ is mapped to $\sigma \in \text{Gal}(L/F)$.

□

We see from that, that our set $\text{Frob}(L/F)$ really consists of the Frobenius automorphisms φ_Σ, where Σ runs through all finite extensions Σ of F in L^{ur} with $\text{Gal}(L^{ur}/\Sigma) \simeq \hat{\mathbb{Z}}$.

We can now define the Neukirch map. This map has been used by Neukirch in his book [Ne1] to prove the reciprocity law. However, Neukirch's approach is different from the one we present here as can be seen in the next chapter in comparison to [Ne1]. However, this part of his construction, the *Neukirch map*, is a very helpful step to proving the local reciprocity law.

Definition 2.3.3. Let L/F be a finite Galois extension. Define

$$\tilde{\Upsilon}_{L/F} : \text{Frob}(L/F) \longrightarrow F^*/N_{L/F}L^*$$

with

$$\tilde{\sigma} \mapsto N_{\Sigma/F}\pi_\Sigma \mod N_{L/F}L^*,$$

where Σ is the fixed field of $\tilde{\sigma} \in \text{Frob}(L/F)$ and π_Σ is any prime element of Σ.

We will now see that the above definition of $\tilde{\Upsilon}$ really is a well defined map.

Lemma 2.3.4. *The map $\tilde{\Upsilon}_{L/F}$ is well defined. Further, if $\tilde{\sigma}|_L = id|_L$, then $\tilde{\Upsilon}_{L/F}(\tilde{\sigma}) = 1$.*

Proof. Let π_1, π_2 be prime elements in Σ. Then we must have $\pi_1 = \pi_2\epsilon$ for a unit $\epsilon \in U_\Sigma$. Let E be the compositum of the extensions Σ and L of F. From the preceding proposition 2.3.2 we know that Σ is a finite extension, and L is one by definition. Therefore E is a finite extension of F.
We have $\Sigma \subset E \subset \Sigma^{ur}$ (remember equation 2.3, where we had $\Sigma^{ur} = L^{ur}$). Hence, the extension E/Σ is unramified. In the explainations on page 40 we saw $U_\Sigma = N_{E/\Sigma}(U_E)$,

whence $\epsilon = N_{E/\Sigma}\eta$ for some $\eta \in U_E$. Therefore, by the multiplicativity of the norm, we obtain

$$N_{\Sigma/F}\pi_1 = N_{\Sigma/F}(\pi_2\epsilon) = N_{\Sigma/F}\pi_2 \cdot N_{\Sigma/F}(N_{E/\Sigma}\eta) =$$
$$N_{\Sigma/F}\pi_2 \cdot N_{L/F}(N_{E/L}\eta),$$

where the last equality is true because we have, as is stated in the appendix, $N_{E/F}(\alpha) = N_{L/F}(N_{E/L}(\alpha))$ for any finite extension E of F and any intermediate field L, with $\alpha \in E$. We obtain that $N_{\Sigma/F}\pi_1 \equiv N_{\Sigma/F}\pi_2 \mod N_{L/F}L^*$ since $N_{E/L}\eta = U_L$ by our discussion on page 40.

If $\tilde{\sigma}|_L = id|_L$, then it is clear that we must have $L \subset \Sigma$. We again use the property of norms for intermediate fields

$$N_{\Sigma/F}\pi_\Sigma = N_{L/F}(N_{\Sigma/L}(\pi_\Sigma)).$$

Now the inner term on the right, $N_{\Sigma/L}(\pi_\Sigma)$, cannot have norm 0. That can easily be seen by remembering how we extended a valuation to an extension (namely using the norm map). Hence, $N_{\Sigma/L}(\pi_\Sigma) \in L^*$ and

$$N_{\Sigma/F}\pi_\Sigma \in N_{L/F}L^*.$$

□

We will now give a few properties about the Neukirch map. We will therefore alter the map a little bit to obtain not just a homomorphism, but an isomorphism.

Theorem 2.3.5. *Let L be an unramified extension of F of finite degree.*
Then $\tilde{\Upsilon}_{L/F}(\tilde{\sigma})$ does not depend on the choice of $\tilde{\sigma}$ for $\sigma \in \mathrm{Gal}(L/F)$. It induces an isomorphism $\Upsilon_{L/F} : \mathrm{Gal}(L/F) \to F^*/N_{L/F}L^*$ and

$$\Upsilon_{L/F}(\varphi_F|_L) \equiv \pi_F \mod N_{L/F}L^*$$

for a prime element π_F in F.

Before we begin the proof, we would like to remember that $\tilde{\sigma} \in \mathrm{Gal}(F^{ur}/F)$ denoted the extension of $\sigma \in \mathrm{Gal}(L/F)$ from L to F^{ur} for any unramified extension of F, which therefore is a subextension of the extension F^{ur}/F.

Proof. We saw in the assertion of proposition 2.2.1, that the Galois group $\mathrm{Gal}(F^{ur}/F)$ is generated by the Frobenius element φ_F. Now L/F is an unramified extension and as such a subextension of F^{ur}:

$$F \subset L \subset F^{ur}.$$

We have the following identity for Galois groups:

$$\mathrm{Gal}(F^{ur}/F)/\,\mathrm{Gal}(F^{ur}/L) \simeq \mathrm{Gal}(L/F).$$

From that we obtain that σ must be equal to $\varphi_F^n|_L$ for some $n \geq 1$. Let $m = [L : F]$ be the finite degree of the extension. Then we get $\tilde{\sigma} = \varphi_F^d$ with $d = n + lm > 0$ for some integer l. This can be seen very easily by simply restricting $\tilde{\sigma}$ to L. The last term

will be the identity as we have $m = [L : F]$ and therefore $m = |\operatorname{Gal}(L/F)|$ by the main theorem of Galois theory.
We know that the fixed field Σ of $\tilde{\sigma}$ is a finite extension of F by propositon 2.3.2. Since L/F was unramified in this case, Σ is the unramified extension of F of degree d. This unramified exention of degree d is unique by proposition 2.2.1. By what we had so far, we can take π_F as a prime element of Σ.
Then

$$\tilde{\Upsilon}_{L/F}(\tilde{\sigma}) = N_{\Sigma/F}\pi_F = \pi_F^d = \pi_F^n \cdot \pi_F^{lm} \equiv \pi_F^n \mod N_{L/F}L^*, \tag{2.4}$$

since $\pi_F^m = N_{L/F}\pi_F$ by basic norm properties for finite extensions and π_F^m is clearly in $N_{L/F}L^*$.

From the multiplicativity of the norm it can easily be seen that $\tilde{\Upsilon}$ is a homomorphism. The composite of $\tilde{\sigma_1}$ and $\tilde{\sigma_2}$ has a fixed field Σ_{12}, which must be a subfield of Σ_1 and Σ_2, hence a finite extension of F. Let $\pi_{\Sigma_{12}}$ be the respective prime element. Since this extension is again unramified, we can take $\pi_{\Sigma_{12}}$ to be π_F. It is now also clear that $\tilde{\Upsilon}$ must send φ_F to $\pi_F \mod N_{L/F}L^*$.

Our discussion on page 40 shows that $\pi_F \mod N_{L/F}L^*$ generates the group $F^*/N_{L/F}L^*$ which is cyclic of order $[L : F]$. Hence it can now easily be seen that $\Upsilon_{L/F}$ is an isomorphism.

□

To close this section we will give three more commutative diagrams that will be very helpful in the proof of the local reciprocity law.

Lemma 2.3.6. *Let L/F be a finite separable extension and let L/M be a finite Galois extension, $\sigma \in \operatorname{Gal}(F^{sep}/F)$. Let us define $\sigma^*(\tilde{\tau}) = \sigma\tilde{\tau}\sigma^{-1}|_{\sigma L^{ur}}$ for $\tilde{\tau} \in \operatorname{Frob}(L/M)$. Then the diagram of maps*

$$\begin{tikzcd}
Frob(L/M) \arrow[r, "\tilde{\Upsilon}_{L/M}"] \arrow[d, "\sigma^*"'] & M^*/N_{L/M}L^* \arrow[d, "\sigma"] \\
Frob(\sigma L/\sigma M) \arrow[r, "\tilde{\Upsilon}_{\sigma L/\sigma M}"] & (\sigma M)^*/N_{\sigma L/\sigma M}(\sigma L^*)
\end{tikzcd}$$

is commutative.

Proof. If Σ is the fixed field of $\tilde{\tau}$ then $\sigma\Sigma$ is the fixed field of $\sigma\tilde{\tau}\sigma^{-1}$. It is obvious that $\sigma\Sigma$ is contained in the fixed field of $\sigma\tilde{\tau}\sigma^{-1}$. Conversely, any other field L containing $\sigma\Sigma$, but $L \supset \sigma\Sigma$ is a proper inclusion, cannot be fixed by $\sigma\tilde{\tau}\sigma^{-1}$. That is, because then $\sigma^{-1}L$ is a proper supset of Σ. Hence, there is some $\alpha \in \sigma^{-1}L$ for which we have $\tilde{\tau}(\alpha) \neq \alpha$.
For a prime element π in Σ, $\sigma\pi$ is prime in $\sigma\Sigma$. This can be easily verified using corollary 1.4.15. We have $N_{\sigma\Sigma/\sigma M} = \sigma N_{\Sigma/M}\pi$. This can be seen using the fact that σ is an automorphism and considering the way we calculated the norm. We can now prove the commutativity.

First, using the maps $\tilde{\Upsilon}$ and σ, we obtain:

$$\sigma(\tilde{\Upsilon}_{L/M}(\tilde{\tau})) = \sigma(N_{\Sigma/M}\pi).$$

Second, using the maps σ^* and $\tilde{\Upsilon}_{\sigma L/\sigma M}$ we get

$$\tilde{\Upsilon}_{\sigma L/\sigma M}(\sigma^*) = \tilde{\Upsilon}_{\sigma L/\sigma M}(\sigma\tilde{\tau}\sigma^{-1}|_{\sigma L^{ur}}) = N_{\sigma\Sigma/\sigma M}(\sigma\pi)$$

because $\sigma\pi$ was a prime element of $\sigma\Sigma$, the fixed field of $\sigma^* = \sigma\tilde{\tau}\sigma^{-1}|_{\sigma L^{ur}}$. □

In the next proposition we have two extensions of F and will therefore obtain a more general commutativity.

Proposition 2.3.7. *Let M/F and E/L be finite separable extensions, and let L/F and E/M be finite Galois extensions. Then the diagram of maps*

$$\begin{tikzcd}
\mathit{Frob}(E/M) \arrow[r, "\tilde{\Upsilon}_{E/M}"] \arrow[d] & M^*/N_{E/M}E^* \arrow[d, "N^*_{M/F}"] \\
\mathit{Frob}(L/F) \arrow[r, "\tilde{\Upsilon}_{L/F}"] & F^*/N_{L/F}(L^*)
\end{tikzcd}$$

is commutative. Here the left vertical homomorphism is the restriction $\sigma|_L^{ur}$ of $\sigma \in$ Frob(E/M) and the right vertical homomorphism is induced by the norm map $N_{M/F}$. The left vertical map is surjective if $M = F$.

To get a better idea of with what kind of extensions we are dealing here, we give a little diagram:

$$\begin{tikzcd}
F \arrow[r, dash, "\text{finite, Galois}"] \arrow[d, dash, "\text{finite}"] & L \arrow[d, dash, "\text{finite}"] \\
\text{M} \arrow[r, dash, "\text{finite, Galois}"] & \text{E}
\end{tikzcd}$$

Proof. We see that $\tilde{\sigma} \in \text{Frob}(E/M) \subset \text{Gal}(E^{ur}/M)$. So for $\tilde{\sigma}|_{L^{ur}} \in \text{Gal}(L^{ur}/F)$ we deduce that $\tilde{\tau}|_{F^{ur}}$ is a positive integer power of φ_F, since $\tilde{\sigma}$ is a positive interger power of φ_M. Hence, $\tilde{\tau} \in \text{Frob}(L/F)$.
Let Σ be the fixed field of $\tilde{\sigma}$. Then $T = \Sigma \cap L^{ur}$ is the fixed field of $\tilde{\tau}$. This can be seen, since the given field must be contained in the fixed field of $\tilde{\tau}$, but it also cannot be bigger for obvious reasons.
The extension Σ/T is totally ramified, since $L^{ur} = T^{ur}$ because we see that L^{ur} is an unramified extension of T, but no unramified extension of it can be bigger than L^{ur}. So $T = \Sigma \cap T^{ur}$. Hence for a prime element π_Σ in Σ the element $\pi_T = N_{\Sigma/T}\pi_\Sigma$ is prime

in T. This is again a simple result from considering how we extend valuations to finite extensions and that totally ramified means nothing less than $f = f(\Sigma/T) = 1$. We get

$$N_{T/F}\pi_T = N_{\Sigma/F}\pi_\Sigma = N_{M/F}(N_{\Sigma/M}\pi_\Sigma).$$

Finally, if $M = F$, then the left vertical map is surjective, since every extension of $\tilde{\sigma} \in \mathrm{Frob}(L/F)$ to $\mathrm{Gal}(E^{ur}/F)$ belongs to $\mathrm{Frob}(E/F)$.

□

We now state the last corollary of this section, which gives us another commutative diagram.

Corollary 2.3.8. *Let M/F be a Galois subextension in a finite Galois extension L/F. Then the diagram of maps*

$$\begin{tikzcd}
\mathrm{Frob}(L/M) \arrow[r] \arrow[d, "\tilde{\Upsilon}_{L/M}"] & \mathrm{Frob}(L/F) \arrow[r] \arrow[d, "\tilde{\Upsilon}_{L/F}"] & \mathrm{Frob}(M/F) \arrow[d, "\tilde{\Upsilon}_{M/F}"] & \\
M^*/N_{L/M}L^* \arrow[r, "N^*_{M/F}"] & F^*/N_{L/F}L^* \arrow[r] & F^*/N_{M/F}M^* \arrow[r] & 1
\end{tikzcd}$$

is commutative. Here the central homomorphism of the lower exact sequence is induced by the identity map of F^*.

Proof. This is an easy consequence from the preceding proposition. For the left commutative diagram we use $E = L$ and for the right one $M = F$. □

2.4 The Hazewinkel Homomorphism

In this section we will define and describe the Hazewinkel homomorphism. This homomorphism works the opposite way from the Neukirch map. Combining those two we will obtain a nice description of the local reciprocity law.

Before we can proceed defining the Hazewinkel homomorphism we need some preliminary work.

It can be seen that the maximal unramified extension F^{ur} of F is a Henselian discrete valuation field with algebraically closed residue field and its completion is a local field with algebraically closed residue field.

However, for our aim, proving the local reciprocity law, the complete case is sufficient. We will therefore denote this completion of F^{ur} by $\mathcal{F}$.

First we state a lemma that is a corollary of Hensel's lemma 1.3.11.

Corollary 2.4.1. *Let F be a complete discrete valuation field. Let $f(x)$ be a monic polynomial with coefficients in $\mathcal{O}$. Let $f(\alpha_0) \in \mathcal{M}^{2s+1}$, $f'(\alpha_0) \notin \mathcal{M}^{s+1}$ for some $\alpha_0 \in \mathcal{O}$ and integer $s \geq 0$. Then there exists $\alpha \in \mathcal{O}$ that $\alpha - \alpha_0 \in \mathcal{M}^{s+1}$ and $f(\alpha) = 0$.*

Let now $\mathcal{L}$ be a finite separable extension of $\mathcal{F}$. Every separable extension is of course algebraic. Since the residue field of $\mathcal{F}$ is algebraically closed, the extension $\mathcal{L}/\mathcal{F}$ can only be totally ramified.

Lemma 2.4.2. *The norm maps*

$$N_{\mathcal{L}/\mathcal{F}} : \mathcal{L}^* \to \mathcal{F}^*, \quad N_{\mathcal{L}/\mathcal{F}} : \mathcal{U}_{\mathcal{L}} \to \mathcal{U}_{\mathcal{F}}$$

are surjective.

Proof. The Galois group $\text{Gal}(\mathcal{L}/\mathcal{F})$ is soluble by lemma 1.5.23. It follows from group theory, that it is sufficient to consider the case of a Galois extension of prime degree. Such extensions cannot have any proper subextensions. But since the Galois group must be soluble, this means we are dealing with an abelian extension. Let l denote the degree of the abelian extension.
Now $\mathcal{L}$ is a finite, hence algebraic, extension of $\mathcal{F}$. We know that the norm of a prime element of $\mathcal{L}$ is a prime element of $\mathcal{F}$. The extension $\mathcal{L}/\mathcal{F}$ is totally ramified, hence the ramification index $f = f(\mathcal{L}/\mathcal{F}) = 1$. Therefore we have

$$w(\alpha) = \frac{1}{f} v \circ N_{\mathcal{L}/\mathcal{F}}(\alpha) = v \circ N_{\mathcal{L}/\mathcal{F}}(\alpha) \quad \text{for } \alpha \in \mathcal{L}.$$

Let us now regard a prime element $\pi_{\mathcal{L}}$ of $\mathcal{L}$. Then $w(\pi_{\mathcal{L}}) = 1$, hence

$$1 = v \circ N_{\mathcal{L}/\mathcal{F}}(\pi_{\mathcal{L}}) = v\left(N_{\mathcal{L}/\mathcal{F}}(\pi_{\mathcal{L}})\right)$$

which declares $N_{\mathcal{L}/\mathcal{F}}(\pi_{\mathcal{L}})$ to be a prime element of $\mathcal{F}$.
Now, as we stated above, $\mathcal{F}$ is complete. Hence we can apply the results from the previous section about the norm map and the commutativity diagrams and deduce the maps surjectivity. □

We now state, but do not prove, a proposition that we will need to show that the Hazewinkel homomorphism that we define later is similar to of the inverse of the Neukirch map.

Definition 2.4.3. For a finite Galois extension $\mathcal{L}/\mathcal{F}$ we denote by $U(\mathcal{L}/\mathcal{F})$ the subgroup of $U_{1,L}$ generated by $u^{\sigma-1}$ where u runs through all elements of $U_{1,L}$ and σ runs through all element of $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$.

Proposition 2.4.4. *Let $\gamma \in \mathcal{L}^*$ be such that $\gamma^{\varphi-1} \in U(\mathcal{L}/\mathcal{F})$. Then $N_{\mathcal{L}/\mathcal{F}}\gamma$ belongs to the group $N_{L/F}L^*$.*

The proof of the above lemma is quite technical and will be omitted since it depends on much more technical preliminary work.

Let L be a finite Galois totally ramified extension of F. As we denoted at the beginning of this section, let $\mathcal{F}$ be the completion of the maximal unramified extension F^{ur} of F. We saw, that the extension $\mathcal{L}/\mathcal{F}$ must be totally ramified. It can be shown, that the Galois group $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$ of the extension $\mathcal{L}/\mathcal{F}$ is isomorphic to $\mathrm{Gal}(L/F)$.

Before proceeding to defining the Hazewinkel homomorphism we need another proposition. But first a new group theoretic definition.

Definition 2.4.5. For a group F the notation G^{ab} stands for the maximal abelian quotient of G and is called *Verlagerung*.

At this point, we will define a notation, which is commonly used in algebraic books. At first it seems a bit odd, but when explained, it is quite natural[2].

Definition 2.4.6. We will denote $\sigma(u)$ by u^σ. As for usual powers of u, the rule $u^{a+b} = u^a \cdot u^b$ for any $u \in F$ with F any field, applies. We can naturally extend this definition to for example $u^{\sigma-1} = u^\sigma \cdot u^{-1} = \sigma(u) \cdot u^{-1}$ as it will be used in the rest of the section.

Every unit in $U_\mathcal{L}$ can be factorized as $\theta\epsilon$ with $\theta \in R^*$, $\epsilon \in U_{1,\mathcal{L}}$, where R^* is the set of multiplicative representatives of the residue field of F. Since by our notation from above we have $\theta^{\sigma-1} = 1$ because $\theta \in \mathcal{F}$ is fixed by σ, we deduce that $U(\mathcal{L}/\mathcal{F})$ coincides with the subgroup of $U_\mathcal{L}$ generated by $u^{\sigma-1}$, $u \in U_\mathcal{L}$, $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$.

Proposition 2.4.7. *Let $\mathcal{L}$ be a finite Galois extension of F. For a prime element π of $\mathcal{L}$ define*

$$\ell : \mathrm{Gal}(\mathcal{L}/\mathcal{F}) \to U_\mathcal{L}/U(\mathcal{L}/\mathcal{F}), \quad l(\sigma) = \pi^{\sigma-1} \mod U(\mathcal{L}/\mathcal{F}).$$

The map ℓ is a homomorphism which does not depend on the choice of π. It induces a monomorphism $\ell : \mathrm{Gal}(\mathcal{L}/\mathcal{F}) \to U_\mathcal{L}/U(\mathcal{L}/\mathcal{F})$.
The sequence

$$1 \to \mathrm{Gal}(\mathcal{L}/\mathcal{F})^{ab} \xrightarrow{l} U_\mathcal{L}/U(\mathcal{L}/\mathcal{F}) \xrightarrow{N_{\mathcal{L}/\mathcal{F}}} U_\mathcal{F} \to 1$$

is exact.

[2] For the general notation please see the appendix at A.1.21.

We can now proceed defining the Hazewinkel homomorphism.

Let φ be the continuous extension of the Frobenius automorphism φ_L on $\mathcal{L}$. Let π be a prime element of $\mathcal{L}$. Let E be the maximal abelian extension of F in L. For $\alpha \in \mathcal{F}^*$ by lemma 2.4.2 there is $\beta \in \mathcal{L}^*$ such that $\alpha = N_{\mathcal{L}/\mathcal{F}}\beta$. Since $F^* \subset \mathcal{F}$ we can also find such a β for $\alpha \in F^*$.
Then $N_{\mathcal{L}/\mathcal{F}}\beta^{\varphi-1} = \alpha^{\varphi-1} = 1$ and by proposition 2.4.7

$$\beta^{\varphi-1} \equiv \pi^{1-\sigma} \mod U(\mathcal{L}/\mathcal{F})$$

for some $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$ which is uniquely determined as an element of $\mathrm{Gal}(\mathcal{E}/\mathcal{F})$ where $\mathcal{E} = E\mathcal{F}$.

To make the situation we are dealing with a little clearer, we give a diagram:

$$\begin{tikzcd}
F \arrow[r, dash] \arrow[d, dash, "\text{maximal abelian}"'] & \mathcal{F} \arrow[d, dash] \\
E \arrow[r, dash] \arrow[d, dash] & \mathcal{E} \arrow[d, dash] \\
\mathrm{L} \arrow[r, dash] & \mathcal{L}
\end{tikzcd}$$

Definition 2.4.8. Define the *Hazewinkel homomorphism*

$$\Psi_{L/F} : F^*/N_{L/F}L^* \to \mathrm{Gal}(L/F)^{ab}, \ \ \alpha \mapsto \sigma|_E.$$

We will now see that the map defined above is really well defined and a homomorphism.

Lemma 2.4.9. *The map $\Psi_{L/F}$ is well defined and is a homomorphism.*

Proof. We proceed by proving first that the map is well defined and second that it is a homomorphism.

Well-defined First, for it to be well defined we need to prove the independence of it on the choice of π. But this is just the assertion of propostion 2.4.7 since such a β exists and we use the map ℓ. For this map the independence of of the choice of π is part of the assertion. So we assume $\pi \in L$. This can be done since L of course has prime elements and $\mathcal{L}$ is nothing else than the completion of the maximal unramified extension. But earlier we had that for unramified extensions L/F a prime element of F is also one of L and vice-a-versa.
If $\alpha = N_{\mathcal{L}/\mathcal{F}}\gamma$ then $\gamma\beta^{-1}$ belongs to the kernel of $N_{\mathcal{L}/\mathcal{F}}$. This is really obvious since we had $\alpha = N_{\mathcal{L}/\mathcal{F}}\beta$. Therefore, again by proposition 2.4.7 $\gamma\beta^{-1} = \pi^{\tau-1}\zeta$ with $\zeta \in U(\mathcal{L}/\mathcal{F})$. Then

$$\gamma^{\varphi-1} = \beta^{\varphi-1}\zeta^{\varphi-1} \equiv \beta^{\varphi-1} \mod U(\mathcal{L}/\mathcal{F})$$

which proves the correctness of the definition.

Homomorphism If we have $N_{\mathcal{L}/\mathcal{F}}(\beta_1) = \alpha_1$ and $N_{\mathcal{L}/\mathcal{F}}(\beta_2) = \alpha_2$, we can choose $\beta_1\beta_2$ for $\alpha_1\alpha_2$. Therefore, again by proposition 2.4.7 we see that $\Psi_{L/F}$ really is a homomorphism, since ℓ is one. □

We are dealing with a totally ramified extension L/F. For such extensions we know, that the norm of a prime element π_L in L is a prime element in F. Remember that for unramified extensions prime elements of L were also prime elements of F. This can be seen easily considering the way we extend valuations and that totally ramified means $f = 1$. Hence,

$$F^*/N_{L/F}L^* = U_F/N_{L/F}U_L$$

as by definition $v(\pi_F)$ generates the group $v(F^*)$ and we again use the unique representation of an arbitrary element $\alpha = \epsilon\pi^i$ for $\epsilon \in U$ and π a prime element.

We will now prove, that the Hazewinkel homomorphism $\Psi_{L/F}$ is the inverse to $\Upsilon^{ab}_{L/F}$, which is induced by the Neukirch homomorphism.

This theorem is a first step to the local reciprocity law. It asserts the law in the case of a totally ramified extension.

Theorem 2.4.10. *Let L/F be a finite Galois totally ramified extension. Let E/F be the maximal abelian subextension of L/F. Then*

1. *For every $\tilde{\sigma} \in \operatorname{Frob}(L/F)$*

$$\Psi_{L/F}(\tilde{\Upsilon}_{L/F}(\tilde{\sigma})) = \tilde{\sigma}|_E.$$

2. *Let $\alpha \in F^*$ and let $\tilde{\sigma} \in \operatorname{Frob}(L/F)$ be such that $\tilde{\sigma}|_E = \Psi_{L/F}(\alpha)$. Then*

$$\tilde{\Upsilon}_{L/F}(\tilde{\sigma}) \equiv \alpha \mod N_{L/F}L^*.$$

Therefore, $\Psi_{L/F}$ is an isomorphism, $\tilde{\Upsilon}_{L/F}(\tilde{\sigma})$ does not depend on the choice of $\tilde{\sigma}$ for $\sigma \in \operatorname{Gal}(L/F)$ and induces the Neukirch homomorphism

$$\Upsilon_{L/F} : \operatorname{Gal}(L/F) \to F^*/N_{L/F}F^*.$$

The latter induces an isomorphism $\Upsilon^{ab}_{L/F}$, between $\operatorname{Gal}(L/F)^{ab} = \operatorname{Gal}(E/F)$ and $F^*/N_{L/F}L^*$ which is inverse to $\Psi_{L/F}$.

Proof. First we prove the assertions one and two.

(1) We will proceed as follows: We will start at an element $\tilde{\sigma}$. Then we use some very helpful representations of $\tilde{\tilde{\Upsilon}}(\sigma)$ to get a better representation that we can apply the Hazewinkel homomorphism on. Finally we will see that those maps really work in some sense in opposite directions.
We first note that the Galois group $\operatorname{Gal}(L^{ur}/F)$ of L^{ur}/F is isomorphic to $\operatorname{Gal}(L^{ur}/L) \times \operatorname{Gal}(L^{ur}/F^{ur})$. Hence $\tilde{\sigma} \in \operatorname{Frob}(L/F) \subset \operatorname{Gal}(L^{ur}/F)$ is equal to $\sigma\varphi^m$ for some positive

integer m and $\sigma \in \mathrm{Gal}(L^{ur}/F^{ur})$. φ is again the continuous extension of the Frobenius element φ_L of $\mathrm{Gal}(L^{ur}/L)$.
Let π_Σ be a prime element of the fixed field Σ of $\tilde{\sigma}$. We saw in equation 2.3 that $\Sigma^{ur} = L^{ur}$. Now if π_Σ is a prime element of Σ, we have $\pi_\Sigma = \pi\epsilon$ for some $\epsilon \in U_{L^{ur}}$, where π is a prime element of L. Therefore

$$\pi^{1-\tilde{\sigma}} = \pi_\Sigma \cdot \epsilon^{-1} \cdot \tilde{\sigma}(\pi_\Sigma \epsilon^{-1})^{-1} = \epsilon^{-1} \cdot \tilde{\sigma}(\epsilon^{-1})^{-1} =$$

$$= \tilde{\sigma}(\epsilon) \cdot \epsilon^{-1} = \epsilon^{\tilde{\sigma}-1} = \epsilon^{\sigma\varphi^m - 1}$$

Let $\Sigma_0 = \Sigma \cap F^{ur}$, then $[\Sigma_0 : F] = m$ by the general main theorem of Galois theory and the fact that φ generates the group $\mathrm{Gal}(L^{ur}/L)$ by proposition 2.2.1. Then of course $N_{\Sigma/F} = N_{\Sigma_0/F} \circ N_{\Sigma/\Sigma_0}$ and N_{Σ/Σ_0} acts as $N_{\Sigma^{ur}/\Sigma_0^{ur}}$. The first equivalence can again be deduced easily observing that we extend valuations as

$$w = \frac{1}{f} v \circ N_{\Sigma/\Sigma_0}.$$

Now Σ is clearly an extension of Σ_0 and Σ^{ur} one of Σ_0^{ur}. We now have

$$\begin{tikzcd}
\Sigma_0 \arrow[r, dash] \arrow[d, dash] & \Sigma \arrow[d, dash] \\
\Sigma_0^{ur} \arrow[r, dash] & \Sigma^{ur}
\end{tikzcd}$$

We can now extend our valuation on Σ_0 to Σ^{ur} in both ways which of course MUST lead to the same result. Therefore and by the way we construct that extention, the norm maps must act the same.
Further

$$N_{\Sigma^{ur}/\Sigma_0^{ur}} = N_{L^{ur}/F^{ur}} = N_{\mathcal{L}/\mathcal{F}}$$

which can be deduced by equation 2.3 and by the definition of Σ_0. The last equality is simple since $\mathcal{L}$ is just the completion of L^{ur}. It can be seen that $N_{\Sigma_0/F}$ acts as $1 + \varphi + \cdots + \varphi^{m-1}$. We have

$$N_{\Sigma/F}\pi_\Sigma = N_{L^{ur}/F^{ur}}\epsilon_1 \cdot N_{L^{ur}/F^{ur}}\pi^m, \qquad \text{where} \quad \epsilon_1 = \epsilon^{1+\varphi+\cdots+\varphi^{m-1}}$$

by the same representation of $\pi_\Sigma = \pi\epsilon$.
So $\alpha = N_{\Sigma/F}\pi_\Sigma \equiv N_{L^{ur}/F^{ur}}\epsilon_1 \mod N_{L/F}L^*$ since π was a prime element of L. Further, $\Psi_{L/F}(\alpha)$ can be calculated by looking at $\epsilon_1^{\varphi-1}$. We deduce

$$\epsilon_1^{\varphi-1} = \epsilon^{\varphi^m-1} \equiv \epsilon^{\sigma\varphi^m-1} = \pi^{1-\tilde{\sigma}} \mod U(\mathcal{L}/\mathcal{F}).$$

This completes the proof of step one.

(2) We now proceed showing assertion two. This part is proven quite similiar to part one. Therefore we will not go very deep into detail as it just uses the same techniques as part one. Let $\alpha = N_{\mathcal{L}/\mathcal{F}}$ and $\beta^{\varphi-1} = \pi^{1-\sigma} \mod U(\mathcal{L}/\mathcal{F})$ with $\sigma \in \mathrm{Gal}(L/F)$. Then again, as shown above, $\tilde{\sigma} = \sigma\varphi^m$ and similarly to the previous

$$\tilde{\Upsilon}_{L/F}(\tilde{\sigma}) = N_{\Sigma/F}\pi_\Sigma \equiv N_{L^{ur}/F^{ur}}\epsilon_1 \mod N_{L/F}L^*$$

and

$$\epsilon_1^{\varphi-1} \equiv \pi^{1-\sigma} \equiv \beta^{\varphi-1} \mod U(\mathcal{L}/\mathcal{F}).$$

From proposition 2.4.4 applied to $\gamma = \epsilon_1\beta^{-1}$ we deduce that $N_{\mathcal{L}/\mathcal{F}}\gamma$ belongs to $N_{L/F}L^*$ and therefore

$$N_{\mathcal{L}/\mathcal{F}}\epsilon_1 \equiv N_{\mathcal{L}/\mathcal{F}}\beta = \alpha \mod N_{L/F}L^*.$$

But this proves assertion two.

We will now explain, why those assertions justify seeing the Hazewinkel homomorphism partly as the inverse of the Neukirch map. This argument is also a very important one for the proof of the local reciprocity law.

From assertion one we can deduce the surjectivity of $\Upsilon_{L/F}$. From assertion two and the fact that we have $\tilde{\Upsilon}(\tilde{\sigma}) = 1$ if $\tilde{\sigma}|_L = id|_L$, by taking $\tilde{\sigma} = \varphi$, so that $\tilde{\sigma}|_E = id_E = \Upsilon_{L/F}(\alpha)$ we deduce that $\alpha \in N_{L/F}L^*$. But that means that $\Psi_{L/F}$ is injective. Hence, $\Psi_{L/F}$ is an isomorphism. Now from assertion one we conclude that $\tilde{\Upsilon}$ does not depend on the choice of a lifting of $\tilde{\sigma} \in \mathrm{Gal}(L/F)$ and therefore determines the map $\Upsilon_{L/F}$.
It remains to show that the Hazewinkel homomorphism really is a homomorphism in the case of a totally ramified extension. Since we can take $\widetilde{\sigma_1\sigma_2} = \tilde{\sigma_1}\tilde{\sigma_2}$ we can deduce from assertion one that $\Upsilon_{L/F}$ is a homomorphism. Due to proposition 2.3.2 and assertion two we see that this homomorphism must be surjective. From assertion one we deduce that its kernel is contained in $\mathrm{Gal}(L/E)$. The latter conincides with the kernel, since the image of $\Upsilon_{L/F}$ is abelian. Remember that E was the maximal abelian extension. We therefore know, that $\mathrm{Gal}(L/E)$ must be the smallest abelian subgroup. The image of the Neukirch map is clearly abelian as it is a quotient *field* of F^*.

□

We will now give a corollary for the case of $\mathcal{F}$ again being the completion of the maximal unramified extension of F.

Corollary 2.4.11. *Let $\mathcal{F}$ be the completion of the maximal unramified extension of F, and let $\mathcal{L} = L\mathcal{F}$.*
For $\sigma \in \mathrm{Gal}(L/F)$ there exists $\eta \in \mathcal{L}^*$ such that

$$\eta^{\varphi-1} = \pi^{1-\sigma}.$$

Then $\epsilon = N_{\mathcal{L}/\mathcal{F}}\eta$ beglongs to F^* and

$$\Upsilon_{L/F}(\sigma) = N_{\mathcal{L}/\mathcal{F}}\eta.$$

Conversely, for every $\epsilon \in F^*$ there exists $\eta \in \mathcal{L}^*$ such that

$$\epsilon \equiv N_{\mathcal{L}/\mathcal{F}}\eta \mod N_{L/F}L^*$$

$$\eta^{\varphi-1} = \pi^{1-\sigma} \qquad \text{for some } \sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F}).$$

Then $\Psi_{L/F}(\epsilon) = \sigma|_E$.

The proof of this corollary needs no further technical details then the one above. But since it is quite long itself, and technical as the one above, it will be omitted.

2.5 The Local Reciprocity Law

In this section we will state and prove the local reciprocity law.

First, we need a very useful lemma, that allows use to see the finite Galois extension we will have in the local reciprocity law as a composition of an unramified one and a Galois totally ramified one.

Lemma 2.5.1. *Let L/F be a finite abelian extension. Then there is a finite unramified extension M/L such that M is an abelian extension of F, M is the compositum of an unramified extension M_0 of F and an abelian totally ramified extension K of F.*
For every such M we have $N_{M/F}M^* = N_{K/F}K^* \cap N_{M_0/F}M_0^*$.

Proof. We know from the previous sections, that $\mathrm{Gal}(L^{ur}/L)$ is topologically generated by an element φ_L, hence abelian. Now, L/F is a finite abelian extension, hence $L^{ur} = LF^{ur}$ is one of F, since a finite extension is always algebraic and therefore proposition 1.5.19 applies. Let $\tilde{\varphi} \in \mathrm{Gal}(LF^{ur}/F)$ be an extension of φ_F. Let K be the fixed field of $\tilde{\varphi}$. Then we must have $K \cap F^{ur} = F$, since φ_F generates $\mathrm{Gal}(F^{ur}/F)$, hence K is a totally ramified extension of F. It is also abelian as a subextension of an abelian extension, and subgroups of abelian groups are always abelian.
The compositum M of K and L is an unramified extension of L, since $K^{ur} = L^{ur}$. This can be seen since K must be a subfield of $LF^{ur} = L^{ur}$. The field M, as a compositum of two abelian extensions, is an abelian extension of F and $\mathrm{Gal}(M/F) \simeq \mathrm{Gal}(M/K) \times \mathrm{Gal}(M/M_0)$. This proves the first assertion.

We now proceed proving the part about norms, since we will also need that in the following proof of the local reciprocity law.
Now the left hand side of the formula of the lemma is contained in the right hand side, which we will denote by $\mathcal{N}$. We have $\mathcal{N} \cap U_F \subset N_{K/F}U_K \subset N_{M/F}U_M$, since $U_K \subset N_{M/K}U_M$ can be deduced by investigating more technical properties about the norm map. We will, however, not proof that. See [FeVo2, Chpt 3] for a proof of it.
If π_M is a prime element of M, then $N_{M/F}\pi_M \in \mathcal{N}$. By knowing that M_0 is an unramified extension, we can see that we must have

$$v_F(N_{M/F}\pi_M)\mathbb{Z} = v_F(N_{M_0/F}M_0^*).$$

This is an easy consequence of the way we extend valuations, the same argument we used many times before. So every $\alpha \in \mathcal{N}$ can be written as $\alpha = N_{M/F}\pi_M^m \epsilon$ with $\epsilon \in \mathcal{N} \cap U_F$ and some m. Thence $\mathcal{N}$ is contained in $N_{M/F}M^*$ and we have $\mathcal{N} = N_{M/F}M^*$.

□

We can now proceed stating and proving the local reciprocity law. The proof is quite long, but since we provided very useful lemmas that we can use, it is suprisingly clearly structured. It is, in fact, mostly applying the previous lemmas and propositions in the right order on the right objects and not using any further constructions.

Theorem 2.5.2 (Local Reciprocity Law)**.** *Let L/F be a finite Galois extension. Let E/F be the maximal abelian subextension of L/F.*

Then $\Psi_{L/F}$ is an isomorphism, $\tilde{\Upsilon}_{L/F}(\tilde{\sigma})$ does not depend on the choice of $\tilde{\sigma}$ for $\sigma \in$ $\mathrm{Gal}(L/F)$ and induces the Neukirch homomorphism

$$\Upsilon_{L/F} : \mathrm{Gal}(L/F) \to F^*/N_{L/F}L^*.$$

The latter induces an isomorphism $\Upsilon^{ab}_{L/F}$ between $\mathrm{Gal}(L/F)^{ab} = \mathrm{Gal}(E/F)$ and $F^*/N_{L/F}L^*$ (which is inverse to $\Psi_{L/F}$ for totally ramified extensions).

Proof. First, we consider the case of an abelian extension L/F, such that L is the compositum of the maximal unramified extension L_0 of F in L and an abelian totally ramified extension K of F. Then by the previous lemma $N_{L/F}L^* = N_{K/F}K^* \cap N_{L_0/F}L_0^*$. From proposition 2.3.7 applied to the surjective maps

$$\mathrm{Frob}(L/F) \to \mathrm{Frob}(L_0/F) \quad \text{and} \quad \mathrm{Frob}(L/F) \to \mathrm{Frob}(K/F),$$

and from what we had on the Neukirch map and the Hazewinkel homomorphism so far (theorems 2.3.5 resp. 2.4.10) we deduce that $\tilde{\Upsilon}_{L/F}$ does not depend on the choice of $\tilde{\sigma}$ modulo $N_{K/F}K^* \cap N_{L_0/F}L_0^*$, therefore modulo $N_{L/F}L^*$. So we get the map $\Upsilon_{L/F}$. Now from what we had in the previous sections we deduce that $\Upsilon_{L/F}$ is a homomorphism modulo $N_{K/F}K^* \cap N_{L_0/F}L_0^*$, so it is a homomorphism modulo $N_{L/F}L^*$. It is injective, since if $\Upsilon_{L/F}(\sigma) \in N_{L/F}L^*$, then σ acts trivially on L_0 and K, and hence on L. Its surjectivitiy follows from the commutative diagram of corollary 2.3.8.

Second, we consider the case of an arbitrary finite abelian extension L/F. By the previous lemma and the preceding arguments there is an unramified extension M/L such that the map $\tilde{\Upsilon}_{M/F}$ induces the isomorphism $\Upsilon_{M/F}$. The map $\mathrm{Frob}(M/F) \to \mathrm{Frob}(L/F)$ is surjective by the assertion of proposition 2.3.7. We deduce using proposition 2.3.7 again that $\tilde{\Upsilon}_{L/F}$ induces the well defined map $\Upsilon_{L/F}$, which is a surjective homomorphism. Let $\sigma \in \mathrm{Gal}(M/F)$ be such that $\Upsilon_{L/F}(\sigma) = 1$. Then we apply the commuative diagram of corollary 2.3.8 to the extensions M/F and L/F, where $M \supset L \supset F$. We already saw that $\tilde{\Upsilon}_{M/F}$ induces the isomorphism $\Upsilon_{M/F}$. Then from the above mentioned diagram and the surjectivity of Υ for every finite abelian extension we deduce that we can find $\tau \in \mathrm{Gal}(M/L) \subset \mathrm{Gal}(M/F)$, such that $\Upsilon_{M/F}(\sigma) = \Upsilon_{M/F}(\tau)$. The injectivity of $\Upsilon_{M/F}$ now implies that $\sigma = \tau$. Hence, τ also acts trivially on L.

Finally, we consider the case of a finite Galois extension where we argue by induction on the degree of L/F. We can assume that L/F is not abelian, since in that case our first part of the proof would apply.

Every $\sigma \in \mathrm{Gal}(L/F)$ belongs to the cyclic subgroup of $\mathrm{Gal}(L/F)$ generated by it. As we already saw, $\tilde{\Upsilon}_{L/F}(\tilde{\sigma})$ does not depend on the choice of $\tilde{\sigma}$ and therefore determines the map $\Upsilon_{L/F}$.

Lemma 1.5.23 asserted that the Galois group $\mathrm{Gal}(L/F)$ is soluble. Now every σ belongs to its generated cyclic subgroup, which is of course also abelian. This subgroup must be a proper one, since $\mathrm{Gal}(L/F)$ would be abelian otherwise, thence we could apply the second case. But, being a proper subgroup allows us to use the induction hypothesis. Going up by the degree from n to $n+1$ means nothing else but adding an additional element to the Galois group $\mathrm{Gal}(L/F)$ by the main theorem of Galois theory (A.3.27). We can now find, that for each abelian extension E/F we have $\Upsilon_{E/F}$ is surjective by the second case. Now, L/F is nothing else but the finite composition of those extensions, hence $\Upsilon_{L/F}$ must be surjective.

In the next several paragraphs we shall show that $\Upsilon_{L/F}(\mathrm{Gal}(L/E)) = 1$. Due to surjectivity of Υ this implies that the map $N^*_{E/F}$ in the diagram of corollary 2.3.8 (where we put M=E) is zero. Since $\Upsilon_{E/F}$ is an isomorphism we see from the diagram of the corollary that $\Upsilon_{L/F}$ is a surjective homomoprhism with kernel $\mathrm{Gal}(L/E)$. This will proof the theorem, since $\mathrm{Gal}(L/F)^{ab} = \mathrm{Gal}(E/F)$, hence the canonical map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(L/F)^{ab}$ has kernel $\mathrm{Gal}(L/E)$.

So it remains to prove that $\Upsilon_{L/F}$ maps every element of the derived group $\mathrm{Gal}(L/E)$ to 1. Since $\mathrm{Gal}(L/F)$ is soluble, we have $E \neq F$. Proposition 2.3.7 shows that $\Upsilon_{L/F}(\rho) = N^*_{E/F}(\Upsilon_{L/E}(\rho))$ for every $\rho \in \mathrm{Gal}(L/E)$. Since by the induction assumption $\Upsilon_{L/E}$ is a homomorphism, it suffices to show that

$$\Upsilon_{L/F}(\tau\sigma\tau^{-1}\sigma^{-1}) = N^*_{E/F}(\Upsilon_{L/E}(\tau\sigma\tau^{-1}\sigma^{-1})) = 1$$

for every $\sigma, \tau \in \mathrm{Gal}(L/F)$. (Remember that the derived group of a group G is the set of commutators $aba^{-1}b^{-1}, a, b \in G$ as described in the appendix). We can then use the same argument as in the second case.
To show that, we use lemma 2.3.6 and the induction hypothesis.

Suppose that the subgroup G_1 of $G = \mathrm{Gal}(L/F)$ generated by $\mathrm{Gal}(L/E)$ and τ is not equal to G. We can denote that group by $G_1 = \mathrm{Gal}(L/K)$, since according to the main theorem of Galois theory applied for finite extensions every subgroup of the Galois group $G = (L/F)$ has a corresponding intermediate field K.
So, from the induction hypothesis and lemma 2.3.6

$$\Upsilon_{L/K}(\tau\sigma\tau^{-1}\sigma^{-1}) = \Upsilon_{L/K}(\tau)\Upsilon_{L/K}(\sigma\tau^{-1}\sigma^{-1}) = \Upsilon_{L/K}(\tau)\cdot\sigma^{-1}(\Upsilon_{L/K}(\tau)) = \Upsilon^{1-\sigma}_{L/K}(\tau),$$

and so

$$\Upsilon_{L/F}(\tau\sigma\tau^{-1}\sigma^{-1}) = N^*_{K/F}(\Upsilon_{L/K}(\tau)^{1-\sigma}) = 1$$

by proposition 2.3.7 and hence

$$= N^*_{K/F}(N_{\Sigma/K}(\tau)^{1-\sigma} = N_{\Sigma/K}(\tau)\cdot\sigma(N_{\Sigma/K(\tau)^{-1}}) =$$

$$= N^*_{K/F}(N_{\Sigma/K}(\tau)\cdot N^*_{K/F}(\sigma(N_{\Sigma/K}(\tau)^{-1})) = \alpha\cdot\alpha^{-1} = 1$$

where Σ denots the fixed field of τ and for some $\alpha \in F$. Remember that the norm is the product of all automorphisms from the Galois group, hence it does not matter if we use $N_{K/F}\alpha$ or $N_{K/F}(\sigma(\alpha))$.

In the remaining case the image of τ generates $\mathrm{Gal}(E/F)$. Hence $\sigma = \tau^m\rho$ for some $\rho \in \mathrm{Gal}(L/E)$ and integer m. We deduce $\tau\sigma\tau^{-1}\sigma^{-1} = \tau^m(\tau\rho\tau^{-1}\rho^{-1})\tau^{-m}$ and similarly to the preceding

$$\Upsilon_{L/F}(\tau^m(\tau\rho\tau^{-1}\rho^{-1})\tau^{-m}) = \Upsilon_{L/F}(\tau\rho\tau^{-1}\rho^{-1}) = N^*_{E/F}(\Upsilon_{L/E}(\rho)^{\tau-1}) = 1.$$

□

We will now give a few consequences of the local reciprocity law. The most important one will be the existence theorem 2.6.5.

Corollary 2.5.3. *1. Let L/F be a finite Galois extension and let E/F be the maximal abelian subextension in L/F. Then $N_{L/F}L^* = N_{E/F}E^*$.*

2. Let L/F be a finite abelian extension, and M/F a subextension in L/F. Then $\alpha \in N_{L/M}L^*$ if and only if $N_{M/F}(\alpha) \in N_{M/F}L^*$.

Proof. The first assertion follows immediately from the theorem. The second assertion follows the diagram of corollary 2.3.8 (with Frob being replaced with Gal) in which the homomorphism $N^*_{M/F}$ is injective due to the theorem. □

We now give two more commutative diagrams. However, we will not proof them.

Proposition 2.5.4. *1. Let M/F be a finite separable extension and let L/M be a finite Galois extension, $\sigma \in \mathrm{Gal}(F^{sep}/F)$. Then the diagram*

$$\begin{tikzcd}
\mathrm{Gal}(L/M) \arrow[r, "\Upsilon_{L/M}"] \arrow[d, "\sigma^*"'] & M^*/N_{L/M}L^* \arrow[d, "\sigma"] \\
\mathrm{Gal}(\sigma L/\sigma M) \arrow[r, "\Upsilon_{\sigma L/\sigma M}"] & (\sigma M)^*/N_{\sigma L/\sigma M}(\sigma L)^*
\end{tikzcd}$$

is commuative.

2. Let M/F, E/L be finite separable extensions, and let L/F and E/M be finite Galois extensions. Then the diagram

$$\begin{tikzcd}
\mathrm{Gal}(E/M) \arrow[r, "\Upsilon_{E/M}"] \arrow[d] & M^*/N_{E/M}E^* \arrow[d, "N^*_{M/F}"] \\
\mathrm{Gal}(L/F) \arrow[r, "\Upsilon_{\sigma L/\sigma F}"] & F^*/N_{L/F}L^*
\end{tikzcd}$$

is commutative.

2.6 The Reciprocity Map

To conclude this chapter, we show that we get a good description of the Galois group of a finite abelian extension out from the local reciprocity law. In the center of that description is the so-called reciprocity map. We will use this map to state the existence theorem.

We need the discussion in this section to understand the various generalizations of the reciprocity law. Since the proofs of the following statements would be rather long and premise some more theory we did not develop in the above sections, we will omit them. The main aim of this section is to give a general idea of what we obtain from the local reciprocity law, so we can seek for a generalization of the results we obtained so far.

The homomorphism inverse to the Neukirch map $\Upsilon_{L/F}$ induces the surjective homomorphism

$$(.,L/F): \quad F^* \to \mathrm{Gal}(L/F)^{ab}.$$

If we have a look at the Hazewinkel map, which is a homomorphism in the totally ramified case, we can see that it has similarities to the map define above. Acutally, it coincides with it, if we extend the Hazewinkel homomorphism in a canonical way.

We can now proceed stating a very important propostion.

Proposition 2.6.1. *Let H be a subgroup in $\mathrm{Gal}(L/F)^{ab}$, and let M be the fixed field of H in $L \cap F^{ab}$. Then*

$$(.,L/F)^{-1}(H) = N_{M/F}M^*.$$

Let L_1, L_2 be abelian extensions of finite degree over F, and let $L_3 = L_1L_2, L_4 = L_1 \cap L_2$. Then

$$N_{L_3/F}L_3^* = N_{L_1/F}L_1^* \cap N_{L_2/F}L_2^*,$$

$$N_{L_4/F}L_4^* = N_{L_1/F}L_1^* \ N_{L_2/F}L_2^*.$$

The field L_1 is a subfield of the field L_2 if and only if $N_{L_2/F}L_2^* \subset N_{L_1/F}L_1^*$. In particular, $L_1 = L_2$ if and only if $N_{L_1/F}L_1^* = N_{L_2/F}L_2^*$.
If a subgroup N in F^* contains a norm subgroup $N_{L/F}L^*$ for some finite Galois extension L/F, then N itself is a norm subgroup.

The first assertion of this proposition is an immediate consequence of the local reciprocity law and the commutative diagrams that we obtained from it.

Passing to the projective limit, we get

$$\Psi_F : F^* \to \varprojlim_L F^*/N_{L/F}L^* \to \varprojlim_L \mathrm{Gal}(L/F)^{ab} = \mathrm{Gal}(F^{ab}/F)$$

where L runs through all finite Galois (or all finite abelian) extensions of F.

Definition 2.6.2. The homomorphism Ψ_F from the construction above is called the *reciprocity map.*

With this reciprocity map, we get a bijection that lets us obtain a description of all finite abelian extensions of a local field F. But first we need to make some observations on this map.

Theorem 2.6.3. *The reciprocity map is well defined.*
Its image is dense in $\mathrm{Gal}(F^{ab}/F)$*, and its kernel coincides with the intersection of all norm subgroups* $N_{L/F}L^*$ *in* F^* *for finite Galois (or finite abelian) extensions* L/F.
If L/F *is a finite Galois extension and* $\alpha \in F^*$*, then the automorphism* $\Psi_F(\alpha)$ *acts trivially on* $L \cap F^{ab}$ *if and only if* $\alpha \in N_{L/F}L^*$.
The restriction of $\Psi_F\alpha$ *on* F^{ur} *coincides with* $\varphi_F^{v_F(\alpha)}$ *for* $\alpha \in F^*$.
Let L *be a finite separable extension of* F*, and let* σ *be an automorphism of* $\mathrm{Gal}(F^{sep}/F)$*. Then the diagrams*

$$\begin{tikzcd}
L^* \arrow[r, "\Psi_L"] \arrow[d, "\sigma"'] & \mathrm{Gal}(L^{ab}/L) \arrow[d, "\sigma^*"] \\
(\sigma L)^* \arrow[r, "\Psi_{\sigma L}"] & \mathrm{Gal}((\sigma L)^{ab}/\sigma L)
\end{tikzcd}$$

$$\begin{tikzcd}
L^* \arrow[r, "\Psi_L"] \arrow[d, "N_{L/F}"'] & \mathrm{Gal}(L^{ab}/L) \arrow[d] \\
F^* \arrow[r, "\Psi_F"] & \mathrm{Gal}(F^{ab}/F)
\end{tikzcd}$$

$$\begin{tikzcd}
F^* \arrow[r, "\Psi_F"] \arrow[d] & \mathrm{Gal}(F^{ab}/F) \arrow[d, "Ver"] \\
L^* \arrow[r, "\Psi_F"] & \mathrm{Gal}(L^{ab}/L)
\end{tikzcd}$$

are commutative, where $\sigma^*(\tau) = \sigma\tau\sigma^{-1}$ *as in previous sections, the right vertical homomorphism of the second diagram is the restriction and*

$$Ver : \mathrm{Gal}(F^{sep}/F)^{ab} \to \mathrm{Gal}(F^{sep}/L)^{ab} = \mathrm{Gal}(L^{ab}/L).$$

With the above discussed properties of the reciprocity map, we can now state the existence theorem. In this theorem we exhibit an additional feature of the reciprocity map. One step towards proving the existence theorem is the following observation:

Proposition 2.6.4. *Let* L *be a finite separable extension of* F*. Then the norm map* $N_{L/F} : L^* \to F^*$ *is continous and* $N_{L/F}L^*$ *is an open subgroup of finite index in* F^*.

At this point we would like to remember on the fact that every local field has a natural topology implied by its valuation. The term open subgroup refers to this topology explained in the first chapter.

Theorem 2.6.5 (Existence Theorem)**.** *There is a one-to-one correspondence between open subgroups of finite index in F^* and the norm subgroups of finite abelian extensions:*

$$N \leftrightarrow N_{L/F}L^*.$$

This correspondence is an order reversing bijection between the lattice of open subgroups of finite index in F^* (with respect to the intersection $N_1 \cap N_2$ and the product $N_1 N_2$) and the lattice of finite abelian extensions of F (with respect to the intersection $L_1 \cap L_2$ and the compositum $L_1 L_2$).

From this very important theorem we obtain the following fact about the reciprocity map:

Corollary 2.6.6. *The reciprocity map Ψ_F is injective and continuous.*

This describes the way that this one-to-one correspondence works. So we get a description of the finite abelian extensions of a local field F only by looking at its open subgroups of finite index. So the structure of the abelian extensions of such fields is hidden in the field itself. This is a very strong assertion. Of course, we would like to try generalize this result in some ways. An overview of how this has been done within the last decade is given in the last chapter. The work done in this chapter was mostly to understand how we obtain the local reciprocity law in an arithmetical way. This way has also been followed to find various generalizations.

Chapter 3

A Cohomological Approach

In this chapter we will give another approach proving to the local reciprocity law. Our first approach was a purely number theoretic one, giving a lot of useful properties of local fields and their extensions.
This approach however, is purely group theoretic, using cohomology groups. Due to limited space we will not go into detail. Instead we try to give a general idea of what is used and how we get the results. For the more detailed cohomological approach see [Ne3]. This chapter is mainly an abridgement of what J. Neukirch describes in his book. At the end of this chapter we will state Artin's global reciprocity law and deduce the well-known quadratic reciprocity law from it using the so-called Hilbert symbol.

3.1 Definitions

Our first subsection will contain crucial definitions from group cohomology.

Our first definition will be the definition of an abstract G-module. Later we will use as our group G the Galois group of an extension.

Definition 3.1.1. Let G be a profinite group. An *abstract G-module M* is an abelian group M together with an action

$$G \times M \to M, \quad (g, m) \mapsto g(m)$$

such that

1. $1(m) = m$

2. $(gh)(m) = g(h(m))$

3. $g(m + n) = g(m) + g(n)$

holds for all $g, h \in G, m, n \in M$.

In the definition we used a profinite group. We will later use G to be a finite group which always is also a profinite group in a trivial way.

Remark 3.1.2. *When we use for example a Galois group as G, this definition is just the natural equivalent to the usual definition of a module as know from Algebra.*

Our next definition is the definition of a cohomology group. In order to be able to define such groups we need some preliminary work.

First we regard a profinite group G. Then we have natural projections:

$$d_i : G^{n+1} \to G^n, \quad i = 0, 1, \ldots, n,$$

given by omitting the i-th component.
We will assume our G-modules to be discrete. This however, will not cause any problem in the application we have in mind - the reciprocity law.

For every G-module A we form the abelian group

$$X^n = X^n(G, A) = \mathrm{Map}(G^{n+1}, A)$$

of all continuous maps $x : G^{n+1} \to A$, i.e. of all continuous functions $x(\sigma_0, \ldots, \sigma_n)$ with values in A. Here the $\sigma_i \in G$. We will see later that this notation is quite natural since we will use a Galois group as G and every Galois group is a profinite group. Then X^n is a G-module in a natural way by

$$(\sigma x)(\sigma_0, \ldots, \sigma_n) = \sigma x(\sigma^{-1}\sigma_0, \ldots, \sigma^{-1}\sigma_n)$$

Now the maps $d_i : G^{n+1} \to G^n$ induce G-homomorphisms $d_i^* : X^{n-1} \to X^n$ by

$$d_i^* : x \mapsto x \circ d_i.$$

With these maps we form the alterning sum

$$\partial^n = \sum_{i=0}^{n} (-1)^i d_i^* : X^{n-1} \to X^n$$

where we will sometimes denote ∂^n by ∂ since it is clear what n is.
Thus for $x \in X^{n-1}$, ∂x is the function

$$(\partial x)(\sigma_0, \ldots, \sigma_n) = \sum_{i=0}^{n} (-1)^i x(\sigma_0, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n)$$

Moreover, we have the G-homomorphism $\partial^0 : A \to X^0$, which associates to $a \in A$ the constant function $x(\sigma_0) = a$.

Definition 3.1.3. We call such a sequence with maps ∂ a *complex* if $\partial^{n+1}\partial^n = 0$. We will denote this by $\partial\partial = 0$ since the powers should be clear.

Proposition 3.1.4. *The sequence*

$$0 \longrightarrow A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \longrightarrow \dots$$

is exact.

Definition 3.1.5. An exact sequence of G-modules $0 \to A \to X^0 \to X^1 \to X^2 \to \dots$ is called a *resolution* of A.

We now set

$$C^n(G,A) = X^n(G,A)^G$$

by which $C^n(G,A)$ consists of the continuous functions $x : G^{n+1} \to A$ such that

$$x(\sigma\sigma_0, \dots, \sigma\sigma_n) = \sigma x(\sigma_0, \dots, \sigma_n)$$

for all $\sigma \in G$. These functions are called *n-cochains* of G with coefficients in A.

From the resolution we therefore obtain another sequence

$$C^0(G,A) \xrightarrow{\partial^1} C^1(G,A) \xrightarrow{\partial^2} C^2(G,A) \longrightarrow \dots,$$

which in general is no longer exact. However, it is still a complex, i.e. $\partial\partial = 0$, which is an easy consequence from the sequence in the proposition being a complex.

We now set

$$\begin{aligned} Z^n(G,A) &= ker(C^n(G,A) \xrightarrow{\partial^{n+1}} C^{n+1}(G,A)) \\ B^n(G,A) &= im(C^{n-1}(G,A) \xrightarrow{\partial^n} C^n(G,A)) \end{aligned}$$

and $B^0(G,A) = 0$. The elements of $Z^n(G,A)$ and $B^n(G,A)$ are called the *n-cocycles* and *n-coboundaries* respectively. Since $\partial\partial = 0$ we see that $B^n(G,A) \subseteq Z^n(G,A)$.

We can now proceed defining a cohomology group.

Definition 3.1.6. For $n \geq 0$ the factor group

$$H^n(G,A) = Z^n(G,A)/B^n(G,A)$$

is called the *n-dimensional cohomology group* of G with coefficients in A.

Remark 3.1.7. *In our definition A is an abelian group. There is also a non-abelian cohomology group, using a non-abelian group A*[1]*.*

Before we can proceed defining the cup product, which will be use in stating the reciprocity law in a cohomological way, we need to define the tensor product.

Definition 3.1.8. Let A and B be modules over the ring of intergers $\mathbb{Z}$. Let F be the free abelian group on the set $A \times B$. Let K be the subgroup of F generated by all elements of the following forms (for all $a, a' \in A, b, b' \in B, r \in R$):

[1] See [Se1] for more on this.

1. (a+a',b)-(a,b)-(a',b)
2. (a,b+b')-(a,b)-(a,b')
3. (ar,b)-(a,rb)

The quotient group F/K is called the *tensor product* of A and B. It is denoted by $A \otimes_R B$ (or simply $A \otimes B$ if $R = \mathbb{Z}$). The coset $(a, b) + K$ of the element (a, b) in F is denoted $a \otimes b$. The coset of $(0, 0)$ is denoted 0.

With this definition we can define the cup product.

If A and B are two G-modules, then $A \otimes_{\mathbb{Z}} B$ is also a G-module (by $\sigma(a \otimes b) = \sigma a \otimes \sigma b$), and we obtain for every pair $p, q \geq 0$ bilinear map

$$C^p(G, A) \times C^q(G, B) \xrightarrow{\cup} C^{p+q}(G, A \otimes B) \tag{3.1}$$

by

$$(a \cup b)(\sigma_0, \ldots, \sigma_p) = a(\sigma_0, \ldots, \sigma_p) \otimes b(\sigma_p, \ldots, \sigma_{p+q}).$$

For this map we have the following proposition:

Proposition 3.1.9. *$\partial(a \cup b) = (\partial a) \cup b + (-1)^p(a \cup \partial b)$.*

From this proposition it follows that $a \cup b$ is a cocycle if a and b are cocycles. Given that a and b are cocycles we have:

$$0 \cup b + (-1)^p(a \cup 0).$$

By the third form of the tensor product we see that this must be in K and therefore is zero in the tensor product. Similiarly we see that the same must hold if a and b are coboundaries.

Therefore the pairing in equation 3.1 induces a bilinear map

$$H^p(G, A) \times H^q(G, B) \xrightarrow{\cup} H^{p+q}(G, A \otimes B)$$

by

$$(\alpha, \beta) \mapsto \alpha \cup \beta.$$

This map is called the *cup-product*. For $p = q = 0$, we obtain the map

$$A^G \times B^G \longrightarrow (A \otimes B)^G$$

$$(a, b) \mapsto a \times b.$$

Remark 3.1.10. *In this definition A^G means that G acts on A from the right. This notation is frequently used in group theory.*

We aim to state the reciprocity law. This will be done with using the theorem of Nakayama and Tate. In this theorem they use another form of cohomology, the n-Tate cohomology group. This will only be done for finite groups, which is sufficient for what we need it.

We consider the norm residue group

$$H^0(G,A) = A^G/N_GA,$$

where N_GA is the image of the norm map

$$N_G : A \to A, \quad N_Ga = \sum_{\sigma\in G} \sigma a.$$

We already know the norm map from previous chapters. Since this approach is purely abstract, we need to define the maps used. However, this definition coincides with the well known norm map from previous chapters in the case we have in mind - using it for the local reciprocity law.

We call the groups

$$\hat{H}^n(G,A) = \begin{cases} A^G/N_GA & \text{for } n = 0 \\ H^n(G,A) & \text{for } n \geq 1 \end{cases}$$

the *modified cohomology groups*.
This definition holds only for $n \geq 0$. In the application we have in mind, the local reciprocity law, we will need n to be -2. Therefore we will now extend our definition.

We need the next sequence to get our maps ∂_n for negative n, which we will use to construct a sequence that will be used for the Tate cohomology.

For $n \geq 0$, let $\mathbb{Z}[G^{n+1}]$ be the abelian group of all formal $\mathbb{Z}$-linear combinations

$$\sum a_{\sigma_0,\dots,\sigma_n}(\sigma_0,\dots,\sigma_n), \sigma_0,\dots,\sigma_n \in G$$

with its obvious G-module structure. We consider the complete standard resolution of $\mathbb{Z}$, i.e. the sequence of G-modules

$$\dots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\partial_0} X_{-1} \xrightarrow{\partial_{-1}} X_{-2} \longrightarrow \dots$$

where $X_n = X_{-1-n} = \mathbb{Z}[G^{n+1}]$ for $n \geq 0$, and the differentials are defined for $n > 0$ by

$$\begin{array}{rcl} \partial_n(\sigma_0,\dots,\sigma_n) & = & \sum_{i=0}^n(-1)^i(\sigma_0,\dots,\sigma_{i-1},\sigma_{i+1},\dots,\sigma_n) \\ \partial_{-n}(\sigma_0,\dots,\sigma_{n-1}) & = & \sum_{\tau\in G}\sum_{i=0}^n(-1)^i(\sigma_0,\dots,\sigma_{i-1},\tau,\sigma_i,\dots,\sigma_{n-1}), \end{array}$$

while $\partial_0 : X_0 \to X_{-1}$ is given by

$$\partial_0(\sigma_0) = \sum_{\tau\in G} \tau.$$

Using the maps ∂_n we can define the *complete standard resolution* of A as the sequence of G-modules

$$\ldots \longrightarrow X^{-2} \xrightarrow{\partial^{-1}} X^{-1} \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \longrightarrow \ldots$$

where $X^{-1-n} = X^n$ =Hom(X_n, A) =Map(G^{n+1}, A) for $n \geq 0$ and ∂^n =Hom(∂_n, A) for $n \in \mathbb{Z}$. Then the above sequence is a complex using the maps

$$D^{-n} : X^{-n+1} \longrightarrow X^{-n}$$

given by

$$\begin{array}{lll}(D^n x)(\sigma_0, \ldots, \sigma_n) = x(1, \sigma_0, \ldots, \sigma_n) & \text{for} & n \geq 0, \\ (D^{-1}x)(\sigma_0) = \delta_{\sigma_0,1}x(1) & \text{for} & n = 1, \\ (D^{-n}x)(\sigma_0, \ldots, \sigma_{n-1}) = \delta_{\sigma_0,1}x(\sigma_1, \ldots, \sigma_{n-1}) & \text{for} & n \geq 2,\end{array}$$

we get

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = id$$

for all $n \in \mathbb{Z}$. From this we conclude that the above sequence is exact.

Finally we have gathered enough information to define the Tate cohomology group.

For every $n \in \mathbb{Z}$ we now define the *n-th Tate cohomology group* $\hat{H}^n(G, A)$ as the cohomology group of the complex

$$\hat{C}(G, A) = ((X^n)^G)_{n \in \mathbb{Z}}$$

at n:

$$\hat{H}^n(G, A) = H^n(\hat{C}(G, A)),$$

similar as before for $H^n(G, A)$.
Clearly, for $n \geq 0$ we get the previous (modified) cohomology groups.

In order to proceed defining essential objects for the reciprocity law, we first need the restriction.

For an arbitrary closed subgroup H of G and a G-module A, we consider the two homomorphisms

$$H \overset{\text{incl}}{\hookrightarrow} G, \quad A \overset{\text{incl}}{\hookrightarrow} A.$$

On the cochains they induce a restriction map and we obtain homomorphisms on the cohomology

$$\text{res}^H_F : H^n(G, A) \longrightarrow H^n(H, A),$$

called *restriction.* Cleary the restriction is transitive, i.e. for two closed subgroups $F \subseteq H$, we have

$$\text{res}^H_F \circ \text{res}^G_H = \text{res}^G_F.$$

We can now proceed defining the fundamental class, which will get us closer to stating the local reciprocity law in a group cohomological way.

Let G be a finite group. We call a G-module C a *class module* if for all subgroups H of G

1. $H^1(H, C) = 0$ and
2. $H^2(H, C)$ is cyclic of order $|H|$.

Definition 3.1.11. A generator γ of $H^2(G, C)$ is called a *fundamental class.*

In order to define the invariant maps that will be used in the reciprocity law we need to construct a new G-module from a class module.

As we have n-th cocycles we could also define n-th *inhomogeneous* cocycles in a similiar way[2]. These are elements of $\mathcal{C}^n(G, A)$, which is the abelian group of all continuous functions $y : G^n \to A$. From that we could also define, similar to before, the sets $\mathcal{Z}^n(G, A)$ and $\mathcal{B}^n(G, A)$.
We could also show, that we have isomorphisms

$$H^n(G, A) \simeq \mathcal{Z}^n(G, A)/\mathcal{B}^n(G, A)$$

where $\mathcal{Z}$ and $\mathcal{B}$ are similiarly the kernel and the image of the maps between those sets $\mathcal{C}^n$.

To each G-module C and each class $\gamma \in H^2(G, C)$ we associate a G-module $C(\gamma)$ as follows. Let $B = \bigoplus_{\sigma \neq 1} \mathbb{Z} b_\sigma$ be the free abelian group with basis b_σ, indexed by the elements $\sigma \in G$, $\sigma \neq 1$. We set

$$C(\gamma) = C \oplus B,$$

and we let G act on $C(\gamma)$ by the means of an inhomogeneous cocycle $c(\sigma, \tau)$ representing γ as follows: we set $b_1 = c(1, 1)$ and define

$$\sigma b_\tau = b_\tau - b_\sigma + c(\sigma, \tau).$$

This is really a G-action and we could also show that we have map $H^2(G, A) \to H^2(G, C(\gamma))$ which maps γ to zero. $C(\gamma)$ is therefore called the *splitting module* of γ.

[2] Inhomogeneous cocycles are basically such, that are not in the same equivalence class of the coboundaries. For a detailed definition see [Se1].

3.2 The Local Reciprocity Law

In this section we use the definitions of the previous sections to state the local reciprocity law.

We have the following theorem from wich we will get the definition of invariant maps.

Theorem 3.2.1. *Let G be a finite group. For each $n \in \mathbb{Z}$ and each subgroup $H \subseteq G$, the homomorphism*

$$\delta^2 : \hat{H}^n(H, \mathbb{Z}) \to \hat{H}^{n+2}(H, C)$$

is given by the cup-product $\beta \mapsto \gamma_H \cup \beta$, where $\gamma_H = res_H^G(\gamma)$. The following conditions are equivalent:

1. *$C(\gamma)$ is a cohomologically trivial G-module*
2. *C is a class module with fundamental class γ*
3. *δ^2 is an isomorphism for all $n \in \mathbb{Z}$ and all H.*

If C is a class module for G, then by the above theorem we have isomorphisms

$$(\delta^2)^{-1} : H^2(H, C) \longrightarrow \frac{1}{|H|}\mathbb{Z}/\mathbb{Z}, \quad \gamma_H \mapsto \frac{1}{|H|} \mod \mathbb{Z},$$

where $\gamma \in H^2(G, C)$ is a chosen fundamental class. These are called *invariant maps* and denoted by *inv*.

We can now state a very important theorem that we would need to prove the reciprocity law:

Theorem 3.2.2 (Nakayama-Tate)**.** *Let G be a finite group, let C be a class module for G and let $\gamma \in H^2(G, C)$ be a fundamental class. Then, for all integers $i \in \mathbb{Z}$, the cup-product*

$$\hat{H}^i(G, \mathrm{Hom}(A, C)) \times \hat{H}^{2-i}(G, A) \xrightarrow{\cup} H^2(G, C) \simeq \frac{1}{|G|}\mathbb{Z}/\mathbb{Z},$$

where $H^2(G, C) \simeq \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$ is given by $\gamma \mapsto \frac{1}{|G|} \mod \mathbb{Z}$, induces an isomorphism

$$\hat{H}^i(G, \mathrm{Hom}(A, C)) \simeq \hat{H}^{2-i}(G, A)^*,$$

provided that A is $\mathbb{Z}$-free. If, in addition, A is finitely generated, then this is an isomorphism of finite abelian groups.

We now apply this theorem to the case $A = \mathbb{Z}$, $i = 0$ and using that we could also show

$$H^2(G, \mathbb{Z})^* \simeq H^1(G, \mathbb{Q}/\mathbb{Z})^* = \mathrm{Hom}(G^{ab}, \mathbb{Q}/\mathbb{Z})^* = G^{ab}.$$

From that we obtain a crucial theorem with which the local reciprocity law can be proved.

Theorem 3.2.3. *If C is a class module for the finite group G, then we have an isomorphism*

$$\rho = \rho_G : G^{ab} \to C^G/N_G C,$$

called the Nakayama map. *It depends on the choice of a fundamental class $\gamma \in H^2(G, C)$ and satisfies (by definition) the formula*

$$\chi(\sigma) = inv(\rho(\sigma) \cup \delta_\chi)$$

for all characters[3] $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z})$.

This theorem is actually quite close to the local reciprocity law. What still needs to be proved is that it really applies in the case of local fields.

First, it can be shown that for a finite Galois extension L/K of a local field K the multiplicative group K^* is a class module for the Galois group $G(L|K)$. It can also be deduced that we have a canonical fundamental class $\gamma \in H^2(G, K^*)$. Therefore, by the Nakayama-Tate theorem, we obtain the next theorem.

Theorem 3.2.4. *Let $L|K$ be a finite extension of local fields with Galois group G. Let A be a finitely generated $\mathbb{Z}$-free G-module and $A' = \mathrm{Hom}(A, K^*)$. Then for all $i \in \mathbb{Z}$ the cup-product*

$$\hat{H}^i(G, A') \times \hat{H}^{2-i}(G, A) \xrightarrow{\cup} H^2(G, K^*) = \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

induces an isomorphism of finite abelian groups

$$\hat{H}^i(G, A') \simeq \hat{H}^{2-i}(G, A)^*.$$

In the case $i = 0$ and $A = \mathbb{Z}$ we have $H^2(G, \mathbb{Z})^* \simeq H^1(G, \mathbb{Q}/\mathbb{Z})^* = (G^{ab})$, and we obtain the main theorem of local class field theory, the local reciprocity law:

Theorem 3.2.5 (Local Reciprocity Law)**.** *Let K be a local field and let $L|K$ be a finite Galois extension. Then there is a canonical isomorphism*

$$K^*/N_{L/K}L^* \simeq G(L|K)^{ab}.$$

The norm groups $N_{L/K}L^*$ for a finite Galois extension $L|K$ are precisely the open subgroups of finite index in K^*.

Apparently it had been this isomorphism which initiated the use of cohomology in number theory. As we can see, we obtain the very same result with this cohomological approach than with the one in the previous chapter. However, the method we tried to explain here does not use any of the arithmetical properties of local fields. But those fields are used widely in number theory and algebraic geometry. Therefore the first approach, developing the theory of local fields, is probably the more helpful one for understanding number theory and local fields.

[3] See definition 4.3.6 for characters.

As we saw in this cohomological approach, it is not quite as short and simple as one might suggest. It also requires a lot of definitions and would also require some technical properties of those objects defined. Due to limited space and to keep the section an overview, as it was intended, we did not show any of those. Hopefully the idea of what is used and how we proceed in obtaining the local reciprocity law in a cohomological way is given.

3.3 The Global Reciprocity Law

In this section we will state Artin's reciprocity law. The basic idea of this global reciprocity law is that we replace the mulitplicative group from the local law with so-called ideles. We will also see later that this is very suitable for the local-to-global principle.

In addition to the theory we developed in the chapter about valuation theory we define:

Definition 3.3.1. A *prime* p of an algebraic number field K is a class of equivalent valuations of K. The nonarchimedian equivalence classes are called *finite* primes and the archimedian ones *infinite* primes.

As we saw in the theorem of Ostrowski 1.3.5, we have just one infinite prime for complete fields. It can also be shown, that the primes of an extension of $\mathbb{Q}$ can be identified with those of $\mathbb{Q}$ itself. Therefore, since $\mathbb{Q}$ has well known prime ideals, we will identify the primes of an extension of $\mathbb{Q}$ with the primes in $\mathbb{Q}$ and ∞ for the infinite prime.

Remark 3.3.2. *1. We will denote the completion of K at the prime p by K_p.*

2. In the chapter about valuation theory we said that we call $\mathcal{O}_K$ the ring of integers. In addition to this, we say the elements of $\mathcal{O}_K$ are integral in K_p. We saw in the first chapter that $\mathcal{O}_K$ is integrally closed, which justifies the term 'integral'.

Definition 3.3.3. An *adele* of a local field K is a family

$$\alpha = (\alpha_p)$$

of elements $\alpha_p \in K_p$ where p runs through all primes of K and α_p is integral, having non-negative valuation, in K_p for almost all p. It can easily be seen that the adeles form a ring, which is denoted by

$$\mathbb{A}_K = \prod_p K_p.$$

Addition and multiplication are defined componentwise. This kind of product is called the 'restricted product' of the K_p with respect to the subrings $\mathcal{O}_p \subseteq K_p$.

The *idele group* of K is defined to be the unit group

$$I_K = \mathbb{A}_K^*.$$

Thus an idele is a family

$$\alpha = (\alpha_p)$$

of elements $\alpha_p \in K_p^*$ where α_p is a unit in the ring $\mathcal{O}_p$ of integers of K_p, for almost all p. In analogy with $\mathbb{A}_K$ we write the idele group as the restricted product

$$I_K = \prod_p K_p^*$$

with respect to the unit groups $\mathcal{O}_p^*$.

We now discuss why we can have an inclusion map $K^* \to I_K$.

For every finite set of primes S, I_K contains the subgroup

$$I_K^S = \prod_{p \in S} K_p^* \times \prod_{p \notin S} U_p$$

of *S-ideles*, where $U_p = K_p^*$ or $U_p = \mathbb{R}_+^*$ for p depending on a property of the prime which we will not discuss here. For a detailed discussion on this restricted product see [Ne2]. We then clearly have

$$I_K = \bigcup_S I_K^S,$$

if S varies over all finite sets of primes of K.

The inclusions $K \subseteq K_p$ allow us to define the diagonal embedding

$$K^* \to I_K,$$

which associates to $a \in K^*$ the idele $\alpha \in I_K$ whose p-th component is the element a in K_p.

Definition 3.3.4. The elements of the subgroup K^* of I_K are called *principal ideles* and the quotient group

$$C_K = I_K/K^*$$

is called the *idele class group* of K.

We now gathered enough information to state Artin's reciprocity law:

Theorem 3.3.5 (Artin's Reciprocity Law)**.** *Let $L|K$ be a finite Galois extension of global fields with Galois group $G(L|K)$. Then there is a canonical isomorphism*

$$r_{L|K} : G(L|K)^{ab} \longrightarrow C_K/N_{L/K}C_L.$$

The inverse map of $r_{L/K}$ yields a surjective homomorphism

$$(., L|K) : A_K \to G(L|K)^{ab}$$

with kernel $N_{L|K}A_L$. This map is called the *norm residue symbol* of L/K.

A proof of this would be too long. Instead we give a quick description of how we would proceed:

Generally, we obtain the global reciprocity law from theorem 3.2.3. To use this theorem, we have to show that we really have a class module. This is, again, done by using serveral properties of cohomology groups.

For every prime p of K we have the canonical injection

$$[.] : K_p^* \to C_K,$$

which associates to each $a_p \in K_p^*$ the class of the idele

$$[a_p] = (\dots, 1, 1, 1, a_p, 1, 1, 1, \dots).$$

What is really important is the compatibility of local and global class field theory, which follows from the next proposition.

Proposition 3.3.6. *If $L|K$ is an abelian extension and p a prime of K, then the diagram*

$$\begin{tikzcd}
K_p^* \arrow[r, "{(.,L_p|K_p)}"] \arrow[d, "{[.]}"'] & G(L_p|K_p) \arrow[d] \\
C_K \arrow[r, "{(.,L|K)}"] & G(L|K)
\end{tikzcd}$$

is commutative.

3.4 Deducing Quadratic Reciprocity

In this section we will try to demonstrate how the well-known Gaussian reciprocity law can be deduced from the global reciprocity law.

First we need the definition of the Hilbert symbol.

We know from previous sections, primes split into finite and infinite primes, where the infinite primes are the equivalence classes of the archimedian valuations.

Let K be a local field. We will also assume that K contains the group μ_n of roots of unity where n is a natural number prime to the characteristic of K. Let $L = K(\sqrt[n]{K^*})$ be the maximal abelian extension of exponent m. [Ne1, Chapter 3, 3.2] shows that we then have

$$N_{L/K}L^* = K^{*n}.$$

So by class field theory we obtain a canonical isomorphism

$$G(L/K) \simeq K^*/K^{*n}.$$

On the other hand, *Kummer theory*, which is not part of this text, gives us a canonical isomorphism

$$\mathrm{Hom}(G(L|K), \mu_n) \simeq K^*/K^{*n}.$$

Therefore the bilinear pairing

$$G(L|K) \times \mathrm{Hom}(G(L|K), \mu_n) \to \mu_n,$$

$$(\sigma, \chi) \mapsto \chi(\sigma),$$

produces a bilinear pairing

$$\left(\frac{\cdot,\cdot}{p}\right) : K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n$$

which is bilinear in the multiplicative sense. This pairing is called the *Hilbert symbol*. We have the following explicit connection to the previously defined norm residue symbol:

Proposition 3.4.1. *If $a, b \in K^*$, then the Hilbert symbol $\left(\frac{a,b}{p}\right) \in \mu_n$ is given by*

$$(a, K(\sqrt[n]{b})|K)\sqrt{n}b = \left(\frac{a,b}{p}\right)\sqrt[n]{b}.$$

For a proof see [Ne1].

We will now proceed defining the n-th power residue symbol. We will see that it is generalizing the Legendre symbol.

We already saw in previous sections that we have a decomposition $\mathcal{O}^* = \mu_{q-1} \times U^{(1)}$. So every unit $u \in U_K$ has a unique decomposition

$$u = \omega(u) \cdot \langle u \rangle$$

with $\omega(u) \in \mu_{q-1}, \langle u \rangle \in U^{(1)}$ and $u \equiv \omega(u) \mod p$. With this notation we have

Theorem 3.4.2. *If $(n,p) = 1$ and $a, b \in K^*$, then*

$$\left(\frac{a,b}{p}\right) = \omega\left((-1)^{\alpha\beta}\left(\frac{b^\alpha}{a^\beta}\right)^{\frac{q-1}{n}}\right),$$

where $\alpha = v_K(a), \beta = v_K(b)$.

For a proof see [Ne1].

In particular, the theorem shows that (in case $(n,p) = 1$) the Hilbert symbol

$$\left(\frac{\pi,u}{p}\right) = w(u)^{\frac{q-1}{n}}$$

is independent of the choise of the prime element π. We may therefore set

$$\left(\frac{u}{p}\right) := \left(\frac{\pi,u}{p}\right) \qquad \text{for } u \in U_K.$$

$(\frac{u}{p})$ is an n-th root of unity determined by

$$\left(\frac{u}{p}\right) \equiv u^{\frac{q-1}{n}} \mod p_K.$$

We call it the *Legendre symbol* or the *n-th power residue symbol*. Both names are justified by the following proposition.

Proposition 3.4.3. *Let $(n,p) = 1$ and $u \in U_K$. Then*

$$\left(\frac{u}{p}\right) = 1 \Leftrightarrow u \quad \text{is an } n\text{-th power} \quad \text{mod } p_k.$$

The above definition of the n-th power residue symbol is for any prime ideal p of K. We will now extend this definition to any ideal. This is done very similiar as the extension from the Legendre symbol to the Jacobi symbol in basic number theory.

Definition 3.4.4. For any ideal $b = \prod_{p \nmid n} p^{v_p}$ of K prime to n and any number a prime to b, we define the *n-th power residue symbol* by

$$\left(\frac{a}{b}\right) = \prod_{p \nmid n}\left(\frac{a}{p}\right)^{v_p}.$$

Clearly the power residue symbol $\frac{a}{b}$ is multiplicative in both arguments. To see this please compare to the Jacobi symbol, which is based on the Legendre symbol.

We can now state the general reciprocity law of n-th power residues.

Theorem 3.4.5. *If $a, b \in K^*$ are prime to each other and to n, then*

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right)^{-1} = \prod_{p \mid n \cdot \infty}\left(\frac{a,b}{p}\right).$$

The proof of this theorem is quite simple. Although we will refer to [Ne1].

Remark 3.4.6. *The term $p \mid n \cdot \infty$ should be read as p is running through all primes including the infinite one.*

The next theorem is the well known Gaussian Reciprocity law. It follows straight forward from the theorem above.

Theorem 3.4.7 (Gauss' Reciprocity Law)**.** *Let $K = \mathbb{Q}$, $n = 2$ and let a and b be coprime non-negative odd integers. Then*

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

and furthermore

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}.$$

This theorem can be seen using the explicit formula of the Hilbert symbol for $p = 2$ and $p = \infty$.

1. If $p = 2$ and $a, b \in U_{\mathbb{Q}_p}$, then
$$\left(\frac{a, b}{2}\right) = \left(\frac{b, a}{2}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}.$$
2. $\left(\frac{a,b}{p}\right)^{-1} = \left(\frac{b,a}{p}\right)$
3. $\left(\frac{a,b}{\infty}\right) = 1$ in these cases.

Proof. From the previous theorem 3.4.5 we know that we have

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right)^{-1} = \left(\frac{a, b}{2}\right) \cdot \left(\frac{a, b}{\infty}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}} \cdot 1 = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}.$$

□

Chapter 4

Recent Results in Class Field Theory

In this chapter we give a summary of recent results in class field theory. Those are, as can be seen below, widely spreaded.

First, we follow approaches of a more general ground field. Although there have been some interesting results at this part, there are still many unresolved cases.
The second section is dedicated to more general laws. However, in the local case this has been resolved with the Langlands conjecture. Mainly, research focused on finding a nonabelian generalization of the existence theorem. This was approached by nonabelian reciprocity laws. Although the proof of the Langlands conjecture gives the existence of a nonabelian existence theorem, it does not assert the noncommutative reciprocity map. Therefore research on this has been included here in an additional section.
In the third section we try to give a very general idea of the Langlands conjecture and its consequences. There is a lot of terminology needed to even properly state the Langlands correspondence. Once this is done, we discuss several approaches to it. The Langlands conjecture has been proved completely for the local case. For the global Langlands correspondence there is a proof from 2002 in the case of function fields. Of course the Langlands conjecture would be a very important statement, deducing a nonablian global reciprocity law.
The last section summerizes a few results on constructions of class fields, or fields with certain class field towers. As an application, we picked a few recent research results that used parts of class field theory.

There are also very recent results related to class field theory or the Langlands conjectures. Such as Serre's conjecture on representations. Another very intersting part of research goes more detailed into higher dimensional fields and explores all kinds of subjects on them. Ramification theory, as we studied it in the first chapter, is also generalized and studied more detailed on various fields. Those topics, however, are not discussed here.

4.1 Generalizations of the Ground Field

In this first section we will discuss reciprocity laws on more general fields than local fields. Those are, in our definition, complete discrete valuation fields with a finite residue field. We will try to extend the local reciprocity law to a various number of fields, including generally Henselian fields or fields with imperfect residue field. This section should give a summary of what happend in this part of generalization of the local reciprocity law over the last decade. To accomplish that, we picked selected papers and will demonstrate how complicated generalizations can get on them.

Before we begin stating more recent result, we would like to briefly explain the following result. This result allows us to see local fields in a more general context and is one of many generalizations.

In chapter 2 we developed a theory with local fields. We defined local fields to have a finite residue field. More general, most of the theory developed before the local reciprocity law also holds for fields with perfect, but not necessarily finite, residue field (in the appendix of this text we see that every finite field is perfect). Fesenko generalized this approach to the perfect residue field case in his paper [Fe3] in 1994. In his paper, he gives a description of abelian strictly ramified p-extensions of a field complete with respect to a discrete valuation with a perfect residue field of characteristic p. The approach is as follows: He uses similiar techniques as we developed for the finite residue field case and generalizes them. Mainly, he works with the methods Neukirch used in [Ne1].

We will now see that the case of quasilocal fields also admits a generalization to a one dimensional nonabelian local class field theory.

Quasilocal Fields In this paragraph we discuss the role that quasilocal fields play in generalizing local class field theory. In the first case we have a look at strictly quasilocal fields.

First, we need to define what quasilocal fields are.

Definition 4.1.1. A field E is called *primarily quasilocal* (PQL) if for every prime number p, E has no proper finite Galois p-extensions, or the Brauer group $Br(E)$ has trivial p-primary component, or every cyclic field extension of E of degree p embeds as an E-subalgebra in every central division E-algebra of Schur index p.
We call E *strictly primarily quasilocal* if, in addition, whenever p is a prime number and the p-primary part of $Br(E)$ is trivial, E has no nontrivial p-extensions.

Remark 4.1.2.

1. *We used the Brauer group and the Schur index in the above definition. The Brauer group is the group of equivalence classes of central simple algebras. However, we will not go into detail about those terms.*
2. *In ring theory a* central algebra *over a field K is a finite-dimensional associative algebra for which the center is exactly K. A* central division algebra *is an extension*

(a ring) that is a division ring. We will later have the add the term simple *to it, which means there are no non-trivial ideals*[1]*.*

With these definitions above we can define what a strictly quasilocal field is.

Definition 4.1.3. A field K is called *strictly quasilocal*, if its finite extensions are strictly primarily quasilocal.

By the existence theorem we obtained a one-to-one correspondence between the open subgroups of group F^* on the one hand and the abelian extensions on the other. So if we take an open subgroup of finite index from F^*, we can uniquely asign an abelian extension to it. This encourages the following definition:

Definition 4.1.4. For every open subgroup N of finite index of F^*, the multiplicative group of a local field F, there exists an abelian extension L/F, such that $N_{L/F}L^* = N$. This is the *class field* of the subgroup N.

Now I.D. Chipchakov [Ch3] shows, that such fields allow a more general, even non-abelian one dimensional local class field theory. This paper shows that the norm group $N_{R/F}R^*$ possesses a class field denoted by $cl(N_{R/F})$ which is uniquely determined by the norm group, up-to a F-isomorphism. I.D. Chipchakov also showed, that this class field $cl(N_{R/F})$ includes as a subfield the maximal abelian extension R^{ab} of F in R. Hence he deduces a canonical bijection ω of the set of isomorphism classes of a class field upon the set $Nr(F)$ of norm groups of finite separable extensions of F.
The study of such quasilocal fields admits a limitation to the special case of finite abelian extensions. Hence it really is a generalization to a nonabelian local class field theory.

Let $P(F)$ be the set of those prime numbers p for which F is properly included in its maximal p-extension $F(p)$ in F^{sep}.

The main assertion of this paper can be summerized as follows:

Theorem 4.1.5 (Chipchakov)**.** *Let (F, v) be a discrete Henselian strictly quasilocal field with a residue field κ. Then the class field and norm groups of F are related as follows:*

1. *For each $U \in Nr(F)$, there exists a class field $cl(U)$ which is uniquely determined, up to a F-isomorphism. The extension $cl(U)$ over F is abelian if and only if $F(\kappa)$ contains the prime divisors of the index of U in F^*.*

2. *A class field $cl(U)$ of a group $U \in Nr(F)$ embeds as a F-subalgebra in a finite extension R of F in F^{sep} if and only if $N_{R/F}R^*$ is included in U. Furthermore, if $N_{R/F}R^* = U$, then the F-isomorphic copy of $cl(U)$ in R is unique and includes R^{ab}.*

3. *There exists a set $\varphi_U : U \in Nr(F)$ of extensions of F in F^{sep}, such that φ_U is a class field of U, $U \in Nr(F)$, and for each $U_1, U_2 \in Nr(F)$, $\varphi_{U_1 \cap U_2}$ equals the compositum $\varphi_{U_1}\varphi_{U_2}$ and $\varphi_{U_1U_2} = \varphi_{U_1} \cap \varphi_{U_2}$.*

[1] This is an analogue of simple groups.

This covers the case of strictly quasilocal fields.
In another paper by I.D. Chipchakov [Ch1] he claims that every field F admitting a one-dimensional local class field theory is strictly quasilocal provided that $Br(F)$ is nontrivial and F has the following property: every central simple algebra of prime exponent p over F is similar to a tensor product of cyclic division F-algebras of Schur index p. The latter property is known to hold for many important classes of fields. It is currently unknown if it holds in general.

Reciprocity for Higher Local Fields Our next paragraph deals with generalizations to higher local fields. Such higher local fields are widely used. A lot of different theory has been developed on them as we will see in this chapter. The theory we developed in this text can be seen as a one-dimensional case of n-dimensional local fields. However, this should not be confused with the way we extend dimensions the Langlands correspondence later. Therefore, first a definition of what we are using here.

Definition 4.1.6. A complete discrete valuation field K is said to have the structure of an *n-dimensional local field* if there is a chain of fields

$$K = K_n, K_{n-1}, \dots, K_1, K_0$$

where K_{i+1} is a complete discrete valuation field with residue field K_i and K_0 is a finite field. The field K_{n-1} (resp. K_0) is said to be the *first (resp. the last) residue field* of K.

In this paragraph we would like to give a summary of in what context the local reciprocity law still holds for such fields. An overview of some other work done on such fields with be given at the end of this chapter.

Before we can outline some of the major results on such fields, we need to define the frequently used Milnor K-group. Acutally, we can see that such groups are related to abelian extensions. But first the definition.

Let F be a field, A an abelian group. A map

$$f : \underbrace{F^* \times \cdots \times F^*}_{n\text{times}} \to A$$

is called an *n-symbolic map* on F if

1. $f(\dots, \alpha_i\beta_i, \dots) = f(\dots, \alpha_i, \dots) + f(\dots, \beta_i, \dots)$ for $1 \leq i \leq n$ (multiplicativity).
2. $f(\alpha_1, \dots, \alpha_n) = 0$ if $\alpha_i + \alpha_j = 1$ for some $i \neq j$, $1 \leq i, j \leq n$ (*Steinberg property*).

Let I_n denote the subgroup in $\underbrace{F^* \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^*}_{n \text{ times}}$ generated by the elements

$$\alpha_1 \otimes \cdots \otimes \alpha_n \quad \text{with} \quad \alpha_i + \alpha_j = 1 \text{ for some } i \neq j.$$

The *n-th Milnor K-group* of the field F is the quotient

$$K_n(F) = \underbrace{F^* \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^*}_{n \text{ times}} / I_n.$$

The construction of the n-th K-Milnor group shows, that we can extend an n-symbolic map to the n-th group. Following this we obtain a homomorphism $K_n(F) \times K_m(F) \to K_{n+m}(F)$. This shows that the definition of the Milnor groups does make sense in a way that higher groups are still related to the lower ones.

Remark 4.1.7. *Those K-groups are themselves very important as this summary by H. Gillet of a paper [Bl4] by S. Bloch from 1981 states: 'One of the reasons algebraic K-theory is so tantalizing is that even though very little is known about how to compute it, new connections between it and arithmetic and geometry are continually being found or conjectured. For example, K-theory is intimately related to intersection theory [see, for example, D. R. Grayson, [Gr]], S. Bloch [Bl1], crystalline cohomology [S. Bloch [Bl2]], and special values of ζ- and L-functions [C. Soule, [So], S. Bloch [Bl3]].'*

In this aricle S. Bloch finds an analogue for regular arithmetic surfaces with specific properties, of the classical isomorphism between the ideal class group of the ring of integers $\mathcal{O}$ in a number field L and the Galois group $\mathrm{Gal}(H/L)$ *of the* Hilbert class field[2] *H of L.*

First we would like to mention the work done by I. Fesenko in [Fe2], [Fe1], who succeded in establishing a class field theory for such fields if $\mathrm{char}(k(n)) \neq \mathrm{char}(k(n-1)) = p$. Generalizing the method of J. Neukirch (in the case n = 1 of local number fields), he constructed the reciprocity map

$$F : K_n^{top}(F) \to \mathrm{Gal}(F^{ab}/F)$$

as an injection with dense image, where $K_n^{top}(F)$ denotes a well-defined factor of Milnors K-group $K_n(F)$.

This theory however has first been developed by Parshin [Pa1, Pa2, Pa3] for the case of a residue field of characteristic p and by Kato [Ka1, Ka2, Ka3] for the general case. But let us first have a look at what we get in the one dimensional case. For every finite field we can see easily that we have an injective homomorphim

$$\mathbb{Z} \to \mathrm{Gal}(K^{sep}/K).$$

We can interpret this homomorphism as the 0-dimensional local reciprocity map

$$K_0(K) \to \mathrm{Gal}(K^{ab}/K).$$

By convention $K_0(K) = \mathbb{Z}$. This convention proves to be useful. For an explaination why, see [FeVo2, Chapter 9].

[2] See Definition 4.4.1 for the definition.

It is then natural to expect that for an n-dimensional local field F its n-th Milnor K-group $K_n(F)$ should be related to abelian extensions of F. And indeed, there is a higher dimensional local class field theory first developed by A.N. Parshin and K. Kato in the above mentioned papers. Let us briefly describe here how this generalization is obtained. We aim to get a higher dimensional reciprocity map

$$\Psi_F : K_n(F) \to \mathrm{Gal}(F^{ab}/F).$$

Let L/F be a finite Galois extension and $\sigma \in \mathrm{Gal}(L/F)$. Denote by F' the maximal unramified extension of F corresponding the maximal separable extension of its last residue field $\mathbb{F}_q$. Then there is $\tilde{\sigma} \in \mathrm{Gal}(LF'/F)$ such that $\tilde{\sigma}|_L = \sigma$ and $\tilde{\sigma}_{F'}$ is a positive power of the lifting of the Frobenius automorphism of $G_{\mathbb{F}_q}$. The fixed field Σ of $\tilde{\sigma}$ is a finite extension of F. Let $t_1, \dots, t_n$ be a lifting of prime elements of residue fields $\Sigma_1, \dots, \Sigma_{n-1}, \Sigma$ of Σ to Σ. A generalization of the Neukirch map is then defined as

$$\sigma \mapsto N_{\Sigma/F} t_1, \dots, t_n \mod N_{L/F} K_n(L).$$

A specific feature of higher dimensional local fields is that in general for an arbitrary finite Galois extension L/F linearly disjoint with F'/F a generalization of the Hazewinkel homomorphism does not exist. This is due to the fact that the map

$$i_{F/F'} : K_n(F) \to K_n(F')$$

is not injective for $n > 1$. Still one can define a generalization of the Hazewinkel map for extensions which are composed of so-called *Artin-Schreier* extensions, and this is enough to prove that the Neukirch map induces an isomorphism

$$\mathrm{Gal}(L/F)^{ab} \tilde{\to} K_n(F)/N_{L/F} K_n(L)$$

as is shown by I. Fesenko in [Fe4].

Of course on of the central parts of generalizing local class field theory is the existence theorem for higher local fields. This has been elaborated by K. Kato and summarized in [Ka4]. In this paper K. Kato characterizes subgroups of the Milnor group in a categorial way and uses the Milnor group to obtain the existence theorem for higher local fields.

With this fact in mind, we can have a look at what has been obtained from this result in the last decade.

As a first example of what has been done we would like to give a short summary of an article by A. Shiho [Sh2].

As shortly stated above it is known that central statements of class field theory of higher local fields (even though not easy to formulate and develop) are relatively similar to those in class field theory of one-dimensional fields, whereas class field theory of higher-dimensional fields which are not entirely complete has features quite distant from class field theory of one-dimensional fields. In his paper, A. Shiho illustrates this principle for the fraction field K of a *two-dimensional complete normal local ring* A with finite residue field.

Another interesting paper is one elaborating explicit reciprocity laws for p-divisible groups over higher local fields by T. Fukaya ([Fu2]). In this paper T. Fukaya establishes an explicit formula for the generalized Hilbert pairing by systematic work with differential forms.

Remark 4.1.8. *As we saw in chapter 3, we can use the Hilbert pairing to deduce the Gaussian reciprocity law. Therefore having explicit formulas for the Hilbert symbol allows us to deduce the Quadratic reciprocity law in the same way from the generalized one for higher local fields.*

The above mentioned paper can be seen as a generalization of two papers by D. Benois [Be2] and M. Kurihara [Ku1].The first author developed such theory for p-divisible groups over one-dimensional local fields, while M. Kurihara had a closer look on the multiplicative group over higher dimensional local fields. As an application of the higher exponential homomorphisms M. Kurihara gives a simple proof of the explicit reciprocity law for local fields of S. Sen [Se3] and generalizes the explicit reciprocity laws to higher dimensional local fields.

4.2 Generalizations of the Reciprocity Law

In this section we will give various examples af generalizations. One was already mentioned above, the one from I.D. Chipchakov [Ch3] in 2005. We will see here, why this was not the first generalization to nonabelian class field theory. Moreover, we will give a few papers, that will all fit together in the Local Langlands Conjecture. Historically the local reciprocity law was deduced from the global reciprocity law. Later on, purely local proofs were found by Hasse and Chevalley. The Langlands correcpondence, the currently best known generalization of the reciprocity law, has already been proved for the local case, but just for special cases in the global case.

We will, however, start with showing what work has been done before the local Langlands correspondence was shown for the general case. From Artin's reciprocity law, it is natural to go looking for a nonabelian one. But how would a more general reciprocity law look like? Langlands conjectured a certain representation of it, as we will see later.

Our first case will deal with metabelian extensions. Metabelian groups can be thought of as groups that are 'close' to being abelian, in the sense that every abelian group is metabelian, but not every metabelian group is abelian.

Definition 4.2.1. A group G is *metabelian* if there exists a normal subgroup A of G such that both A and G/A are abelian.

Remark 4.2.2. *This definition can easily be seen to coincide with the one from the appendix.*

The generalization of the local reciprocity law follows immediately from the next proposition.

Proposition 4.2.3. *Every abelian group is metabelian.*

The first approach to metabelian extensions was made by H. Koch in [Ko]. In this paper he started with a local field with residue field of cardinality q. Denote by K_f the unramified extension over K of degree f. The theory of fields of norms due to J.-M. Fontaine and J.-P. Wintenberger in [FoWi] implies that finite abelian extensions of $K_f K_\pi$ correspond to certain abelian extensions of the field of norms attached to $K_f K_\pi$. It is well known that the compositum K_π of all finite abelian extensions over K in which a fixed prime element π of K is a norm can be described by means of Lubin-Tate formal groups. Such groups are formally uniquely descriped by a property[3]. Therefore the finite abelian extensions can be described using Lubin-Tate formal groups.

However, in practice it is a very intricate matter to get any explicit description. The currently discussed paper by H. Koch [Ko] provides a description of finite abelian extensions of $K_f K_\pi$.

This was a first step to generalizing the local reciprocity law. A next paper by H. Koch and E. de Shalit [KoSh] gave a specific main result about metabelian extension. Let

[3] For more on them see [FeVo2, Chapter 8, Section 1].

therefore G_d be a certain set of all pairs $(\pi^n \cdot \epsilon \cdot h(X)) \in K^* \times k[[X]]^*$ satisfying a certain condition depending on d. Then denote by $G(L)$ the inverse limit of G_d, $d \in \mathbb{N}$, with respect to a natural transition map $G_{dd'} \to G_d$.

The main result is that the correspondence $L \to N_{L/K}G(L)$ is one-to-one between all finite metabelian extensions of K and all open subgroups of finite index in $G(K)$ and there is a canonical isomorphism

$$G(K)/N_{L/K}G(L) \simeq G(L/K)$$

which is compatible with field extensions. Although this result is quite excellent, according to the reviewer of this paper, I. Fesenko, it would be important to find an exposition of the theory without using formal groups and generalize it to the case of perfect residue fields.

The next result is due to E.W. Zink in [Zh]. In this paper he extends local class field theory to the maximal nilpotent extension of *class* 2 of K. In a paper by F. Laubie, [La4], he extends those two approches by E.W. Zink and H. Koch and E. de Shalit. The isomorphism that those two papers state is extended to the absolute Galois group G_K of the field K. He uses the assumption that there is a fixed Frobenius automorphism φ in the Galois group of this extension. Namely, he constructs a complete group $\mathcal{G}(K, \varphi)$ and its continuous isomorphism to G_K satisfying the usual properties of the reciprocity map, with some exceptions.

Using the norm fields of arithmetically profinite extensions of local fields defined by J.-M. Fontaine and by J.-P. Wintenberger [FoWi] and the results of H. Koch and E. de Shalit, F. Laubie defines recursively a family of arithmetically profinite extensions of K which cover K^{sep}. This leads to a description of Galois groups $G_d(K, \varphi)$, $(d \geq 1)$, of the maximal Galois extensions of K fixed by φ^d, and finally to the group

$$G_k = \varprojlim_{d} G_d(K, \varphi).$$

However, as we discussed at the beginning of this section, a nonabelian generalization of the local reciprocity law would probably be the most natural one. There has also been done some work on this. We saw at the end of chapter 2, that the most important theorem obtained from the local reciprocity law is the existence theorem 2.6.5. In this theorem, a one-to-one correspondence is given, which is described by the reciprocity map. Hence, having a reciprocity map for nonabelian extensions would be a good progress on a nonabelian reciprocity law. Before the local Langlands correspondence, which implies a nonabelian law, was proved, there was some work done by I. Fesenko on this topic.

In [Fe5] I. Fesenko constructs a local reciprocity map for totally ramified arithmetically profinite extensions generalizing the Neukirch and Hazewinkel maps. It is shown that the abelian case is a restricted case of this construction and so is the metabelian class field theory of H. Koch and E. de Shalit, which is proved without the use of the *Coleman homomorphism* or *Lubin-Tate groups.*

However, it describes the reciprocity map, while the Langlands correspondence only gives a statement about having such a map. Nevertheless, the Langlands correspondence states a lot more than just a nonabelian local reciprocity law.

In a later paper [Fe6] from 2005, I. Fesenko discusses a little bit more about the image of such a noncommuative local reciprocity map.

4.3 The Langlands Conjecture

In this section we will state the Langlands conjecture and describe the cases that have already been proved.

The Langlands conjecture can be seen as a very general reciprocity law, generalizing the local and the global case in various ways. The local case has been stated in cases, for archimedian and non-archimedian fields. The local case has been proved by Langlands himself in the case of an archimedian field in [La5]. In this case the formulation of the problem is much simpler. We will, however, not go into detail but focus on the non-archimedian case.

We will try to give the necessary background information to state the local Langlands correspondence properly. The local Langlands correspondence for has been proved by G. Laumon, M. Rapoport and U. Stuhler in 1993 ([LaRaSt]) for non-archimedian local fields of characteristic p and by M. Harris and R. Taylor for characteristic 0 in 2001 ([HaTa]).

The global case for function fields was proved by L. Lafforgue in 2002 ([La2]), who followed the approaches by V. Drinfeld from [Dr2]. L. Lafforgue was awarded the fields medal for his progress on the global Langlands correspondence.

Before we go into detail, let us have a look what is meant by the Langlands correspondence.

Remark 4.3.1. *The Langlands correspondence is a part of a far reaching series of conjectures, called the Langlands program. We will, however, only try to explain the correspondence itself and not go into detail about the program. For a more detailed explaination on the program see for example [Be3].*

4.3.1 The Local Langlands Correspondence

In this subsection we will try to elaborate the local Langlands correspondence. To do so, we need a few more definitions, such as group representations and the Weil group.

Definition 4.3.2. A *representation* of a group G on a vector space V over a field K is a group homomorphism from G to $GL(V)$, the general linear group on V, which is the group of automorphisms of V. That is, a representation is a map

$$\rho : G \to GL(V)$$

such that

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2), \qquad \text{for all } g_1, g_2 \in G.$$

In other words, ρ should be a homomorphism.

Given two such representations, we need to define, when we consider them to be the same.

Definition 4.3.3. Given two K vector spaces V and W, two representations

$$\rho_1 : G \to GL(V)$$

and

$$\rho_2 : G \to GL(W)$$

are said to be *equivalent* or *isomorphic* if there exists a vector space isomorphism

$$\alpha : V \to W$$

so that for all g in G

$$\alpha \circ \rho_1(g) \circ \alpha^{-1} = \rho_2(g).$$

For stating the Langlands correspondence correctly we will also need irreducible represenations. To understand them, we need to define, that we want our group G to act on V in a usual way[4].

Definition 4.3.4. A subspace W of V that is fixed under the group action is called a *subrepresentation*. If V has exactly two subrepresentations, namely the zero-dimensional subspace and V itself, then the representation is said to be *irreducible*.

For more information on group representations see [FuHa].

To give a first idea of what we demand in the local Langlands correspondence, we need to define the Weil group.

Assume that F is a p-adic local field, i.e. a finite extension of $\mathbb{Q}_p$ for some prime p. Let the ring of integers be $\mathcal{O}_F$. This ring has a unique maximal ideal, necessarily principal, and we let π be any generator, a so-called *prime element*. Denote by q the cardinality of the residue field $k = \mathcal{O}_F/(\pi)$[5]. We can also see easily that a Galois automorphism $\tau \in \mathrm{Gal}(\overline{F}/F) = G_F$ induces an automorphism $\overline{\tau}$ of the residue field $\overline{k}$ of $\overline{F}$. The map $\tau \mapsto \overline{\tau}$ is surjective.

Definition 4.3.5. The *Weil group* is defined as the dense subgroup of Galois automorphisms τ such that $\overline{\tau}$ is of the form $x \mapsto x^{q^m}$ for some integer m.

We also know that $\mathrm{Gal}(\overline{k}/k)$ is isomorphic to $\hat{\mathbb{Z}}$. Therefore we can see that the kernel of the map $\tau \mapsto m$ is a closed subgoup of $\mathrm{Gal}(\overline{F}/F)$, called the *inertia subgroup I_F* of F[6]. An element τ mapping to $m = 1$ is called a *Frobenius automorphism*. In any case we have an isomorphism

$$W(\overline{F}/F) \simeq \mathbb{Z} \times I_F$$

and we use this to make $W(\overline{F}/F)$ into a topological group, taking the product of the discrete topology on $\mathbb{Z}$ and relative topology from $\mathrm{Gal}(\overline{F}/F)$ on I_F[7]. With this definition, the restriction r' of the reciprocity map induces an isomorphism of topological groups

$$r' : F^* \to W(\overline{F}/F)^{ab}.$$

Before we proceed, we need to at least define what character groups are.

[4] See the appendix for more information on group actions.

[5] If we look closely, we see that this residue field coincides with the residue field defined in the first chapter.

[6] We will not elaborate this in detail, as we are only trying to give a general idea about the Langlands correspondence. For more detailed information about this see for example [Wi1].

[7] For the topology on profinite groups see [Wi1].

Definition 4.3.6. Let G be an arbitrary group. A complex-valued function f defined on G is called a *character* of G if f has the multiplicative property

$$f(ab) = f(a)f(b)$$

for all a, b in G, and if $f(c) \neq 0$ for some c in G.

We now consider the isomorphism of character groups

$$\sigma_1 : \mathrm{Hom}(F^*, \mathbb{C}^*) \to \mathrm{Hom}(W(\overline{F}/F), \mathbb{C}^*)$$

induced by r'. Now, considering the above, we could show that an irreducible representation is the nonabelian generalization of a character. Hence we define $\mathcal{G}_n$ to be equivalence classes of irreducible n-dimensional representations of $W(\overline{F}/F)$ for all $n \geq 1$.

Remark 4.3.7. *In the first case that Langlands showed ([La5]), the one for a local archimedian field, $\mathcal{G}_n$ is either trivial or $\mathbb{Z}/2\mathbb{Z}$.*

Before we can state the local Langlands correspondence we need a few more terms on representations. We use $G = \mathrm{GL}_n(F)$ and let (π, V) be a representation of G on a complex vector space V. It can be shown that G has a family of open compact subgroups $\{K_m\}_{m \geq 1}$.

Definition 4.3.8. A representation (π, V) is *admissible* if

1. every vector $v \in V$ is fixed by K_m for some m
2. the subspace of vectors fixed by each K_m is finite dimensional.

Remark 4.3.9. *We could also show that to each irreducible unitary representation (π', V') there is attached an admissible representation (π, V) in a natural way.*

We now get to the last definition we need to state the Langlands correspondence.

Definition 4.3.10. A representation π is called *supercuspidal* if the support of every matrix coefficient is compact modulo the center of G.

Now the **Local Langlands Correspondence** asserts that for all n, there exists a natural bijection

$$\sigma_n : \mathcal{C}_n \to \mathcal{G}_n,$$

where $\mathcal{C}_n$ is the set of equivalence classes of supercuspidal representations of $G = \mathrm{GL}_n(F)$. We can now also see, why this really is a generalization of the local reciprocity law. To see this, we consider the case $n = 1$ and then we basically get back to the reciprocity map r'.

This does not seem to complicated. But the key of the Langlands correspondence is in the word **natural**. To be able to see where we are going with this, we need to explain what is meant by 'natural'. This is where the L-function and the ϵ-factor are introduced. We aim to introduce factors, such that σ_n is defined uniquely.

We now proceed to introducing the Hecke L-function. Generally, L-factors generalize the individual factors of the Euler product representation of the Riemann zeta function $\zeta(s)$, such that

$$L(s) = \prod_{p \ \ odd, \ \ prime} \frac{1}{1 - \chi^{-}(p)p^{-s}}$$

where

$$\chi^{-}(p) \equiv \left\{ \begin{array}{rl} 1 & \text{for } p \equiv 1 \bmod 4 \\ -1 & \text{for } p \equiv 3 \bmod 4 \end{array} \right\} = \left(\frac{-1}{p} \right).$$

In a similiar way we can attach an L-function to each continuous homomorphism

$$\chi : \mathbb{A}_F^*/F^* \to \mathbb{C}^*.$$

Such a homomorphism is called a *Hecke character*. Such a Hecke character gives rise, by restriction, to a homomorphism $\chi_v : F_v^* \to \mathbb{C}^*$ for all places v of F. Then the *Hecke L-function* is defined as an infinite product

$$L(s, \chi) = \prod_v L(s, \chi_v)$$

of local factors $L(s, \chi_v)$.

Hecke proved that they satisfy a global functional equation of the form

$$L(s, \chi) = \epsilon(s, \chi) L(1 - s, \chi^{-1})$$

for some factor $\epsilon(s, \chi)$. This is where we introduce the second factor we need to state the Langlands correspondence properly, the *ϵ-factors*.

Now, using the so-called *ζ-integrals*, we could describe the Hecke L-function on representations. It was shown by G. Henniart ([He2]) that the following statement of the local Langlands correspondence defines σ_n uniquely.

Remark 4.3.11. *To prove the uniqueness G. Henniart attached pairs to the L-function and the ϵ-factor. But as it gets even more complicated using this, we omit more information on them here.*

If π is an irreducible representation of $\mathrm{GL}_n(F)$, then there is a character ω_π of Z, called the *central character of* π connected to π. We regard ω_π as a character of F^*.

Theorem 4.3.12 (Local Langlands Correspondence, [Ro1])**.** *There exists a unique family of bijections*

$$\sigma_n : \mathcal{C} \to \mathcal{G}_n$$

for $n \geq 1$ satisfying the following conditions:

1. *σ_1 is the correspondence of abelian local class field theory.*
2. *For all pairs $\pi \in \mathcal{C}_n$ and $\pi' \in \mathcal{C}'_n$, we have*

$$L(s, \pi \times \pi') = L(s, \sigma_n(\pi) \otimes \sigma_{n'}(\pi'))$$

and

$$\epsilon(s, \pi \times \pi') = \epsilon(s, \sigma_n(\pi) \otimes \sigma_{n'}(\pi')).$$

3. For all $\pi, \sigma_1(\omega_\pi) = det(\sigma_n(\pi))$.

Now, having stated the Langlands correspondence, we can get back to what happend recently. As already discussed in the introduction, the local correspondence for fields of characteristic p has been shown by G. Laumon, M. Rapoport and U. Stuhler in 1993 ([LaRaSt]). This paper contains basic and profound work on so-called *$\mathcal{D}$-elliptic sheaves*. By properties of them and using the cohomology of *moduli spaces* he accomplishes to prove a reciprocity law generalizing the one given in a paper by Drinfelds ([Dr1]) where he proved the 2-dimensional case with the same methods. As a consequence, the authors find enough representations to establish the basic local Langlands conjecture for GL_d, d arbitrary, of a local field of equal characteristic. This was the prove of the case where the ground field has characteristic p.

Later, in 2001, M. Harris and R. Taylor succeded in proving the case for non-archimedian fields of characterisic 0 ([HaTa]). Basically, they generalized an approach by P. Deligne ([De]) and H. Carayol ([Ca]) of a study of elliptic modular curves and *Shimura curves* at *primes of bad reduction.* A few months after this was published, G. Henniart found a simpler and more elementary proof in preparing lectures on the topic ([He3]). To keep things simple, we would only like to go a little into Henniarts proof. Let F be a finite extension of $\mathbb{Q}_p$. For each integer $n \geq 1$, we construct a bijection from the set $\mathcal{G}_F^0(n)$ of isomorphism classes of irreducible degree n representations of the Weil group of F, onto the set $A_F^0(n)$ of isomorphism classes of *smooth* irreducible supercuspidal representations of $\mathrm{GL}_n(F)$. Those bijections preserve ϵ-factors for pairs, as briefly mentioned in remark 4.3.11, and hence he obtains a proof of the Langlands conjectures for GL_n over F, which is more direct than M. Harris and R. Taylors.

Those two cases complete the proof of the local Langlands correspondence. Before that, Henniart already covered several other cases ([He1, He4]). In order to complete the local Langlands correspondence one needs to consider all suitable representations of the so-called *Weil-Deligne group* on the Galois theoretic side and all irreducible admissible representations of $\mathrm{GL}_n(k)$ on the other side. This is where we are facing a problem with the global Langlands correspondence, since this *Weil-Deligne group* has no global equivalence. A nice overview on this can be found for example in [Cog].

4.3.2 The Global Langlands Correspondence

In this subsection we will state the Langlands correspondence for global fields. Then we will give a short summary on the progress of proving it. Of course as the local Langlands correspondence, the global correspondence should be a generalization of the global reciprocity law. We will follow J.W. Cogdell ([Cog]) and formulate the global Langlands correspondence separately for characteristic p and 0.

Global fields of positive characteristic The formulation of the global Langlands conjecture by Drinfeld and Lafforgue is essentially the same as in the local nonarchimedian case. Although a few modifications are made.

To describe the global case, we need another definition.

Definition 4.3.13. Let ρ be a Galois representation for K with representation space A. We say that ρ is *unramified* if the inertia group I_K acts trivially on A.

In the case of a field of characteristic p, on the Galois side we consider a set $Rep_n^0(\mathcal{G}, \overline{\mathbb{Q}}_l)_f$. This set should be the isomorphism classes of irreducible continuous l-adic representations $\rho : \mathcal{G}_k \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ which are unramified outside a finite number of places and have a determinant of finite order.

On the other side we have a set $\mathcal{A}_n^0(k; \overline{\mathbb{Q}}_l)$, the space of some $\overline{\mathbb{Q}}_l$-valued *cuspidal* representations.

Then we can state the global Langlands correspondence as follows:

Theorem 4.3.14 (Global Langlands Correspondence for characteristic $p > 1$)**.** *For each $n \geq 1$ there exists a bijective map $\mathcal{A}_n^0(k; \overline{\mathbb{Q}}_l)_f \to Rep_n^0(\mathcal{G}_k, \overline{\mathbb{Q}}_l)_f$, denoted $\pi \mapsto \rho_\pi$ with the following properties:*

1. *For $n = 1$ the bijection is given by global class field theory.*
2. *For any $\pi \in \mathcal{A}_n^0(k; \overline{\mathbb{Q}}_l)_f$ and $\pi' \in \mathcal{A}_{n'}^0(k; \overline{\mathbb{Q}}_l)_f$, we have*
$$L(s, \rho_\pi \otimes \rho_{\pi'}) = L(s, \pi \times \pi')$$
and
$$\epsilon(s, \rho_\pi \otimes \rho_{\pi'}) = \epsilon(s, \pi \times \pi').$$
3. *For any $\pi \in \mathcal{A}_n^0(k; \overline{\mathbb{Q}}_l)_f$ the determinant of ρ_π corresponds to the central character of π under global class field theory.*
4. *The global bijections should be compatible with the local bijections of the local Langlands correspondence.*

Those are, mainly, the most important statements for the global Langlands correspondence. There would be two other conditions, but as those would not give any more information to understand what we are trying to say, they are omitted here. For a complete list of conditions see [Cog].

Fields of positive characteristic In this case the conjectured correspondence looks a little bit different. First, if k is a global field, let us denote its ring of adeles by $\mathbb{A}$. As already mentioned above, there is no global form of the Weil-Deligne group. So for a more general approach, we need a global analogue. But unfortunately no such analogue is available. Instead the conjectures are envisioned in terms of a conjectural *Langlands group* $\mathcal{L}_k$ by D. Ramakrishnan ([Ra]). This conjectured group should fit into a commutative diagram with another conjectural group, the *motivic Galois group*[8].

First a definition of a term that will occur in the text below. However, it will give no extra information as we are only trying to give a very general idea of things. But to make the subject a little less confusing, we will add this definition.

[8] This group is also conjectured by D. Ramakrishnan in [Ra].

Definition 4.3.15. A *modular form* is a (complex) analytic function on the upper half-plane satisfying a certain kind of functional equation and growth condition[9].

Based on the above definition we obtain the following term:

Definition 4.3.16 (Automorphic Form)**.** The general notion of *automorphic form* is the extension to analytic functions, perhaps of several complex variables, of the theory of modular forms.

In these terms, in general it is conjectured (in [Ra] and [Cl]) that we have the following types of global correspondences:

1. The irreducible n-dimensional representations of $\mathcal{G}_k$ should be in bijective correspondence with the cuspidal representations of $\mathrm{GL}_n(\mathbb{A})$ of Galois type.

2. The irreducible n-dimensional representations of $\mathcal{M}_k$ should be in bijective correspondence with the *algebraic* cuspidal representations of $\mathrm{GL}_n(\mathbb{A})$. These are analogues of algebraic Hecke characters.

3. The irreducible n-dimensional representations of $\mathcal{L}_k$ should be in bijective correspondence with all cuspidal representations of $\mathrm{GL}_n(\mathbb{A})$.

Of course, all of these correspondences should satisfy properties similar to those on the local conjectures, particularly the preservation of L- and ϵ-factors (with some twists), compatibility with the local correspondences, etc.

There is very little known about this case. However, there are many partial results of a general nature if we start on the automorphic side and try to reconstruct the associated Galois representation.

When $n = 2$ and $k = \mathbb{Q}$, P. Deligne ([De]) associated to every cuspidal representation π of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ with certain properties a compatible system of ℓ-adic representations. This was extend later by P. Deligne and J.P. Serre ([DeSe]). Again, this work was extend to totally real fields k, but still with $n = 2$ by a number of people[10]. The case with k an imaginary quadratic field is also already covered.

Although there has also been done work on the other direction, starting with a specific Galois representation and showing that it is modular, there is no general result.

The most important progress in the case of a field of characteristic p has been made by L. Lafforgue ([La1]). He proves Langlands correspondence for GL_r over function fields. His proof is a generalization of Drinfeld's proof ([Dr2]) in the case of rank 2.

To close this section we are trying to briefly elaborate the work that has been done on the compatibility of the local and the global Langlands correspondence. This is an important part of the Langlands correspondence, as the global case demands to be compatible with

[9] For a real definition see [La3].

[10] See [Cog] for a list of them.

the local correspondence. This mostly covers work on special cases, as there is no general proof of the global Langlands conjecture. But for example J. Bellaiche ([Be]) proved the following:

Let π be an automorphic representation of the unitary group $U(3)$, the group of all unitary matrices. For l a prime, let ρ_l be the l-adic Galois representation attached to π. Then J. Bellaiche showed that, up to *semisimplification*, ρ_l gives the representation predicted by the local Langlands correspondence at every finite place for a *density one set* of primes l. In his proof he also used the work of M. H. Harris and R. L. Taylor ([HaTa]), who proved the same result for $U(n)$ under some assumptions, namely up to *semisimplification*, that are not required in J. Bellaiche's proof anymore.

Based on the results of M.H. Harris and R. Taylor ([HaTa]), R Taylor and T. Yoshida succeded in 2006 in proving the compatibility of local and global Langlands correspondences for GL_n ([TaYo]).

We conclude this section with this information. Hopefully, we succeded in trying to give an idea of what the the Langlands correspondence is. For more information see any of the books published on the Langlands program. We would also like to mention that there is also a geometric way of describing the Langlands correspondence. This can already be assumed by the things that were used in several proofs, as some of the important work has been done using for example *elliptic sheaves* and of course modular forms.

4.4 Constructions and Applications

In this section we will give a few examples on constructions of class fields and results obtained from class field theory.

4.4.1 Class Field Towers

In this first subsection we will explain the *class field tower problem.*

Definition 4.4.1. Given a number field K, there exists a unique maximal unramified abelian extension L of K which contains all other unramified abelian extensions of K. This finite field extension L is called the *Hilbert class field* of K.

In these terms the *class field tower problem* can be stated as follows:

Class Field Tower Problem Given a number field K we construct a class field tower:

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots ,$$

where K_{i+1} is the Hilbert class field of K_i. Now the problem is, if this tower stops after a finite number of steps. A positive answer would have the implication that the last field in the tower had class number 1. This would mean, that in it all ideals of K - actually all ideals from $K_{i_{max}}$ itself - would become principal.

However, this problem was decided in the negative by E.Golod and I. Safarevich in 1964 ([GoSa]). The main theorem of their result can be stated as follows:
Let k be a finite extension of the rational field $\mathbb{Q}$, and p a prime number.We denote by γ the minimal number of generators of the p-Sylow subgroup of the divisor class group[11] and by ρ the minimal number of generators of the unit group. The principal theorem is that, if $\gamma \geq 3 + 2(\rho + 2)^{\frac{1}{2}}$, then there exists an infinite Galois p-extension of k such that all prime divisors are unramified over k. The simplest example for this is the field

$$\mathbb{Q}(\sqrt{4849845}).$$

The result of E. Golod and I. Safarevich gives a specific description, under which conditions such infinite class field towers occur. This was specified with the p^n*-rank* of a group. To properly define this rank, we need a theorem from Kronecker:

Theorem 4.4.2 (Kronecker)**.** *Every finite Abelian group can be written as a group direct product of cyclic groups of prime power group orders.*

Definition 4.4.3. For any prime number p and any positive integer n, the p^n*-rank*, denoted by $r_{(p^n)}(G)$ of a finitely generated abelian group G is the number of copies of the cyclic group Z_{p^n} (or C_{p^n}) appearing in the Kronecker decomposition of G.

[11] For an explaination of the divisor class group see [Ne2].

For our next definition, we need to explain p-class field theory a little bit.

Let P be a set of prime numbers and let G be a pro-P-group, i.e. a profinite group all of whose quotients G/N by open normal subgroups N have order divisible only by primes in P^{12}.
Let $d : G \to \mathbb{Z}_P$ be a surjective homomorphism onto the group $\mathbb{Z}_P = \prod_{p \in P} \mathbb{Z}_P$, and let A be a G-module. A *Henselian P-valuation* with respect to d is by definition a homomorphism

$$v : A_k \to \mathbb{Z}_P$$

which satisfies the following properties:

1. $v(A_K) = Z \supseteq \mathbb{Z}$ and $Z/nZ \simeq \mathbb{Z}/n\mathbb{Z}$ for all natural numbers n which are divisible only by primes in P,
2. $v(N_{K|k}A_K) = f_K Z$ for all finite extensions $K|k$, where $f_K = (d(G) : d(G_K))$.

Definition 4.4.4. Now, under these terms, a *p-class field* is the class field asigned to a field extension when we have G is of course our Galois group and the G-module A_K is given by k^*.

Remark 4.4.5. *In this case we use r_k instead of r_{p^n} because p^n is unique here.*

Definition 4.4.6. Let K be an algebraic number field and p a prime number. Let $K^{(0)} = K$ and $K^{(i)}$ denote the Hilbert p-class field of $K^{(i-1)}$ for $i \geq 1$. The tower

$$K^{(0)} = K \subseteq K^{(1)} \subseteq \cdots \subseteq K^{(\infty)} = \bigcup_{i \geq 0} K^{(i)}$$

is called the *p-class field tower* of K.

Now in these terms, the result can be summerized as: Let k be an imaginary quadratic number field. If $r_k \geq 5$, then k has an infinite 2-class field tower.

Following this condition, there has been done a lot of work lately to give other criteria for such infinite class field towers on other fields.

For example, E. Benjamin ([Be1]) elaborated sufficient conditions for imaginary quadratic number fields k with $r_k = 4$ to have infinite 2-class field towers, thus proving special cases of the conjecture by J. Martinet ([Ma4]) according to which an imaginary quadratic number field k satisfying $r_k = 4$ has an infinite 2-class field tower.

There has been more recent research on this conjecture, covering more special cases by Y. Sueyoshi ([Su]). In this paper, he investigates J. Martinet's conjecture for fields K whose discriminant is divisible by exactly one negative prime discriminant, and shows that many of these fields have an infinite Hilbert 2-class field tower. In particular, under the hypotheses already stated, if the 4-class rank of K is positive, then the Hilbert 2-class field tower of K is infinite.

[12] For more explaination on profinite groups see the Introduction, the Appendix and [Wi1].

A. Mouhib focusses on the case where K is real quadratic and $r_2 = 4$. In this special situation, C. Maire ([Ma1]) proved that K has an infinite 2-class field tower when the 4-rank r_4 is 4. His main results assert that the 2-class field tower of a real quadratic number field is infinite under the sufficient conditions $r_4 \geq 4$ and $r_4^+ \geq 3$, where r_4^+ denotes the 4-rank of the so-called *narrow 2-class group.*

Similiarly, there have been results on 3-class field towers as well. As for example by E. Yoshida ([Yo]) on *biquadratic* fields. The paper gives a necessary and sufficient condition for the 3-class field tower of K to terminate at $K^{(1)}$, when the extension $K/\mathbb{Q}$ is biquadratic and contains $\sqrt{-3}$.

It is a nice result, that even very naturally occuring fields, such as $\mathbb{Q}(\zeta_m)$, can have infinite class field towers. Due to a paper from I. Shparlinski from 2008 ([Sh1]), we have the following result:
For a positive integer m, let $\zeta_m = e^{\frac{2\pi i}{m}}$ and $K_m = \mathbb{Q}(\zeta_m)$ denote the m-th cyclotomic field. For an integer $v \geq 1$ and a real number $x > 1$ he defines $\log_v x$ inductively by

$$\log_1 x = \max\{\log x, 1\},$$

where $\log x$ is the natural logarithm and

$$\log_v x = \max\{\log(\log_{v-1} x), 1\} \quad \text{for} \quad v > 1.$$

The main result is that for x sufficiently large and all $m \leq x$, except for possibly $O(x \log_2 x)^{-0.08}$ values, K_m has an infinite Hilbert p-class field tower.

In contrast to this, A. Nomura ([No]) had a look on the case of a cyclic cubic field. He gives conditions under which we have a non-trivial class field tower.

Definition 4.4.7. Such a *biquadradic* extension of a field F is a Galois extension K of F such that $\mathrm{Gal}(K/F)$ is isomorphic to the *Klein-4-group.*

Remark 4.4.8. *We will now need the term of the* genus field*. Since this is an important term in class field theory, we would like to give its definition.*

Definition 4.4.9. The *genus field* G of a number field K is the maximal abelian extension of K which is obtained by composing an absolutely abelian field with K and which is unramified at all finite primes of K. The *genus number* of K is the degree $[G : K]$ and the *genus group* is the Galois group of G over K.

Let $l_p(K)$ be the length of the tower, that is, the least non-negative integer n such that $K_n^{(p)} = K_{n+1}^{(p)}$. He specialized to the case where $p = 3$. The primary result of the paper is a sufficient condition for when $l_3(K) > 1$ in this case. Let $m(K)$ be the number of rational primes ramified in $K/\mathbb{Q}$. First, he shows that if $m(K) > 3$, then $l_3(K) > 1$. The he states and proves the main result, which asserts that if $m(K) = 3$, then $l_3(K) > 1$ if and only if the class number of the *genus field* of K is divisible by 3.

There has also been done some work in another direction, namely classifying fields that have an abelian p-class field tower by K. Okano ([Ok]). In this paper he classifies the imaginary quadratic fields whose cyclotomic $\mathbb{Z}_p$-extensions have abelian p-class field towers in the case where p is odd.

As a result, we see, that even though the very interesting class field tower problem has been solved, there has been done a lot of work on class field towers lately. The above mentioned articles cover only special cases, hence there are still open questions concerning class field towers.

4.4.2 Computations and Applications

One very important assertion of class field theory is the existence theorem. It states, that to a given subgroup, we can assign a field extension. Unfortunately, it does not give any information about how this extension looks like. As a first part of this subsection, we will briefly summerize recent approaches to computing these class fields.

There exist very satisfactory algorithms to compute the discriminant, the ring of integers and the class group of a number field, and especially of a quadratic field. For the computation of the Hilbert class field, however, there exists an efficient version only for complex quadratic fields, using complex multiplication, and a general method for all number fields, using *Kummer theory*, which is not really satisfactory except when the ground field contains enough roots of unity.
However, there is a paper by H. Cohen and X. Roblot ([CoRo]), which gives an idea for real quadratic fields. In this paper, they explore a third way, available for totally real fields, which uses the units appearing in *Stark's conjectures*[13], the so-called *Stark units*, to provide an efficient algorithm to compute the Hilbert class field of a real quadratic field. This method relies on the truth of *Stark's conjecture* (which is not yet proved!). Although, they can prove independently of the conjecture that the field obtained is indeed the Hilbert class field.

Another approach by S. Pauli ([Pa4]) gives a way of constructing the finite extension L/K associated to a subgroup G of K^* in the case of a local field K, an extension of $\mathbb{Q}_p$, a p-adic field.

If G contains the group $U_1(K)$ of 1-units of K the extension L/K is tamely ramified (or unramified). The construction of L is straightforward in this case. If G has index p in K^* and G is not contained in $U_1(K)$ then L/K is a wildly ramified $\mathbb{Z}/p\mathbb{Z}$-extension, and hence is generated by a root of one of the polynomials given by S. Amano [Am]. In the paper by S. Pauli an algorithm is given for determining which *Amano polynomial* corresponds to a specified index-p subgroup $G \leq K^*$. It is then shown how the constructions for L in these two special cases may be used to construct the extension L/K corresponding to an arbitrary closed subgroup G of K^* with finite index.

The above paper covers the local case. But there is also an algorithm by C. Fieker ([Fi]) to compute class fields in the global case. He does so by reducing the problem to the

[13] For an explaination of them pleae see for example a book from J. Tate [Ta], who extended the original conjectures from Stark to its present form.

construction of cyclic extensions of prime power degree p^r whose compositum is the field L, which is the abelian extension according to the existence theorem[14].

To conclude this section, we would like to give a few examples of results that have been obtained using the assertions from class field theory.

As a first result, we would like to point at an article by H. Cohen, F. Diaz y Diaz and M. Oliver ([CoDiOl]). To see what they obtained, we need a little introduction to the subject. Let K be a number field, and let G be a transitive subgroup of the symmetric group S_n. The *inverse problem of Galois theory* asks whether there exists an extension L/K of degree n such that the Galois group of the Galois closure of L is isomorphic to G. This problem is far from being solved. However, we are focusing on the number $N_{K,n}(G,X)$ of such extensions up to K-isomorphism, such that the discriminant of L/K is at most equal to X, at least in some asymptotic sense. A general conjecture due to G. Malle ([Ma2], [Ma3]), states that there should exists constants $a_K(G)$, $b_K(G)$, and $c_K(G)$ such that

$$N_{K,n}(G,X) \sim c_K(G) X^{a_K(G)} \log(X)^{b_K(G)-1}.$$

G. Malle also gave formulas for $a_K(G)$ and $b_K(G)$ (Although it has been shown in the meantime by J. Klueners ([Kl]), that the formula for $b_K(G)$ cannot be applied to every case). Now the currently discussed paper discusses a few special cases for abelian groups. For the case of the cyclic group C_l they need the surjectivity of the local reciprocity map.

Another paper by G. Cornelissen ([Cor]) deals with describtions of class numbers. Let q be an odd prime, e a non-square in the finite field $\mathbb{F}_q$ with q elements, $p(T)$ an irreducible polynomial in $\mathbb{F}_q[T]$ and A the *affine coordinate ring* of the *hyperelliptic curve* $y^2 = ep(T)$ in the (y,T)-plane. They use class field theory to study the dependence on $\deg(p)$ of the divisibility by 2, 4, and 8 of the class number of the Dedekind ring A.

As a last, very nice result obtained from the reciprocity law, we have a look on Mersenne primes.

Definition 4.4.10. A *Mersenne number* is a positive integer that is one less than a power of two

$$M_n = 2^n - 1.$$

A *Mersenne prime* is a Mersenne number that is prime.

H. Lenstra and P. Stevenhagen consider Mersenne primes $M_p = 2^p - 1$ for primes $p \equiv 1 \mod 3$ ([LeSt]). These can be represented in the form $M_p = x^2 + 7y^2$, and it is easily seen that we always have $4 \mid x$. Numerical experiments suggest that in fact $8 \mid x$, and, amazingly, this can be proved using Artins reciprocity law.

[14] In the global case the existence theorem is called the *Takagi theorem.*

Appendix A

Appendix

In this last chapter of this text we give a short summary of algebraic, number theoretic and topological aspects. The selection of topics coverd here should help the reader to follow various proofs and to get a better understanding of some introductions into new topics. For group theory, most parts can be found in [Ro2]. For field and ring theory, see [Hu1] and for algebraic number theory [Ne2].

A.1 Group Theory

In this first section of the appendix we would like to give most of the terms and theorems used from group theory. However, the reader should be familiar with basic group theory. Therefore we will focus on definitions and theorems that are not part of any basic Algebra course. For more information on groups see for example [Ro2].

A.1.1 Definitions and Isomorphism Theorems

In this first subsection we basically list definitions that are used in the text. Those are partly very basic ones, but on the other hand also rarely used ones. Most of what follows can be found in any group theoretic book, unless a reference is given.

Definition A.1.1. A *group* $(G, \cdot)$ is a nonempty set G equipped with an operation '$\cdot$' such that:

1. G is closed under the operation '$\cdot$'
2. '$\cdot$' is an associative operation

   and G contains an element e such that

3. $e \cdot a = a = a \cdot e$ for all $a \in G$
4. for every $a \in G$, there is an element $b \in G$ with

$$a \cdot b = e = b \cdot a.$$

Now, a *subgroup* is a group $(H, \cdot)$, where H is a subset of G and $(G, \cdot)$ is a group. Usually subgroups are denoted by $H \leq G$ or $H < G$.

Remark A.1.2. *We will usually denote the group operation by '$\cdot$'. When not denoting any group operation, we will assume that it is '$\cdot$'. It is also very common to write 'ab' instead of '$a \cdot b$' for $a, b \in G$. However, this will never be subject of any confusion.*

Among subgroups, the normal ones are of high importance:

Definition A.1.3. A subgroup $K \leq G$ is a *normal subgroup*, denoted by $K \lhd G$, if

$$gKg^{-1} = K$$

for every $g \in G$.

Remark A.1.4. *Sometimes a normal subgroup K is defined to have $gKg^{-1} \leq K$. But this is just the same as above. The alternative definition gives one part of the inclusion, and replacing g with g^{-1} lets us deduce $K \leq gKg^{-1}$.*

A group G is called *abelian*, if

$$a \cdot b = b \cdot a \quad \text{for all } a, b \in G.$$

Remark A.1.5. *It is quite easy to see that in an abelian group every subgroup is normal.*

The following term of a group extension could also be defined using exact sequences.

Definition A.1.6. Let two groups A and B be given. A group G is called an *extension* of A by B if G contains a normal subgroup A', isomorphic to A, whose factor group is isomorphic to B,

$$A' \simeq A, \qquad G/A' \simeq B.$$

Note that the extension G is not uniquely determined by giving the groups A and B. Examples can be found in [Ku2]. By a *class of a group extension* we will mean its class of isomorphic groups.

Since we will need this term, we will also define what the free abelian group is. This should not be confused with a free group in general.

Definition A.1.7. An abelian group F is *free abelian* if it is a direct sum of infinite cyclic groups. More precisely, there is a subset $X \subset F$ of elements of infinite order, called a *basis* of F, with $F = \sum_{x \in X} \langle x \rangle$ i.e. $F \simeq \sum \mathbb{Z}$.

For a group we can define the center, which is trivial in the abelian case.

Definition A.1.8. The *center* of a group G, denoted by $Z(G)$, is the set of all $a \in G$ that commute with every element of G. Namely,

$$Z(G) = \{a \in G \mid ag = ga \quad \text{for all } g \in G\}.$$

For an abelian group, we obviously have $Z(G) = G$.

Normal subgroups have the property, that left and right cosets coincide. We can therefore consider a new group G/N for a normal subgroup N and a group G. It is quite easy to see that this really is a group. The elements of this group are denoted by gN for $g \in G$. In this case g is called a representative of the coset gN.

Definition A.1.9. Let $(G, \cdot)$ and $(H, \circ)$ be groups. A function $f : G \to H$ is a *group homomorphism*, if for all $a, b \in G$

$$f(a \cdot b) = f(a) \circ f(b).$$

An *isomorphism* is a homomorphism that is also a bijection. We say that G is *isomorphic* to H, denoted by $G \simeq H$, if there exists an isomorphism $f : G \to H$.

The subgroup K of G with $f(K) = \{0\}$ is called the *kernel* of f and denoted by $\ker f$.

With this in mind, we can state the important *isomorphism theorems*:

Theorem A.1.10 (First Isomorphism Theorem)**.** *Let G, H be groups and*

$$f : G \to H$$

a homomorphism with kernel K. Then K is a normal subgroup of G and

$$G/K \simeq \mathrm{im} f.$$

Theorem A.1.11 (Second Isomorphism Theorem)**.** *Let N and T be subgroups of G with N normal. Then $N \cap T$ is normal in T and*

$$T/(N \cap T) \simeq NT/N.$$

Theorem A.1.12 (Third Isomorphism Theorem)**.** *Let $K \leq H \leq G$, where both K and H are normal subgroups of G. Then H/K is a normal subgroup of G/K and*

$$(G/K)/(H/K) \simeq G/H.$$

Next we will define a class of groups, which is close to abelian groups. But to do so, we need commutators.

Definition A.1.13. If $a, b \in G$, the *commutator* of a and b, denoted by $[a, b]$ is

$$[a, b] = aba^{-1}b^{-1}.$$

The *commutator subgroup* (or derived subgroup) of G, denoted by G', is the subgroup of G generated by all the commutators of G.

Theorem A.1.14. *The commutator subgroup G' is a normal subgroup of G. Moreover, if $H \lhd G$, then G/H is abelian if and only if $G' \leq H$.*

Similiar to the commutator subgroup, we can proceed defining:

$$G^{(0)} = G,\ \ G^{(1)} = G' \text{ and recursively } G^{(i+1)} = \left(G^{(i)}\right)'.$$

Obviously we have

$$G \geq G' \geq G^{(2)} \geq G^{(3)} \geq \cdots,$$

and of course all groups $G^{(i)}$, the so-called *higher derived groups*, are characteristic subgroups of G. A *characteristic subgroup* is a subgroup K of G, where every automorphism from G maps K into itself.

Definition A.1.15. A group G is *soluble*, if $G^{(k)} = \{e\}$ for some $k \in \mathbb{N}$.

Now a group G is called *metabelian*[1], if G is soluble with $G^{(2)} = \{e\}$.

Remark A.1.16. *Soluble groups are of high interest in group theory, but also in Galois theory. For example, solubility is used to prove that there can be no formula to solve equations of degree greater than* 4. *This is a theorem by Abel.*

An abelian group D is called *divisible* if every element $d \in D$ has an n-th root in D. That is, for every $n > 0$, there exists $x \in D$ with $x^n = d$.
An easy observation shows that, D is divisible if and only if $D^n = D$ for every positive n.

In these terms, we say a group is *p-divisible*[2] if $D^{p^k} = D$ for every positive integer k. Since $D^{p^k} = \underbrace{D \cdot \cdots \cdot D}_{p \text{ times}}$, it is obvious that p-divisibility is implied by $D^p = D$.

Theorem A.1.17. *A group G is divisible if and only if it is p-divisible for every prime p.*

For the next definition, we need to make the following observation. Given any element $g \in G$, we define a map

$$\alpha_g : G \to G$$

as follows:

$$\alpha_g(a) \mapsto gag^{-1}.$$

This map is an automorphism of G, called an *inner automorphism*.

Definition A.1.18. A group G is called *complete* if every automorphism of G is an inner automorphism and it has trivial center, $Z(G) = 1$.

To close this subsection, we would like to give one last definition, that is a little bit out of the context.

Definition A.1.19. A subgroup G of the symmetric group S_n is said to be *transitive*[3] if given any $i \neq j$ $(1 \leq i, j \leq n)$, there exists $\sigma \in G$ such that $\sigma(i) = j$.

[1] [Hu2]
[2] [Fu1]
[3] [Hu1]

A very helpful tool in investigating groups are exact sequences.

Definition A.1.20. A sequence of groups A_i and homomorphisms f_i

$$\cdots \to A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} A_4 \to \cdots$$

is an *exact sequence* if the image of each map is the kernel of the next map. A *split exact sequence* is an exact sequence of groups A, B, C and homomorphisms f, g of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

This definition asserts, that f must be an injective homomorphism and g must be a surjective one. This is usually denoted as

$$A \hookrightarrow B \twoheadrightarrow C.$$

A.1.2 Sylow Theorems and p-Groups

We will now proceed to a very important group theoretic aspect of finite groups, the Sylow theorems. Hence for the next paragraphs, we will assume G to be a finite group. Most parts of this section are from [Ro2], but can also be found in any other group theoretic book.

When having a first look at the statement of the Sylow theorems, we would not suggest that the method of proving them needs the action of a group on a set. Hence, and because we also need it to properly define group representations, we will give an idea of what is meant by this.

Definition A.1.21. If X is a set and G is a group, then X is a *G-set* if there is a function $\alpha : G \times X \to X$, denoted by

$$\alpha : (g, x) \mapsto gx,$$

such that:

1. $e \cdot x = x$ for all $x \in X$, where e denotes the unity element of G,

2. $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$.

It is very common to say that G *acts* on X.

Remark A.1.22. *It is very common to denote $g(x)$ as x^g.*

A very commonly used action is *conjugation.* This is, when a group G or a subgroup $H \leq G$ acts on itself by $gx \mapsto gxg^{-1}$. Given this action, we define:

Definition A.1.23. If $a \in G$, then the *centralizer* of a in G, denoted by $C_G(a)$, is the set of all $x \in G$ which commute with a:

$$C_G(a) = \{x \in G \mid xa = ax\}.$$

It is immediate that $C_G(a)$ is a subgroup of G.

Definition A.1.24. If $H \leq G$ and $g \in G$, then the *conjugate* gHg^{-1} is

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

The conjugate gHg^{-1} is often denoted by H^g.

The conjugate is a subgroup isomorphic to H. Normal subgroups are themselves of course their only conjugates.

Definition A.1.25. If $H \leq G$, then the *normalizer* of H in G, denoted by $N_G(H)$, is

$$N_G(H) = \{a \in G : aHa^{-1} = H\}.$$

It is immediate that $N_G(H)$ is a subgroup of G. An easy observation shows that $H \lhd N_G(H)$. Indeed, $N_G(H)$ is the largest subgroup of G in which H is normal.

Definition A.1.26. If X is a G-set and $x \in X$, then the *stabilizer* of x, denoted by G_x is the subgroup

$$G_x = \{g \in G \mid gx = x\} \leq G.$$

The order of a group G has consequences for its structure. Usually the more complicated the prime factorization of $|G|$, the more complicated the group. The Sylow theorems are statements about certain subgroups of a group with a given finite order.

Definition A.1.27. If p is a prime, then a *p-group* is a group in which every element has order a power of p.

The following gives part of the inner structure of G, and would also be used to prove the Sylow theorems.

Theorem A.1.28 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Corollary A.1.29. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Theorem A.1.30. *If $G \neq 1$ is a finite p-group, then its center $Z(G) \neq 1$.*

Similiar to p-groups, we can define p-subgroups of a group G, with $p \mid |G|$.

Definition A.1.31. For a prime p, a *p-subgroup* H is a subgroup of a group G, with $p \mid |G|$ and H is a p-group.

Among p-subgroups, there are certain ones of special interest.

Definition A.1.32. If p is a prime, then a *Sylow p-subgroup* P of a group G is a maximal p-subgroup.

We now proceed stating, for completness reasons, the Sylow theorems:

Theorem A.1.33 (Sylow, 1892)**.** *If P is a Sylow p-subgroup of a finite group G, then all Sylow p-subgroups of G are conjugate to P.*

The next theorem gives an idea about the number of Sylow p-subgroups.

Theorem A.1.34 (Sylow)**.** *If there are r Sylow p-subgroups, then r is a divisor of $|G|$ and $r \equiv 1 \mod p$.*

The following theorem asserts the existence of Sylow p-subgroups.

Theorem A.1.35 (Sylow)**.** *If G is a finite group of order $p^n m$, where $(p, m) = 1$, then G has a subgroup of order p^n.*

A.2 Ring Theory

In this section we will summerize basic definitions and theorems about rings that are used in this text.

Definition A.2.1. A *ring* is a nonempty set R together with two binary operations (usually denoted as addition $(+)$ and multiplication) such that:

1. $(R, +)$ is an abelian group
2. $(ab)c = a(bc)$ for all $a, b, c \in R$ (associative multiplication)
3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (left and right distributive laws).

   If, in addition:

4. $ab = ba$ for all $a, b \in R$,

   then R is said to be a *commutative ring*. If R contains an element 1_R such that

5. $1_R a = a 1_R = a$ for all $a \in R$,

   then R is said to be a *ring with identity*.

Similiar to subgroups, we can define subrings. Normal subgroups play a special role in group theory. Equivalently, we have ideals in ring theory.

Definition A.2.2. Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R. If S is itself a ring under these operations then S is called a *subring*. A subring I of a ring R is a *left ideal* provided

$$r \in R \quad \text{and} \quad x \in I \quad \Rightarrow rx \in I$$

I is a *right ideal* provided

$$r \in R \quad \text{and} \quad x \in I \quad \Rightarrow xr \in I$$

I is an *ideal* if it is both a left and a right ideal.

In number theory, we are specifically intersted in prime ideals, that mostly play the part of primes in the integers.

Definition A.2.3. An ideal P in a ring R is said to be *prime* if $P \neq R$ and for any ideals A, B in R

$$AB \subset P \ \Rightarrow A \subset P \ \text{ or } \ B \subset P.$$

Theorem A.2.4. *If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$*

$$ab \in P \ \Rightarrow a \in P \ \text{ or } \ b \in P, \tag{A.1}$$

then P is prime. Conversely if P is prime an R is commutative, then P satisfies condition A.1.

Theorem A.2.5. *In a commutative ring R with identity $1_R \neq 0$ an ideal P is prime if and only if the quotient ring R/P is an integral domain.*

From the first chapter on, we are dealing with maximal ideals. They are a nice thing to deal with, as the quotient structure is a field. We use this fact very often.

Definition A.2.6. An ideal M in a ring R is said to be *maximal* if $M \neq R$ and for every ideal N such that $M \subseteq N \subseteq R$, either $N = M$ or $N = R$.

Definition A.2.7. A ring R which has a unique maximal ideal is called a *local ring.*

Next we get some more about invertible elements.

An element a in a ring R with identity is said to be *left [resp. right] invertible* if there exists $c \in R$ [resp. $b \in R$] such that $ca = 1_R$ [resp. $ab = 1_R$. The element c [resp. b] is called a *left [resp. right] inverse* of a. An element $a \in R$ that is both left and right invertible is said to be *invertible* or to be a *unit*.

Lemma A.2.8. *The set of non-invertible elements of a ring R forms a unique maximal ideal M in R.*

The next theorem gives a connection between maximal and prime ideals in commutative rings.

Theorem A.2.9. *If R is a commutative ring such that $R^2 = R$ (in particular if R has an identity), then every maximal ideal M in R is prime.*

We can now have a look at the quotient structures.

Theorem A.2.10. *1. If M is maximal and R is commutative, then the quotient ring R/M is a field.*

2. If the quotient ring R/M is a division ring, then M is maximal.

Remark A.2.11. *A* division ring *is like a field, but the multiplicative operation lacks to be abelian.*

This text uses a certain theorem about ideals in ring extensions. Therefore we need a few definitions.

Definition A.2.12. Let S be a commutative ring with identity and R a subring of S containing 1_S. Then S is said to be an *extension ring* of R.

For number theory, the term 'integral' element is very important.

Definition A.2.13. A polynomial $f(x)$ over a ring R is said to be *monic*, if its leading coefficient is 1.

Definition A.2.14. Let S be an extension ring of R and $s \in S$. If there exists a monic polynomial $f(x) \in R[x]$ such that s is a root of f (that is $f(s) = 0$), then s is said to be *integral* over R. If every element of S is integral over R, S is said to be an *integral extension* of R.

With the above terms, we can define a set

$$\overline{R} = \{s \in S \mid s \text{ is integral over } R\}.$$

This set is called the integral closure of R in S.
A ring R contained as a subring in anothe ring S is said to be *integrally closed in S* if R is its own integral closure in S. If we do not refer to a certain extension ring, and say R is *integrally closed*, we mean R is integrally closed in its field of fractions.

With these terms, we can state the Lying-Over-Theorem that is used in this text.

Theorem A.2.15 (Lying-Over-Theorem)**.** *Let S be an integral extension ring of R and P a prime ideal of R. Then there exists a prime ideal Q in S which lies over P (that is, $Q \cap R = P$).*

Another theorem will prove to be useful in the quite technical proofs of this text.

Theorem A.2.16. *Let S be an integral extension ring of R and let Q be a prime ideal in S which lies over a prime ideal P in R. Then Q is maximal in S if and only if P is maximal in R.*

We close this short section with a Lemma about polynomials.

Definition A.2.17. Let D be a unique factorization domain and $f = \sum_{i=0}^{n} a_i x^i$ a nonzero polynomial in $D[x]$. A greatest common divisor of the coefficients $a_0, a_1, \ldots, a_n$ is called a *content* of f and is denoted by $C(f)$.
If $f \in D[x]$ and $C(f)$ is a unit in D, then f is said to be *primitive*.

The following Lemma about polynomials over rings is due to Gauss.

Lemma A.2.18 (Gauss)**.** *If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) \approx C(f)C(g)$. In particular, the product of primitive polynomials is primitive.*

Lemma A.2.19 (Gauss)**.** *Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.*

A.3 Field Theory

In this section we will summarize a few field theoretic aspects that are widely used in this text.

First, for completeness reasons, the definition of a field.

Definition A.3.1. A nonzero element a in a ring R is said to be a *left [resp. right] zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$ [resp. $ba = 0$]. A *zero divisor* is an element of R which is both a left and a right zero divisor.

A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an *integral domain*. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a *division ring*. A *field* is a commutative division ring.

A commonly used criteria to classify fields is their characteristic. We will define it, however, generally for rings.

Definition A.3.2. Let R be a ring. If there is a least positive integer n such that

$$na = 0 \quad \text{for all} \quad a \in R,$$

then R is said to have *characteristic* n. If no such n exists, R is said to have characteristic zero. The characteristic of a ring is usually denoted by $\operatorname{char} R = n$ or $\operatorname{char} R = 0$.

From the beginning of this text, we deal with different kinds of field extensions.

Definition A.3.3. A field F is said to be an *extension field* of a field K (or simply an extension of K) provided that K is a subfield of F.

If we have the situation that $K \subset E \subset F$ are subfields, then E is said to be an *intermediate field* of K and F.
If F is a field and $X \subset F$, then the *subfield generated by* X is the intersecion of all subfields of F that contain X:

$$\langle X \rangle = \bigcap \{C \leq F \mid X \subseteq C\}.$$

If F is an extension of K and $X \subset F$, then the subfield generated by $K \cup X$ is called the *subfield generated by* X *over* K and is denoted $K(X)$. If X contains only one element u, then $K(u)$ is said to be a *simple extension*.

In this text, we only have algebraic extensions.

Definition A.3.4. Let F be an extension field of K. An element u of F is said to be algebraic over K provided that u is a root of some nonzero polynomial $f \in K[x]$. F is called an *algebraic extension* of K if every element of F is algebraic over K.

Theorem A.3.5. *If F is an extension field of K and $u \in F$ is algebraic over K, then*

1. $K(u) = K[u]$,

2. *$K(u) \simeq K[x]/(f)$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions $f(u) = 0$ and $g(u) = 0$ ($g \in K[x]$) if and only if f divides g.*

3. *$[K(u) : K] = n$,*

4. *$\{1_K, u, u^2, \dots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K,*

5. *every element of $K(u)$ can be written uniquely in the form*
$$a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} \text{ with } (a_i \in K).$$

We will use those facts often. From this it can easily be seen, that every finite extension must be algebraic.

Definition A.3.6. Let F be an extension field of K and $u \in F$ algebraic over K. The monic irreducible polynomial f of the preceding theorem is called the *irreducible* or *minimal* or *minimum polynomial of u*. The *degree of u over K* is $\deg f = [K(u) : K]$.

Such polynomials are widely used to describe field extensions.

Definition A.3.7. Let F be a field and $f \in F[x]$ a polynomial of positive degree. f is said to *split* over F if f can be written as a product of linear factors in $F[x]$.

Definition A.3.8. Let K be a field and $f \in K[x]$ a polynomial of positive degree. An extension field F of K is said to be a *splitting field over K of the polynomial f* if f splits in $F[x]$ and $F = K(u_1, \dots, u_n)$ where $u_1, \dots, u_n$ are the roots of f in F.

Theorem A.3.9. *The following conditions on a field F are equivalent:*

1. *Every nonconstant polynomial $f \in F[x]$ has a root in F.*

2. *Every nonconstant polynomial $f \in F[x]$ splits over F.*

3. *Every irreducible polynomial in $F[x]$ has degree one.*

4. *There is no algebraic extension field of F (expect F itself).*

5. *There exists a subfield K of F such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.*

A field that satisfies the equivalent conditions of this theorem is said to be *algebraically closed*.
It is also important to know that there is a maximal algebraic extension of a field.

Theorem A.3.10. *If F is an extension field of K, then the following conditions are equivalent.*

1. *F is algebraic over K and F is algebraically closed.*

2. *F is a splitting field over K of the set of all polynomials in $K[x]$.*

An extension field F of a field K that satisfies the equivalent conditions of this theorem is called an *algebraic closure* of K.
A very important aspect of this text is Galois theory.

Definition A.3.11. Let E and F be extension fields of a field K. If $\sigma : E \to F$ is a nonzero homomorphism of fields, then $\sigma(1_E) = 1_F$. If σ is also a K-module homomorphism then for every $k \in K$

$$\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_F = k.$$

Conversely, if a homomorphism of fields $\sigma : E \to F$ fixes K elementwise (that is, $\sigma(k) = k$ for all $k \in K$), then σ is nonzero and for any $u \in E$,

$$\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$$

whence σ is a *K-module homomorphism.*

Definition A.3.12. A field homomorphism f which also is a K-module homomorphism is called a *K-homomorphism.* Let F be a field extension of K. The group of all K-automorphisms of F is called the *Galois group* of F over K and is denoted by $\mathrm{Aut}_K(F)$.

Hence every element of $\mathrm{Aut}_K(F)$ fixes K elementwise. Another very important observation is, that every automorphism maps a root of a polynomial $f \in K[x]$ to another root of the same polynomial.

Theorem A.3.13. *Let F be an extension field of K, E an intermediate field and H a subgroup of $\mathrm{Aut}_K(F)$. Then*

1. $H' = \{v \in F \mid \sigma(v) = v \text{ for all } \sigma \in H\}$ *is an intermediate field of the extension,*
2. $E' = \{\sigma \in \mathrm{Aut}_K(F) \mid \sigma(u) \text{ for all } u \in E\} = \mathrm{Aut}_E(F)$ *is a subgroup of* $\mathrm{Aut}_K(F)$.

The field H' i called the *fixed field* of H in F. We deduce easily that

$$F' = \mathrm{Aut}_F(F) = 1 \quad \text{and} \quad K' = \mathrm{Aut}_K(F) = G$$

and on the other hand $1' = F$ (that is, F is the fixed field of the identity subgroup). It is not necessarily true, however, that $G' = K$. If so though, we have a *Galois extension.*

Definition A.3.14. Let F be an extension field of K such that the fixed field of the Galois group $\mathrm{Aut}_K(F)$ is K itself. Then F is said to be a *Galois extension* (field) of K or to be *Galois* over K.

Definition A.3.15. If E is an intermediate field of the extension $K \subset F$, E is said to be *stable* if every K-automorphism $\sigma \in \mathrm{Aut}_K(F)$ maps E into itself. This implies, that $\sigma|_E$ is in fact a K-automorphism of E (that is $\sigma|_E \in \mathrm{Aut}_K(E)$).

We now get to define two terms that are, combined, equivalent to Galois.

Definition A.3.16. Let K be a field and $f \in K[x]$ an irreducible polynomial. The polynomial f is said to be *separable* if in some splitting field of f over K every root of f is a simple root.
If F is an extension field of K and $u \in F$ is algebraic over K, then u is said to be *separable* over K provided its irreducible polynomial is separable. If every element of F is separable over K, then F is said to be a *separable extension* of K.

Definition A.3.17. An algebraic closure K^{alg} of K contains a unique separable extension K^{sep} of K containing all (algebraic) separable extensions of K within K^{alg}. This subextension is called a *separable closure* of K.

With this definition of the separable closure, we are able to define the absolut Galois group of a field.

Definition A.3.18. The *absolute Galois group* of a field K is the Galois group

$$\mathrm{Gal}(\overline{K}^{sep}/K)$$

of its separable closure as a field extension.

Definition A.3.19. An algebraic extension field F of K is *normal* over K if every irreducible polynomial in $K[x]$ that has a root in F actually splits in $F[x]$.

Definition A.3.20. A *Galois closure* of a field F is an extension field $L \supseteq F$, such that no proper subextension $K \subset L$ is normal over F.

Hence L is a minimal Galois extension of F.

Lemma A.3.21. *Let F be an algebraic extension field of K. Then F is Galois over K if and only if F is normal and separable over K. If* $\mathrm{char}\, K = 0$*, then F is Galois over K if and only if F is normal over K.*

Remark A.3.22. *If* $\mathrm{char}\, F = 0$*, then every irreducible polynomial over F is separable.*

Proposition A.3.23 (Primitive Element Theorem)**.** *Let L be a finite dimensional extension field of F.*

1. *If L is separable over F, then L is a simple extension of F, namely there exists $u \in L$ such that $L = F(u)$.*

2. *(Artin) More generally, L is a simple extension of F if and only if there are only finitely many intermediate fields.*

Lemma A.3.24. *If E is a separabel extension field of L and L is a separable extension field of F, then E is a separable over F.*

Lemma A.3.25. *If L is a Galois extension of F and E is a stable intermediate field of the extension, then E is Galois over F.*

Corollary A.3.26. *Let F be an algebraic extension field of K. Then F is Galois over K if and only if F is normal and separable over K.*

The next theorem is a very important result of Galois theory. It asserts, that the subgroups of a Galois group correspond one-to-one to the intermediate fields of an extension.

Theorem A.3.27 (Fundamental Theorem of Galois Theory)**.** *If F is a finite dimensional Galois extension of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group* $\operatorname{Aut}_K(F)$ *(given by $E \mapsto E' = \operatorname{Aut}_E(F)$) such that:*

1. *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular,* $\operatorname{Aut}_K(F)$ *has order $[F : K]$.*
2. *F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup $E' = \operatorname{Aut}_K(F)$ is normal in $G = \operatorname{Aut}_K(F)$. In this case, G/E' is (isomorphic to) the Galois group $\operatorname{Aut}_K(E)$ of E over K.*

There is another, generalized version of this fundamental theorem, dealing with infinite extensions. To accomplish such a theorem, we need to consider topological aspects.

It is possible to make $\operatorname{Aut}_K(F)$ into a compact topological group in such a way, that a subgroup H is topologically closed f and only if it is closed in the sence of $H = H''$. This is due to an observation of Krull. Of course even compact topological groups contain subgroups that are neither open nor closed.

Theorem A.3.28 (Generalized Fundamental Theorem)**.** *If F is an algebraic Galois extension field of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all closed subgroups of the Galois group* $\operatorname{Aut}_K(F)$ *(given by $E \mapsto E' = \operatorname{Aut}_E(F)$) such that F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup E' is normal in $G = \operatorname{Aut}_K(F)$. In this case, G/E' is (isomorphic to) the Galois group $\operatorname{Aut}_K(E)$ of E over K.*

In this text we define local fields to have a perfect residue field.

Theorem A.3.29. *The following conditions on a field K are equivalent:*

1. *Every irreducible polynomial in $K[x]$ is separable.*
2. *Every algebraic closure $\overline{K}$ of K is Galois over K.*
3. *Every algebraic extension field of K is separable over K.*
4. *Either $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ and $K = K^p$.*

Definition A.3.30. A field that satisfies the equivalent conditions of theorem A.3.29 is said to be *perfect*.

Lemma A.3.31. *Every finite field is perfect.*

A.4 Algebraic Number Theory

In this section we will explain basic terms from number theory and give a little background information on them.

In algebraic number theory, we usually have the following situation. Let A be an integral domain which is integrally closed, K its field of fractions and L a finite extension of K. We are particularly interested in the integral closure of A in L, denoted by $\mathcal{O}_L$.

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\
A \arrow[r, dash] & \mathcal{O}_L
\end{tikzcd}$$

But first two very important terms that are widely used in this text:

Definition A.4.1. The *trace* and *norm* of an element $x \in L$ are defined to be the trace and determinant of the endomorphism

$$T_x : L \to L, \quad T_x(\alpha) = x\alpha.$$

Since we have a finite extension, we can describe this endomorphism by its action on the basis elements of this extension. Hence we gain a matrix. Now the trace and norm of an element are the trace and determinant of this matrix:

$$\mathrm{Tr}_{L|K}(x) = \mathrm{Tr}(T_x), \quad N_{L|K} = \det(T_x).$$

In the characteristic polynomial

$$f_x(t) = \det(t \cdot I_n - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t]$$

of T_x, $n = [L : K]$, we recognize the trace and the norm as

$$a_1 = \mathrm{Tr}_{L|K}(x) \text{ and } a_n = N_{L|K}(x).$$

Since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$, we obtain homomorphisms

$$\mathrm{Tr}_{L|K} : L \to K \text{ and } N_{L|K} : L^* \to K^*.$$

In the important case where the extension $L|K$ is separable, the trace and norm admit the following Galois-theoretic interpretation that we use a lot.

Proposition A.4.2. *If $L|K$ is a separable extension and $\sigma : L \to \overline{K}$ varies over the different K-embeddings of L into an algebraic closure $\overline{K}$ of K, then we have*

1. $f_x(t) = \prod_\sigma (t - \sigma x)$,
2. $\mathrm{Tr}_{L|K}(x) = \sum_\sigma \sigma x$,

3. $N_{L|K}(x) = \prod_\sigma \sigma x$.

Another very important property of norm and trace is that its compatible with finite field extensions.

Corollary A.4.3. *In a tower of finite field extensions $K \subseteq L \subseteq M$, we have*

$$\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}$$

and

$$N_{L|K} \circ N_{M|L} = N_{M|K}.$$

Definition A.4.4. The *discriminant* of a basis $\alpha_1, \dots, \alpha_n$ of a separable extension $L|K$ is defined by

$$d(\alpha_1, \dots, \alpha_n) = \det((\sigma_j \alpha_j))^2,$$

where σ_i, $i = 1, \dots, n$ varies over the K-embeddings $L \to \overline{K}$.
Because of the relation

$$\mathrm{Tr}_{L|K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j),$$

the matrix $(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j))$ is the product of the matrices $(\sigma_k \alpha_i)^t$ and $(\sigma_k \alpha_j)$.
Thus we may write

$$d(\alpha_1, \dots, \alpha_n) = \det \left(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j) \right).$$

We now regard a more specific field extension. Namely, our integral domain will be $\mathbb{Z}$ with its well known quotient field $\mathbb{Q}$. Then K is an algebraic number field. We are now particularly interested in $\mathcal{O}_K$, the ring of integers of K.

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbb{Z} \arrow[r, dash] & \mathcal{O}_K
\end{tikzcd}$$

Definition A.4.5. A ring R is called *Noetherian* if every ideal is finitely generated.

Definition A.4.6. An integral domain that is

1. Noetherian,
2. integrally closed
3. and in which every nonzero prime ideal is maximal

is called a *Dedekind domain.*

Theorem A.4.7. *The ring $\mathcal{O}_K$ is Noetherian, integrally closed and every prime ideal $P \neq 0$ is a maximal ideal, hence it is a Dedekind domain.*

Definition A.4.8. A *fractional ideal* of K is a finitely generated $\mathcal{O}_K$-submodule $A \neq 0$ of K.

Proposition A.4.9. *The fractional ideals form an abelian group, the* ideal group J_K *of* K*. The identity element is* $(1) = \mathcal{O}_K$ *and the inverse of* $A \in J_K$ *is*

$$A^{-1} = \{x \in K \mid xA \subseteq \mathcal{O}_K\}.$$

The fractional principal ideals $(a) = a\mathcal{O}_K$, $a \in K^*$ form a subgroup of the group of ideals J_K, which is denoted by P_K. The quotient group

$$Cl_K = J_K/P_K$$

is called the *ideal class group* of K.
Along with the group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$, it fits into the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1$$

where the arrow in the middle is given by $a \mapsto (a)$. So the class group Cl_K measures the expansion that takes place when we pass from numbers to ideals.

This concept is very important as we know that the class group is finite, so we not get lost in infinity when passing from numbers to ideals.

Theorem A.4.10. *The ideal class group* $Cl_K = J_K/P_K$ *is finite. Its order*

$$h_K = [J_K : P_K]$$

is called the class number *of* K*.*

Corollary A.4.11. *Every fractional ideal* A *admits a unique representation as a product*

$$A = \prod_{P \text{ prime}} P^{v_P}$$

with $v_P \in \mathbb{Z}$ *and* $v_P = 0$ *for almost all* P*. In other words* J_K *is the free abelian group on the set of nonzero prime ideals* P *of* $\mathcal{O}_K$*.*

To close this section, we give a lemma that will prove useful in our technical proofs.

Lemma A.4.12. *Let* L/F *be a finite extension. Let* $\alpha \in \mathcal{O}_L$ *and let* $f(x)$ *be the monic irreducible polynomial of* α *over* F*. Then* $f(x) \in \mathcal{O}_F$*. Conversely, let* $f(x)$ *be a monic polynomial with coefficients in* $\mathcal{O}_F$*. If* $\alpha \in L$ *is a root of* $f(x)$*, then* $\alpha \in \mathcal{O}_L$*.*

A.5 Topological Groups

In this brief subsection we would like to give a short introduction to topological groups. As special topological groups we will give a little extra information on profinite groups, that were introduced in the introduction of chapter one. It is assumed that the reader has a basic understanding of topology.

Definition A.5.1. A *topological group* G is a topological space and group such that the group operations

$$G \times G \to G, \quad (x, y) \mapsto xy$$

and

$$G \to G, \quad x \mapsto x^{-1}$$

are continuous functions. Here, $G \times G$ is viewed as a topological space by using the product topology.

Definition A.5.2. By a *topologically generated* group G by a set X we mean that $\langle X \rangle$ is a dense subgroup in G.

Such topological groups have interesting and very useful properties. First, an observation shows, that it can contain subgroups that are neither open nor closed. In this text, we need topological groups as *profinite groups*. Those are special topological groups, as they are compact and totally disconnected Hausdorff spaces. Hence we get a list of properties, that prove to be very useful.

Lemma A.5.3. *Let G be a topological group.*

1. *The map $(x, y) \mapsto xy$ from $G \times G$ to G is continuous and the map $x \mapsto x^{-1}$ from G to G is a homoemorphismus. For each $g \in G$ the maps $x \mapsto xg$ and $x \mapsto gx$ from G to G are homoemorphisms.*

2. *If H is an open (resp. closed) subgroup of G then every coset Hg or gH of H in G is open (resp. closed).*

3. *Every open subgroup of G is closed, and every closed subgroup of finite index is open. If G is compact then every open subgroup of G has finite index.*

4. *If H is a subgroup containing a non-empty open subset U of G then H is open in G.*

Remark A.5.4. *There is also a converse theorem of 3 by D. Segal and N.Nikolov ([SeNi]). Namely, for a finitely generated profinite group we know, that every subgroup of finite index is open. This means, the topology on the group is determined by the group structure.*

Example A.5.5. A very nice profinite group is $\hat{\mathbb{Z}}$, the *profinite completion* of the integers. In chapter one we had

$$\mathbb{Z}_p = \varprojlim_{i} \mathbb{Z}/p^i\mathbb{Z}.$$

Similar to this, we define:

$$\hat{\mathbb{Z}} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z}.$$

The numbers $\hat{\mathbb{Z}}$ are also called the *Hensel numbers*.

Profinite groups are characterized to be compact and totally disconnected Hausdorff groups.

Proposition A.5.6. *Let X be a compact Hausdorff totally disconnected space. Then X is the inverse limit of its discrete quotient spaces.*

On the other hand we have:

Lemma A.5.7. *Let G be a topological group. Then G is a profinite group if and only if G is compact and totally disconnected.*

A very important description of a profinite group is with its inverse limit.

Theorem A.5.8. *Let G be a profinite group. If I is a filter base of closed normal subgroups of G such that $\bigcap(N \mid N \in I) = 1$ then*

$$G \simeq \varprojlim_{N \in I} G/N.$$

Moreover

$$H \simeq \varprojlim_{N \in I} H/(H \cap N)$$

for each closed subgroup H and

$$G/K \simeq \varprojlim_{N \in I} G/KN$$

for each closed normal subgroup K.

Remark A.5.9.

1. *It is important to understand, that every open subgroup is closed, hence the above description also holds for open subgroups. However, as already said above, subgroups of profinite groups can be neither open nor closed.*

2. *For profinite groups we can use the set*

$$I = \{N \mid N \lhd_O G\} = \{N \mid N \lhd G,\ N \text{ has finite index in } G\}$$

as a filter base. This explains the term profinite, as because of this G is an inverse limit of finite groups.

To close this section, we would like to give an idea of the Galois group of an infinite extension. Such extensions naturally occur in absolute Galois groups.

Let us assume we have a given field K and an infinite Galois extension L. First we define the set

$$\mathcal{F} = \{M \mid M \text{ a subfield of } K \text{ such that } M/K \text{ is a finite Galois extension}\}.$$

We define a topology in $\mathrm{Gal}(L/K)$ by taking as a base of open neighbourhoods of 1 the family of subgroups

$$\mathcal{N} = \{\mathrm{Gal}(L/M) \mid M \in \mathcal{F}\}.$$

Proposition A.5.10. $\mathrm{Gal}(L/K)$ *is the inverse limit of the finite groups* $\mathrm{Gal}(M/K)$ *with* $L \in \mathcal{F}$. *In particular,* $\mathrm{Gal}(L/K)$ *is a profinite group.*

Absolute Galois groups are always profinite groups[4]. For a finite field the absolute Galois group is isomorphic to $\hat{\mathbb{Z}}$.

[4] [Wi1]

Bibliography

[Am] S. Amano *Eisenstein equations of degree p in a p-adic field.* J. Fac. Sci. Univ. Tokyo Sect. IA Math., 18: 1–21 (1971).

[Ap] T.M. Apostol *Introduction to analytic number theory* New York, NY [u.a.]: Springer (1976).

[Be] J. Bellaiche *Sur la compatibilite entre les correspondances de Langlands locale et globale pour U(3).* Comment. Math. Helv. 81 (2006), no. 2, 449–470 (2006).

[Be1] E. Benjamin *On imaginary quadratic number fields with 2-class group of rank 4 and infinite 2-class field tower.* Pacific J. Math. 201 (2001), no. 2, 257–266 (2001).

[Be2] D. Benois *Périodes p-adiques et lois de réciprocité explicites. (French) [p-adic periods and explicit reciprocity laws]* J. Reine Angew. Math. 493 (1997), 115–151 (1997).

[Be3] J. Bernstein *An introduction to the Langlands program* Boston, Mass. [u.a.]: Birkhäuser (2004).

[Bl1] S. Bloch *K_2 and algebraic cycles.* Ann. of Math. (2) 99, 349–379 (1974).

[Bl2] S. Bloch *Algebraic K-theory and crystalline cohomology.* Inst. Hautes études Sci. Publ. Math. No. 47 (1977), 187–268 (1978).

[Bl3] S. Bloch *Applications of the dilogarithm function in algebraic K-theory and algebraic geometry.* Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), pp. 103–114, Kinokuniya Book Store, Tokyo (1978).

[Bl4] S. Bloch *Algebraic K-theory and classfield theory for arithmetic surfaces.* Ann. of Math. (2) 114 no. 2, 229–265 (1981).

[Ca] H. Carayol *Sur les représentations p-adiques associées aux formes modulaires de Hilbert.* Ann. Sci. école Norm. Sup. (4) 19, no. 3, 409–468 (1986).

[Ch1] I.D. Chipchakov: *One-dimensional local class field theory for primarily quasilocal fields.* C. R. Acad. Bulgare Sci. 57, no. 3, 11–16 (2004).

[Ch2] I.D. Chipchakov: *On nilpotent Galois groups and the scope of the normlimitation theorem in one-dimensional abstract local class field theory.* Acta Univ. Apulensis Math. Inform. No. 10, 149–167 (2005).

[Ch3] I.D. Chipchakov: *Class field theory for strictly quasilocal fields with Henselian discrete valuations* Manuscripta Math. 119, no. 3, 383–394 (2006).

[Cl] L. Clozel *Motifs et formes automorphes: applications du principe de fonctorialité. (French) [Motives and automorphic forms: applications of the functoriality principle]* Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), 77–159 (1990).

[CoDiOl] H. Cohen, F. Diaz y Diaz, M. Oliver *Counting cyclic quartic extensions of a number field.* J. Théor. Nombres Bordeaux 17, no. 2, 475–510 (2005).

[CoRo] H. Cohen, X. Roblot *Computing the Hilbert class field of real quadratic fields.* Math. Comp. 69, no. 231, 1229–1244 (2000).

[Cog] J.W. Cogdell *Langlands conjectures for* GL_n. An introduction to the Langlands program (Jerusalem, 2001), 229–249, Birkhuser Boston, Boston, MA (2003).

[Cor] G. Cornelissen *The 2-Primary Class Group of Certain Hyperelliptic Curves.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 253–260, Contemp. Math., 270, Amer. Math. Soc., Providence, RI (2000).

[De] P. Deligne *Formes modulaires et representations de GL(2), in P. Deligne andW. Kuyk* Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 55–105. Lecture Notes in Math., Vol. 349, Springer, Berlin (1973).

[DeSe] P. Deligne, J.P. Serre *Formes modulaires de poids 1.* Ann. Sci. école Norm. Sup. (4) 7 (1974), 507–530 (1975).

[Dr1] V. Drinfeld *Elliptic modules.* Mat. Sb. (N.S.) 94(136), 594–627, 656 (1974).

[Dr2] V. Drinfeld *Cohomology of compactified moduli varieties of F-sheaves of rank* 2. J. Soviet Math. 46, no. 2, 1789–1821 (1989).

[Fe1] I. Fesenko *A multidimensional local theory of class fields. II* St. Petersburg Math. J. 3, no. 5, 1103–1126 (1992).

[Fe2] I. Fesenko *Class field theory of multidimensional local fields of characteristic 0 with residue field of positive characteristic* Algebra i Analiz 3, no. 3, 165–196 (1991); translation in St. Petersburg Math. J. 3, no. 3, 649–678 (1992).

[Fe3] Fesenko: *Local class field theory: the perfect residue field case.* Izv. Ross. Akad. Nauk Ser. Mat. 57, no. 4, 72–91 (1993); translation in Russian Acad. Sci. Izv. Math. 43, no. 1, 65–81 (1994).

[Fe4] I. Fesenko *Abelian local p-class field theory* Math. Ann. 301, no. 3, 561–586 (1995).

[Fe5] I. Fesenko *Nonabelian local reciprocity maps.* Class field theory—its centenary and prospect (Tokyo), 63–78 (1998).

[Fe6] I. Fesenko *On the image of noncommutative local reciprocity map.* Homology, Homotopy Appl. 7, no. 3, 53–62 (electronic) (2005).

[FeKu] I. Fesenko, M.Kurihara *Invitation to higher local fields (Introduction)* Papers from the conference held in Mnster, August 29 - September 5, 1999. Edited by Ivan Fesenko and Masato Kurihara. Geometry & Topology Monographs, 3. Geometry & Topology Publications, Coventry. front matter+304 pp. (electronic) (2000).

[FeVo1] I. Fesenko, S.V. Vostokov: *Local Fields and Their Extensions* American Math. Soc., Providence, RI (1993).

[FeVo2] I. Fesenko, S.V. Vostokov: *Local Fields and Their Extensions - Second Edition* American Math. Soc., Providence, RI (2003).

[Fi] C. Fieker *Computing class fields via the Artin map.* Math. Comp. 70, no. 235, 1293–1303 (electronic) (2001).

[FoWi] J.M. Fontaine, J.P. Wintenberger *Le "corps des normes" de certaines extensions algébriques de corps locaux.* C. R. Acad. Sci. Paris Sér. A-B 288, no. 6, A367–A370 (1979).

[FrJa] M. D. Fried, M. Jarden: *Field Arithmetic - Second Edition* Berlin [u.a.]: Springer (2005).

[Fu1] L. Fuchs *Infinite Abelian Groups - Volume 1.* New York, NY [u.a.]: Acad. Press. - (Pure and applied mathematics) (1970).

[Fu2] T. Fukaya *Explicit reciprocity laws for p-divisible groups over higher dimensional local fields.* J. Reine Angew. Math. 531, 61–119 (2001).

[FuHa] W. Fulton, J. Harris *Representation theory - A first course.* Springer-Verlag, New York (1991).

[GoSa] E. Golod, I. Safarevich *On the class field tower.* Izv. Akad. Nauk SSSR Ser. Mat. 28 261–272 (1964).

[Gr] Grayson *Products in K-theory and intersecting algebraic cycles.* Invent. Math. 47, no. 1, 71–83 (1978).

[HaTa] M. Harris, R. Taylor *The geometry and cohomology of some simple Shimura varieties.* Annals of Mathematics Studies, 151. Princeton University Press, Princeton, NJ, viii+276 pp (2001).

[He1] G. Henniart *La conjecture de Langlands locale pour $GL(p)$.* C. R. Acad. Sci. Paris Sér. I Math. 299, no. 3, 73–76 (1984).

[He2] G. Henniart *Caractérisation de la correspondance de Langlands locale par les facteurs ϵ de paires.* Invent. Math. 113, no. 2, 339–350 (1993).

[He3] G. Henniart *Une preuve simple des conjectures de Langlands pour GL(n) sur un corps p-adique* Invent. Math. 139, no. 2, 439–455 (2000).

[He4] G. Henniart *La conjecture de Langlands locale pour $GL(3)$.* Mém. Soc. Math. France (N.S.) No. 11–12, 186 pp (1984).

[Hu1] T. Hungerford *Algebra.* New York, NY [u.a.]: Springer (1980).

[Hu2] B. Huppert *Endliche Gruppen 1.* Berlin [u.a.]: Springer (1967).

[Is] M. Ishida *The Genus Fields of Algebraic Number fields.* Lecture Notes in Mathematics, Vol. 555. Springer-Verlag, Berlin-New York. vi+116 pp. (1976).

[Iw] K. Iwasawa: *Local Class Field Theory.* Oxford Univ. Press [u.a.] (1986).

[Ka1] K. Kato *A generalization of local class field theory by using K-groups* J. Fac. Sci. Univ. Tokyo Sect. IA Math. 26, no. 2, 303–376 (1979).

[Ka2] K. Kato *A generalization of local class field theory by using K-groups II* J. Fac. Sci. Univ. Tokyo Sect. IA Math. 27, no. 3, 603–683 (1980).

[Ka3] K. Kato *Galois cohomology of complete discrete valuation fields* Algebraic K-theory, Part II (Oberwolfach, 1980), pp. 215–238, Lecture Notes in Math., 967, Springer, Berlin-New York (1982).

[Ka4] K. Kato *Existence theorem for higher local fields.* Invitation to higher local fields (Mnster, 1999), 165-195 (electronic), Geom. Topol. Monogr., 3, Geom. Topol. Publ., Coventry (2000).

[Kl] J. Klüners *A counterexample to Malles conjecture on the asymptotics of discriminants.* C. R. Math. Acad. Sci. Paris 340, no. 6, 411–414 (2005).

[Ko] H. Koch *Local class field theory for metabelian extensions.* Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993), 287–300, Sympos. Gaussiana, de Gruyter, Berlin (1995).

[KoSh] H. Koch, E. de Shalit *Metabelian local class field theory.* J. Reine Angew. Math. 478, 85–106 (1996).

[Ku1] M. Kurihara *The exponential homomorphisms for the Milnor K-groups and an explicit reciprocity law.* J. Reine Angew. Math. 498, 201–221 (1998).

[Ku2] A.G. Kurosh *Theory of Groups - Volume 1.* Translated and edited by K. A. Hirsch. Chelsea Publishing Co., New York, N.Y. (1955).

[La1] L. Lafforgue *Chtoucas de Drinfeld et correspondance de Langlands.* Invent. Math. 147, no. 1, 1–241 (2002).

[La2] L. Lafforgue *Chtoucas de Drinfeld, formule des traces d'Arthur-Selberg et correspondance de Langlands.* Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002), 383–400, Higher Ed. Press, Beijing (2002).

[La3] S. Lang *Introduction to Modular Forms.* Berlin [u.a.]: Springer (1976).

[La4] S. Lang: *Algebra.* New York, NY [u.a.]: Springer (2002).

[La5] R. Langlands *On the classification of irreducible representations of real algebraic groups.* Representation theory and harmonic analysis on semisimple Lie groups, 101–170, Math. Surveys Monogr., 31, Amer. Math. Soc., Providence, RI, (1989).

[La6] F. Laubie *Une théorie du corps de classes local non abelien. (French. English summary) [A nonabelian local class field theory]* Compos. Math. 143, no. 2, 339–362 (2007).

[LaRaSt] Laumon, Rapoport, Stuhler *$\mathcal{D}$-elliptic sheaves and the Langlands correspondence.* Invent. Math. 113, no. 2, 217–338 (1993).

[LeSt] H. Lenstra, P. Stevenhagen *Artin reciprocity and Mersenne primes.* Nieuw Arch. Wiskd. (5) 1, no. 1, 44–54 (2000).

[Ma1] C. Maire *Un raffinement du théoréme de Golod-Safarevic.* Nagoya Math. J. 150, 1–11 (1998).

[Ma2] G. Malle *On the distribution of Galois groups.* J. Number Theory 92, no. 2, 315–329 (2002).

[Ma3] G. Malle *On the distribution of Galois groups II.* Experiment. Math. 13, no. 2, 129–135 (2004).

[Ma4] J. Martinet *Tours de corps de classes et estimations de discriminants.* Invent. Math. 44, no. 1, 65–73 (1978).

[Mo] A. Mouhib *Sur la tour des 2-corps de classes de Hilbert des corps quadratiques reels.* Ann. Sci. Math. Québec 28 (2004), no. 1-2, 179–187 (2005).

[Ne1] J. Neukirch: *Class Field Theory.* Berlin [u.a.]: Springer (1986).

[Ne2] J. Neukirch: *Algebraic Number Theory.* Berlin [u.a.]: Springer (1999).

[Ne3] J. Neukirch: *Cohomology of Number Fields.* Berlin [u.a.]: Springer (2008).

[No] A. Nomura *A note on the 3-class field tower of a cyclic cubic field.* Proc. Japan Acad. Ser. A Math. Sci. 83, no. 2, 14–15 (2007).

[Ok] K. Okano *Abelian p-class field towers over the cyclotomic Zp-extensions of imaginary quadratic fields.* Acta Arith. 125, no. 4, 363–381 (2006).

[Pa1] A.N. Parshin *Abelian coverings of arithmetic schemes.* Dokl. Akad. Nauk SSSR 243, no. 4, 855–858 (1978).

[Pa2] A.N. Parshin *Local class field theory.* Trudy Mat. Inst. Steklov. 165, 143–170 (1984).

[Pa3] A.N. Parshin *Galois cohomology and Brauer group of local fields.* Trudy Mat. Inst. Steklov. 183, 159–169, 227 (1990).

[Pa4] S. Pauli *Constructing class fields over local fields.* J. Théor. Nombres Bordeaux 18, no. 3, 627–652 (2006).

[Ra] D. Ramakrishnan *Pure motives and automorphic forms.* Motives (Seattle, WA, 1991), 411–446, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI (1994).

[Ro1] J.D. Rogawski *The nonabelian reciprocity law for local fields.* Notices Amer. Math. Soc. 47, no. 1, 35–41 (2000).

[RoTu] J.D. Rogawski, J.B. Tunnell *On Artin L-functions associated to Hilbert modular forms of weight one* Invent. Math. 74, no. 1, 1–42 (1983).

[Ro2] J. Rotman *An Introduction to the Theory of Groups.* New York, NY [u.a.]: Springer (1995).

[SeNi] D.Segal, N.Nikolov *Finite index subgroups in profinite groups.* C. R. Math. Acad. Sci. Paris 337, no. 5, 303–308 (2003).

[Se3] S. Sen *On explicit reciprocity laws.* J. Reine Angew. Math. 313, 1–26 (1980).

[Se1] J.P. Serre *Galois Cohomology.* Berlin [u.a.]: Springer (1967).

[Se2] J.P.Serre *A Course in Arithmetic.* New York, NY [u.a.]: Springer (1973).

[Sh1] I.E. Shparlinksi *Infinite Hilbert class field towers over cyclotomic fields.* Glasg. Math. J. 50, no. 1, 27–32 (2008).

[Sh2] A. Shiho *A note on class field theory for two-dimensional local rings.* Compositio Math. 124, no. 3, 305–340 (2000).

[So] C. Soule *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale.* Invent. Math. 55, no. 3, 251–295 (1979).

[Su] Y. Sueyoshi *Infinite 2-class field towers of some imaginary quadratic number fields.* Acta Arith. 113, no. 3, 251–257 (2004).

[Ta] J. Tate *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$. (French)* Progress in Mathematics, 47. Birkhuser Boston, Inc., Boston, MA (1984).

[TaYo] R. Taylor, T. Yoshida *Compatibility of local and global Langlands correspondences.* J. Amer. Math. Soc. 20, no. 2, 467–493 (electronic) (2007).

[Wil] J.S. Wilson: *Profinite Groups.* Oxford Univ. Press (1998).

[Yo] E. Yoshida *On the 3-class field tower of some biquadratic fields.* Acta Arith. 107, no. 4, 327–336 (2003).

[Zh] I. Zhukov: *Invitation to higher local fields, Part I* Invitation to higher local fields (Mnster, 1999), 5–18 (electronic), Geom. Topol. Monogr., 3, Geom. Topol. Publ., Coventry (2000).

[Zi] E.W. Zink *Lokale projektive Klassenkorpertheorie. II. (German) [Local projective class field theory. II]* Math. Nachr. 114, 123–150 (1983).

List of Notation

$(.,L/F)$	induced homomorphism	59
$\left(\frac{u}{p}\right)$	n-th power residue symbol	76
$\left(\frac{\cdot,\cdot}{p}\right)$	Hilbert symbol	75
$[a,b]$	commutator of a and b	103
$\mathbb{A}$	ring of adeles	72
$\mathcal{A}_n^0(k;\overline{\mathbb{Q}}_l)$	space of some $\overline{\mathbb{Q}}_l$-valued cuspidal representations	93
$A \otimes_R B$	tensor product	65
$\mathrm{Aut}_K(F)$	Galois group of F over K	113
$\mathcal{B}^n(G,A)$	inhomogeneous coboundaries	68
$B^n(G,A)$	n-coboundaries	64
$\hat{C}(G,A)$	n-th Tate cohomology group	67
$\mathcal{C}^n(G,A)$	n-th inhomogeneous cocycles	68
$\mathcal{C}_n$	equivalence classes of supercuspidal representations	90
$C(\gamma)$	splitting module	68
$C^n(G,A)$	set of continuous functions	64
$C_G(a)$	centralizer of a in G	105
C_K	idele class group	73
$\mathrm{char}\, R$	characteristic of R	111
χ^-	Hecke character	91
Cl_K	ideal class group	118
D^{-n}	a map	67
d_i	natural projection	63

d_i^*	induced homomorphism	63
∂^n	alternating sum	63
$e(L/F,w)$	ramification index	17
$\hat{F}$	completion with respect to a valuation	13
$\mathbb{F}((t))$	function field over the field $\mathbb{F}$	34
$\mathcal{F}$	completion of F^{ur}	48
$\overline{F}$	residue class field	9
$f(L/F,w)$	inertia degree	17
$\mathrm{Frob}(L/F)$	Frobenius set	42
$\mathcal{G}_n$	equivalence classes of irrducible representations	90
$G^{(i+1)}$	derived subgroup	104
G_x	stabilizer of x in G	106
$\hat{H}^n(G,A)$	modified cohomology groups	66
$H \leq G$	H is a subgroup of G	102
$H \lhd G$	H is a normal subgroup of G	102
H^g	conjugate of H	106
$H^n(G,A)$	n-cohomology group	64
$H^n(G,A)$	n-th inhomogeneous cohomology	68
h_K	class number	118
I_F	inertia subgroup	89
I_K	group of ideles	72
I_K^S	group of S-ideles	73
I_n	certain generated subgroup for the Milnor K-group	81
inv	invariant map	69
J_K	ideal group	118
K^{sep}	separable closure	114
K_p	completion at a prime	72
$kerf$	kernel of f	103

$\mathcal{L}_k$	Langlands group	93
$\varprojlim$	inverse limit	6
$L(s,\chi)$	Hecke L-function	91
$\mathcal{M}_v$	set of elements of positive valuation	9
μ_{q-1}	set of $(q-1)$-th roots of unity	15
$N_G(H)$	normalizer of H in G	106
$\mathcal{O}_v$	ring of integers	9
π	a prime	11
P	unique prime ideal	9
P_K	principal ideal group	118
φ_F	Frobenius automorphism	35
Ψ_F	reciprocity map	59
$\Psi_{L/F}$	Hazewinkel homomorphism	50
$\mathbb{Q}_p$	p-adic numbers	6
$r_{(p^n)}(G)$	p^n-rank	96
$Rep_n^0(\mathcal{G},\overline{\mathbb{Q}}_l)_f$	isomorphism classes of irreducible l-adic representations	93
res_F^H	restriction	67
ρ	group representation	88
$U^{(1)}$	group of principal units	33
$U^{(i)}$	higher groups of units	36
U_1	group of principal units	36
U_i	higher groups of units	36
U_K	unit group	9
U_v	unit group	9
$\hat{v}$	valuation on the completion	13
x^g	g acts on x	105
X^n	abelian group of maps	63
$\tilde{\Upsilon}_{L/F}$	Neukirch map	43

$\Upsilon_{L/F}$	Neukirch isomorphism	44
$\hat{\mathbb{Z}}$	Hensel integers	120
$\mathbb{Z}_p$	p-adic integers	4
$\mathcal{Z}^n(G, A)$	inhomogeneous cocycles	68
$Z(G)$	center of a group G	102
$Z^n(G, A)$	n-cocycles	64

Index

abelian group, 102
absolute Galois group, 114
absolute residue degree, 33
abstract G-module, 62
adele, 72
admissible representation, 90
algebraic
  closure, 113
algebraically closed, 112
archimedean, 8
  non-, 8
Artin's Reciprocity Law, 73
automorphic form, 94

biquadradic extension, 98
biquadratic, 98

Cauchy sequence, 13
center of a group, 102
central character, 91
centralizer, 105
character, 90
  central, 91
characteristic of a ring, 111
class field, 80
class field
  p, 97
  Hilbert, 96
  tower, 96
Class Field Tower Problem, 96
class module, 67
class number, 118
class of group extension, 102
cohomology group, 64
  modified, 66
commutator, 103
complete discrete valuation field, 13
complete standard resolution, 67
completion, 13
  profinite, 119
complex, 63
conjugate, 106
content, 110
cup-product, 65

$\mathcal{D}$-elliptic sheaves, 92
Dedekind domain, 117
discrete valuation, 10
discriminant of a field, 117
division ring, 111

ϵ-factors, 91
equivalent
  representations, 89
  valuations, 10
exact sequence, 105
  split, 105
existence theorem, 61
extension
  algebraic field, 111
  class of group extension, 102
  field, 111
  Galois, 113
  integral, 109
  maximal unramified, 28
  normal, 114
  of a group, 102
  ring, 109
  separable, 114
  simple field, 111
  tamely ramified, 25
  totally ramified, 25
  unramified, 25
  unramified (infinite), 28

field, 111
  fixed, 113
  genus, 98

  - Henselian, 15
  - intermediate, 111
  - local, 14
    - function, 14
    - n-dimensional, 81
    - number, 14
  - perfect, 115
  - residue, 9
  - valuation, 8
- fixed field, 113
- fractional ideal, 117
- free abelian, 102
- Frobenius automorphism, 35, 89
- fundamental class, 68

- G-set, 105
- Galois, 113
  - closure, 114
  - extension, 113
  - group, 113
    - absolute, 114
- Gauss lemma, 110
- Gauss' Reciprocity Law, 77
- generated subfield, 111
- genus
  - field, 98
  - group, 98
  - number, 98
- group, 101
  - abelian, 102
  - cohomology, 64
  - divisible, 104
  - extension, 102
  - Galois, 113
  - genus, 98
  - homomorphism, 103
  - idele class, 73
  - metabelian, 104
  - Milnor K-, 82
  - modified cohomology, 66
  - of ideles, 72
  - of principal units, 36
  - principal ideals, 118
  - soluble, 104
  - Tate cohomology, 67
  - topological, 119
  - Weil, 89

- Hazewinkel homomorphism, 50
- Hecke
  - L-function, 91
  - character, 91
- Hensel numbers, 120
- Hensel's lemma, 15
- Henselian
  - P-valuation, 97
  - field, 15
- higher derived groups, 104
- Hilbert
  - class field, 96
  - symbol, 75

- ideal, 108
  - class group, 118
  - fractional, 117
  - group, 118
  - left, 108
  - maximal, 109
  - prime, 108
  - right, 108
- idele
  - S, 73
  - class group, 73
  - group, 72
  - principal, 73
- inertia degree, 17
- inertia subgroup, 89
- inner automorphism, 104
- integral, 109
  - domain, 111
  - extension, 109
- integrally closed, 110
- invariant maps, 69
- invertible element, 109
- irreducible representation, 89
- isomorphic representations, 89
- isomorphism, 103
- isomorphism theorem
  - first, 103
  - second, 103
  - third, 103

- K-module homomorphism, 113

kernel, 103

Langlands
- correspondence
  - global, 92
  - local, 88

Langlands group, 93
Laurent series, 34
left ideal, 108
Legendre symbol, 76
lemma
- Gauss, 110
- Hensel, 15

local field, 14
- n-dimensional, 81

local function field, 14
local Langlands Correspondence, 91
local number field, 14
local reciprocity law, 55, 70
local ring, 109
lying-over-theorem, 110

map
- n-symbolic, 81
- invariant, 69
- Neukirch, 43

maximal unramified extension, 28
Mersenne
- number, 100
- prime, 100

metabelian group, 85
modified cohomology groups, 66
modular form, 94
motivic Galois group, 93

n-cochains, 64
n-dimensional cohomology group, 64
n-dimensional local field, 81
n-symbolic map, 81
n-th Milnor K-group, 82
n-th power residue symbol, 76
n-th Tate cohomology group, 67
Neukirch map, 43
non-archimedian, 8
norm, 116
- residue symbol, 73

normal extension, 114
normalized valuation, 10
normalizer, 106

p-adic
- absolute value, 5
- exp. valuation, 5
- integer, 4
- numbers, 6

p-class field, 97
p-divisible, 104
p-group, 106
p^n-rank, 96
p-subgroup, 106
perfect field, 115
polynomial
- irreducible, 112
- minimal, 112
- monic, 109
- primitive, 110

primarily quasilocal, 79
prime
- element, 89
- of a field, 11

principal
- units group, 36
- units, 36

principal ideles, 73
profinite completion, 119
projective limit, 6

quasilocal
- primarily, 79
- strictly, 80
- strictly primarily, 79

ramification index, 17
reciprocity map, 59
representation, 88
- admissible, 90
- equivalent, 89
- isomorphic, 89
- supercuspidal, 90
- unramified, 93

residue
- degree, 17

residue field, 9
- first, 81

last, 81
resolution, 64
complete standard, 67
restriction, 67
right ideal, 108
ring, 108
commutative, 108
division, 109
extension, 109
local, 109
Noetherian, 117
of integers, 10
valuation, 10
with identity, 108

S-ideles, 73
separable
closure, 114
element, 114
extension, 114
polynomials, 114
set of representatives, 17
simple field extension, 111
split, 112
splitting
field, 112
module, 68
stabilizer, 106
stable intermediate field, 113
Steinberg property, 81
strictly
primarily quasilocal, 79
quasilocal, 80
subgroup, 102
commutator, 103
derived, 103
normal, 102
Sylow, 106
transitive, 104
subrepresentation, 89
subring, 108
supercuspidal representation, 90
Sylow subgroup, 106
symbol
Legendre, 76
power residue, 76

tamely ramified, 25
tensor product, 65
theorem
Cauchy, 106
Chipchakov, 80
fundamental theorem of Galois theory, 115
generalized fundamental theorem, 115
isomorphism, 103
Kronecker, 96
lying-over-, 110
Nakayama-Tate, 69
Ostrowski, 13
primitive element, 114
Sylow, 106
topologically generated, 119
totally ramified, 25
trace, 116
transitive subgroup, 104

unit, 109
unramified, 25, 28
representation, 93

valuation, 8
p-adic exponential, 5
discrete, 10
equivalent, 10
field, 8
normalized, 10
ring, 10
valuation field
discrete, 10
complete, 13
Verlagerung, 49

Weil group, 89
Weil-Deligne group, 92

zero divisor, 111