

Local Class Field Theory

Jim L. Brown

Contents

1	Introduction	5
2	Valuations	7
2.1	Definitions and basic facts	7
2.2	Completions	10
2.3	Hensel's Lemma	12
2.4	Extensions of valuations	16
3	Local Fields	25
3.1	Definitions and basic facts	25
3.2	Krasner's Lemma	27
3.3	Eisenstein Extensions	30
3.4	Unramified Extensions	33
3.5	Ramification and Galois theory	37
4	Group Cohomology	43
4.1	Definitions	43
4.2	Hilbert's Theorem 90	47
4.3	Changing the group	50
4.4	Cup Products	53
4.5	Profinite Groups	55
4.6	Homology Groups	56
4.7	The Tate Groups	57
5	Main Results of Local Class Field Theory	67
5.1	Statements of the theorems	67
5.2	The fundamental class	68
5.3	The local reciprocity map	76
5.4	Lubin-Tate formal group laws	81
5.5	Norm subgroups	85
5.6	Final Remarks	95

Chapter 1

Introduction

These are notes for a course in Local Class Field theory taught at Caltech winter term of 2008. There are undoubtedly mistakes in these notes, and they are the author's alone. If you find a mistake, please feel free to e-mail me at jimlb@caltech.edu so that the mistakes can be corrected. These notes have arisen from my attempt to gather what I like from several sources and compile it into one source for the students enrolled in this course. As such, the theorems and proofs have been freely lifted from sources listed in the references. The main references for these notes are [Mi97] and [CF67]. Both are excellent sources and are most likely much more useful than these notes. Please use these at your own risk.

My intention is to follow these notes with notes on Global Class Field theory to be taught next quarter. Those notes will focus on the statements of GCFT and then applications, omitting many of the proofs. If you find these notes at all helpful, please stop back to check out the GCFT notes as they are completed.

Chapter 2

Valuations

2.1 Definitions and basic facts

Valuations will be the basis of everything that is done with local fields. We will eventually see that for a number field K there are a limited number of possibilities for valuations. We begin here with some basic definitions and facts.

Definition 2.1. Let K be a field. A *valuation* on K is a function $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ such that

1. $|x| = 0$ if and only if $x = 0$
2. $|xy| = |x||y|$
3. There exists $c \in \mathbb{R}_{>0}$ such that $|1 + x| \leq c$ whenever $|x| \leq 1$. Note that this is equivalent to the condition that $|x + y| \leq |x| + |y|$

It is immediate from the definition that $|1| = 1 = |-1|$ and $|-a| = |a|$.

Example 2.2. 1. For any field K one can define the trivial valuation by $|x| = 1$ for all $x \in K^\times$.

2. The usual absolute value on \mathbb{R} or \mathbb{C} gives a valuation. We write $|\cdot|_{\mathbb{R}}$ and $|\cdot|_{\mathbb{C}}$ when it is not clear from context.
3. Let K be a number field and $\sigma : K \hookrightarrow \mathbb{C}$ an embedding. The function $|x|_{\sigma} = |\sigma(x)|$ defines a valuation on K .
4. Let \mathfrak{D} be a Dedekind domain and $0 \neq \mathfrak{p} \subseteq \mathfrak{D}$ a prime ideal. Let K be the field of fractions of \mathfrak{D} . For $x \in K^\times$, put $\text{ord}_{\mathfrak{p}}(x)$ to be the power of \mathfrak{p} appearing in the factorization of $x\mathfrak{D}$. Then

$$\begin{aligned} |x|_{\mathfrak{p}} &= (\text{Nm}(\mathfrak{p}))^{-\text{ord}_{\mathfrak{p}}(x)} \\ &= \#(\mathfrak{D}/\mathfrak{p})^{-\text{ord}_{\mathfrak{p}}(x)} \end{aligned}$$

is a valuation on K . More specifically, if $K = \mathbb{Q}$ and $\mathfrak{p} = p$ a rational prime, then for $x \in \mathbb{Q}$ with $x = p^r \frac{a}{b}$ with $\gcd(ab, p) = 1$ we have $|x|_p = p^{-r}$. In

particular, $|p|_p = p^{-1}$. This valuation is generally referred to as the \mathfrak{p} -adic absolute value, or p -adic absolute value in the case $K = \mathbb{Q}$.

Definition 2.3. A valuation on K is said to be *nonarchimedean* if $|x + y| \leq \max(|x|, |y|)$ for all $x, y \in K$. A valuation that is not nonarchimedean is said to be *archimedean*.

Exercise 2.4. Show the valuation given in Part 4 of Example 2.2 is an example of a nonarchimedean valuation.

Definition 2.5. A valuation is said to be *discrete* if there exists $\delta \in \mathbb{R}_{>0}$ such that if $1 - \delta < |x| < 1 + \delta$ then $|x| = 1$.

A valuation on K determines a topology on K . A basis for this topology consists of the sets $B_{x_0, \epsilon} = \{x \in K : |x - x_0| < \epsilon\}$ for $x_0 \in K$ and $\epsilon > 0$.

Exercise 2.6. Let $|\cdot|$ be a valuation on K . The field K is a topological field with respect to the topology determined by $|\cdot|$, i.e., multiplication, addition, and inversion are all continuous.

Definition 2.7. Let K be a field with $|\cdot|$ a nonarchimedean valuation on K . The *valuation ring* of K with respect to $|\cdot|$ is the set

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}.$$

Note that the valuation does not appear in the notation for the valuation ring as it will be clear from context.

Proposition 2.8. Let K be a field and $|\cdot|$ a nonarchimedean valuation on K .

1. The valuation ring \mathcal{O}_K is an integrally closed ring. The units of \mathcal{O}_K are given by $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$ and K is the field of fractions of \mathcal{O}_K .
2. The ideal $\mathfrak{m}_K = \{x \in K : |x| < 1\}$ is the unique maximal ideal of \mathcal{O}_K .
3. If $|\cdot|$ is discrete, then \mathcal{O}_K is a Dedekind domain, in fact, a principal ideal domain. Hence it is a local ring.

Proof. Let $x, y \in \mathcal{O}_K$. Since $|x| = |-x|$ we have $-x \in \mathcal{O}_K$. Similarly, $|xy| = |x||y| \leq 1$, so $xy \in \mathcal{O}_K$ and $|x + y| \leq \max\{|x|, |y|\} \leq 1$, so $x + y \in \mathcal{O}_K$. Thus \mathcal{O}_K is a subring of K . It is clear that

$$\begin{aligned} x \in \mathcal{O}_K^\times &\iff x, x^{-1} \in \mathcal{O}_K \\ &\iff |x|, |x|^{-1} \leq 1 \\ &\iff |x| = 1. \end{aligned}$$

To see that K is the field of fractions of \mathcal{O}_K , observe that $y \in K, y \notin \mathcal{O}_K$ if and only if $|y| > 1$ if and only if $\frac{1}{|y|} < 1$ which implies $\frac{1}{y} \in \mathcal{O}_K$.

Now suppose x is integral over \mathcal{O}_K . Then we have a relation of the form

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathcal{O}_K$$

which implies

$$\begin{aligned} |x|^n &= |a_1 x^{n-1} + \dots + a_n| \\ &\leq \max_i |a_i x^{n-i}| \\ &\leq \max_i |x^{n-i}|. \end{aligned}$$

Now since $|x|^n \leq |x|^j$ for some $0 \leq j \leq n-1$, we have that $|x|^{n-j} \leq 1$. Thus $|x| \leq 1$ and $x \in \mathcal{O}_K$ and hence \mathcal{O}_K is integrally closed. This proves part (1).

Let $x, y \in \mathfrak{m}_K$. We have $|x+y| \leq \max\{|x|, |y|\} < 1$, so $x+y \in \mathfrak{m}_K$. If $x \in \mathfrak{m}_K, y \in \mathcal{O}_K$, then $|xy| = |x||y| < 1$, so $xy \in \mathfrak{m}_K$. Suppose $I \subseteq \mathcal{O}_K$, $I \not\subseteq \mathfrak{m}_K$. Then there exists $z \in I$ such that $|z| = 1$. So $z \in \mathcal{O}_K^\times$, hence $I = \mathcal{O}_K$. Thus we have that \mathfrak{m}_K is the unique maximal ideal. This finishes the proof of part (2).

Suppose now that $|\cdot|$ is discrete. Let $\varpi \in \mathfrak{m}_K$ be such that $|\varpi|$ is maximal (which exists by the discreteness of $|\cdot|$.) Suppose $\alpha \in \mathfrak{m}_K$. Then $|\frac{\alpha}{\varpi}| \leq 1$, so $\frac{\alpha}{\varpi} \in \mathcal{O}_K$. Thus $\alpha \in \varpi \mathcal{O}_K$ and since α was arbitrary in \mathfrak{m}_K we obtain $\mathfrak{m}_K = \varpi \mathcal{O}_K$. Now suppose $I \subseteq \mathfrak{m}_K$ is any ideal, $I \neq 0$. Let $\alpha \in I$ be such that $|\alpha|$ is maximal. The same argument as above shows that $I = \alpha \mathcal{O}_K$. Choose $n \in \mathbb{Z}$ such that $|\frac{\alpha}{\varpi^n}| \leq 1$ but $|\frac{\alpha}{\varpi^{n+1}}| > 1$ (which is again possible by the discreteness of $|\cdot|$.) Then $1 \geq |\frac{\alpha}{\varpi^n}| > |\varpi|$ since $|\frac{\alpha}{\varpi^{n+1}}| > 1$ and $|\frac{\varpi}{\varpi}| = 1$. Thus $\frac{\alpha}{\varpi^n} \in \mathcal{O}_K \setminus \mathfrak{m}_K$, i.e., $\frac{\alpha}{\varpi^n} \in \mathcal{O}_K^\times$. So $I = \varpi^n \mathcal{O}_K$. Thus \mathcal{O}_K is a principal ideal domain.

For \mathcal{O}_K to be a Dedekind domain we need to check:

- (i) integrally closed: done by part (3),
- (ii) Noetherian: done because it is a principal ideal domain,
- (iii) all non-zero primes are maximal: done because only non-zero prime ideal is $\varpi \mathcal{O}_K$.

Thus, we have that \mathcal{O}_K is a Dedekind domain and since we have a unique maximal ideal it is in fact a local ring. \square

Definition 2.9. The *residue field of K* is defined to be $k = \mathcal{O}_K / \mathfrak{m}_K$. If $|\cdot|$ is discrete, then any $\varpi \in \mathcal{O}_K$ such that $\mathfrak{m}_K = \varpi \mathcal{O}_K$ is called a *uniformizer of K* .

Example 2.10. Consider the field \mathbb{Q} and the valuation $|\cdot|_p$ for p a rational prime. The valuation ring $\mathcal{O}_{\mathbb{Q}}$ is the set of rational numbers $\frac{a}{b}$ with $|\frac{a}{b}|_p \leq 1$, i.e., the fractions with $\gcd(b, p) = 1$. This is precisely the ring \mathbb{Z} localized at the prime p , i.e., $\mathbb{Z}_{(p)}$. The maximal ideal is $p\mathbb{Z}_{(p)}$ and the residue field is $k = \mathbb{Z}_{(p)} / p\mathbb{Z}_{(p)} \cong (\mathbb{Z}/p\mathbb{Z})_{(p)} \cong \mathbb{F}_p$.

More generally, for \mathfrak{D} a Dedekind domain, K the field of fractions of \mathfrak{D} , $\mathfrak{p} \subset \mathfrak{D}$ a nonzero prime ideal, and $k = \mathfrak{D}/\mathfrak{p}$, we can consider the valuation as in Example 2.2 part (4) given by

$$|x|_{\mathfrak{p}} = (\#k)^{-\text{ord}_{\mathfrak{p}}(x)}$$

for $x \in K^\times$. We have $\mathcal{O}_K = \mathfrak{D}_{\mathfrak{p}}$, the localization of \mathfrak{D} at \mathfrak{p} , $\mathfrak{m}_K = \mathfrak{p}\mathfrak{D}_{\mathfrak{p}}$, and the residue field is given by $\mathfrak{D}_{\mathfrak{p}} / \mathfrak{p}\mathfrak{D}_{\mathfrak{p}} \cong (\mathfrak{D}/\mathfrak{p})_{\mathfrak{p}} \cong \mathfrak{D}/\mathfrak{p} \cong k$.

2.2 Completions

Recall from basic real analysis that a sequence $\{a_n\}$ is said to be *Cauchy* if for every $\varepsilon > 0$ there exists an integer $N > 0$ so that if $m, n > N$ then $|a_m - a_n| < \varepsilon$. The field \mathbb{R} is the completion of \mathbb{Q} with respect to the normal absolute value, i.e., \mathbb{R} is the field one obtains when adjoining the limit points of all Cauchy sequences in \mathbb{Q} . We extend this notion here.

Definition 2.11. We say K is *complete with respect to a valuation* $|\cdot|$ if K is complete with respect to the topology determined by $|\cdot|$, i.e., if all Cauchy sequences in K converge to an element in K .

Proposition 2.12. Let K be a field and $|\cdot|$ a valuation on K . There exists a field \widehat{K} and a valuation $|\cdot|_{\widehat{K}}$ on \widehat{K} such that \widehat{K} is complete with respect to $|\cdot|_{\widehat{K}}$ and there is an embedding $K \hookrightarrow \widehat{K}$ such that $|x|_{\widehat{K}} = |x|$ for all $x \in K$ and the completion of K in \widehat{K} is \widehat{K} . Moreover, \widehat{K} is unique up to isomorphism and K is dense in \widehat{K} .

Proof. Let \widehat{K} be the topological completion of K . Now see [AM69] Chapter 10 for the proof. \square

Example 2.13. 1. Let K be a number field, $\sigma : K \hookrightarrow \mathbb{C}$ an embedding. The completion of K with respect to $|\cdot|_{\sigma}$ is given by

$$\widehat{K} = \begin{cases} (\mathbb{R}, |\cdot|_{\mathbb{R}}) & \text{if } \sigma(K) \subseteq \mathbb{R} \\ (\mathbb{C}, |\cdot|_{\mathbb{C}}) & \text{if } \sigma(K) \not\subseteq \mathbb{R} \end{cases}$$

where $|\cdot|$ is the normal absolute value on \mathbb{C} .

2. Let $K = k(x)$ where k is a field and define the absolute value on K by $\left|\frac{u}{v}\right|_{\infty} = c^{-(\deg u - \deg v)}$ for some constant $c > 1$. In this case the closure is given by $\widehat{K} = k(\frac{1}{x})$. The absolute value on \widehat{K} is given by $|u|_{\widehat{K}} = c^{-r}$ where $u = x^{-r}(u_0 + u_1x^{-1} + \dots)$ with $u_0 \neq 0$.

We now spend some time on completions in the case of discrete nonarchimedean valuations as these will be of paramount importance. We write $|K|$ for the possible valuations of elements in K . In light of Theorem 2.8 we see that

$$|K| = \{|\varpi|^m : m \in \mathbb{Z}\} \cup \{0\}.$$

Let $x \in \widehat{K}$ with $x \neq 0$ and $\{x_n\}$ a Cauchy sequence converging to x . Note that if $x \in K$, then $\{x\}$ is a Cauchy sequence converging to x and if $x \notin K$, then by definition of \widehat{K} there is a Cauchy sequence converging to x . The fact that $|\cdot|$ is a continuous map implies that $|x_n|$ converges to $|x|$. Thus, we have that the sequence $\{|x_n|\}$ converges to $|x|$ and so $|x|$ is a limit point for the set $|K|$. We know that $|K|$ is a discrete set by assumption so it is necessarily closed, and hence it contains all of its limit points. Thus, $|x| \in |K|$. This shows that $|\widehat{K}| = |K|$ and hence $|\cdot|$ is a discrete valuation on \widehat{K} as well.

Exercise 2.14. For any positive integer n the natural map

$$\mathcal{O}_K/\mathfrak{m}_K^n \longrightarrow \mathcal{O}_{\widehat{K}}/\mathfrak{m}_{\widehat{K}}^n$$

is an isomorphism.

Proposition 2.15. Let $|\cdot|$ be a discrete nonarchimedean valuation on K and S a set of representatives for $k = \mathcal{O}_K/\mathfrak{m}_K$. The series

$$a_{-m}\varpi^{-m} + \cdots + a_0 + a_1\varpi + \cdots + a_n\varpi^n + \cdots$$

with $a_i \in S$ is a Cauchy series, i.e., the sequence defining the series is a Cauchy sequence. Conversely, every Cauchy series is equivalent to a series of this form.

Before we prove this proposition note that it implies that every element of \widehat{K} can be written uniquely as such a series. This will be useful when working with the completions as it allows us to get our hands on the elements.

Proof. Let $x_M = \sum_{i=-m}^M a_i\varpi^i$. We have if $M < N$ that

$$|x_M - x_N| \leq |\varpi|^{M+1}.$$

Thus, $\{x_n\}$ is a Cauchy sequence as claimed.

Let $x \in \widehat{K}$. The fact that $|\widehat{K}| = |K|$ allows us to write $x = \varpi^m\alpha_0$ first $\alpha_0 \in \mathcal{O}_{\widehat{K}}^\times$. The previous exercise with $n = 1$ gives that there exists $a_0 \in S$ so that $\alpha_0 - a_0 \in \mathfrak{m}_{\widehat{K}}$. This implies that $\frac{\alpha_0 - a_0}{\varpi} \in \mathcal{O}_{\widehat{K}}$ and so there exists $a_1 \in S$ so that $\frac{\alpha_0 - a_0}{\varpi} - a_1 \in \mathfrak{m}_{\widehat{K}}$. Continuing, we get $a_2 \in S$ so that $\frac{\alpha_0 - a_0 - a_1\varpi}{\varpi} - a_2 \in \mathfrak{m}_{\widehat{K}}$. Taking the limit of this process we obtain

$$\alpha_0 = a_0 + a_1\varpi + a_2\varpi^2 + \cdots$$

and so

$$x = a_0\varpi^m + a_1\varpi^{m+1} + a_2\varpi^{m+2} + \cdots$$

as desired. To see the uniqueness, note that $|\sum a_i\varpi^i| = |\varpi|^r$ if r is the first nonzero coefficient. Thus, $\sum a_i\varpi^i = 0$ if and only if $a_i = 0$ for all i . \square

Let \mathbb{Q}_p be the completion of \mathbb{Q} with respect to $|\cdot|_p$ and \mathbb{Z}_p the valuation ring of \mathbb{Q}_p . The previous proposition gives that any element of \mathbb{Q}_p can be written in the form

$$a_{-m}p^{-m} + \cdots + a_0 + a_1p + \cdots + a_np^n + \cdots .$$

Similarly, any element in \mathbb{Z}_p can be written in the form

$$a_0 + a_1p + \cdots + a_np^n + \cdots .$$

Our results show that $\mathfrak{m}_{\mathbb{Q}_p} = p\mathbb{Z}_p$, the residue field is given by $k \cong \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ and $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ for n a positive integer.

More generally, let \mathfrak{D} be a Dedekind domain and $\mathfrak{p} \subset \mathfrak{D}$ a prime ideal. Set $k = \mathfrak{D}/\mathfrak{p}$ and K be the field of fractions of \mathfrak{D} . Let $\varpi \in \mathfrak{p}$ with $\varpi \notin \mathfrak{p}^2$. Then

$|\varpi| = (\#k)^{-1}$. Let \mathcal{S} be a set of representatives for $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. It is clear that ϖ is a uniformizer of this ring. Set $K_{\mathfrak{p}}$ to be the completion of K with respect to $|\cdot|_{\mathfrak{p}}$. Our previous proposition gives

$$K_{\mathfrak{p}} = \left\{ \sum_{n \geq m} a_n \varpi^n : m \in \mathbb{Z}, a_n \in \mathcal{S} \right\},$$

$$\mathcal{O}_{K_{\mathfrak{p}}} = \left\{ \sum_{n \geq 0} a_n \varpi^n : a_n \in \mathcal{S} \right\},$$

$$\mathfrak{m}_{K_{\mathfrak{p}}} = \varpi \mathcal{O}_{K_{\mathfrak{p}}},$$

and k is the residue field (see Example 2.10.) We call such a field $K_{\mathfrak{p}}$ a *\mathfrak{p} -adic field*.

Exercise 2.16. *Is 7 a unit in \mathbb{Z}_5 ? If so, what is 7^{-1} ? Is -1 a square in \mathbb{Q}_5 ? If so, what is $\sqrt{-1}$?*

2.3 Hensel's Lemma

Hensel's lemma will be a very important result in our study of local fields. It gives conditions under which one can lift roots of polynomials from the residue field to the valuation ring. We will give two forms of Hensel's lemma.

Throughout this section K is a field complete with respect to a discrete nonarchimedean valuation $|\cdot|$.

Lemma 2.17. *Let $x, y \in K$ with $|x| < |y|$. Then we have $|x + y| = |y|$.*

Proof. The fact that $|x| < |y|$ implies that $\left| \frac{x}{y} \right| < 1$ and so $\frac{x}{y} \in \mathfrak{m}_K$. Thus, $1 + \frac{x}{y} \in \mathcal{O}_K^{\times}$ and so $\left| 1 + \frac{x}{y} \right| = 1$. This gives the result. \square

Theorem 2.18. (*Newton's Lemma*) *Let $f \in \mathcal{O}_K[x]$. Suppose there exists $\alpha_0 \in \mathcal{O}_K$ so that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then there exists a unique $\alpha \in \mathcal{O}_K$ so that*

1. $f(\alpha) = 0$
2. $|\alpha - \alpha_0| \leq \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$.

Proof. The proof is basically applying Newton's method to the polynomial f . Define $f_j \in \mathcal{O}_K[x]$ by the Taylor expansion of $f(x)$:

$$f(x + y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots.$$

Thus, $f_1(x) = f'(x)$ for example. Set $\beta_0 = -\frac{f(\alpha_0)}{f'(\alpha_0)}$.

Claim: $|\beta_0| < 1$.

Pf: Suppose $|f'(\alpha_0)| > 1$. Then since $\alpha_0 \in \mathcal{O}_K$ and $f(x) \in \mathcal{O}_K[x]$, we have $|f(\alpha_0)| < 1$ and so the result is clear in this case. Now suppose that $|f'(\alpha_0)| \leq 1$. Then $|f(\alpha_0)| < |f'(\alpha_0)|^2 \leq |f'(\alpha_0)|$. Thus, we have the result.

We would like to show that $|f(\alpha_0 + \beta_0)| < |f(\alpha_0)|$. Observe that we have

$$\begin{aligned} |f(\alpha_0 + \beta_0)| &= |f(\alpha_0) + f_1(\alpha_0)\beta_0 + f_2(\alpha_0)\beta_0^2 + \cdots| \\ &\leq \max_{j \geq 0} |f_j(\alpha_0)\beta_0^j|. \end{aligned}$$

If $j = 0$ or $j = 1$ is the maximum we are done. Thus, suppose not. Then we have

$$\begin{aligned} |f(\alpha_0 + \beta_0)| &\leq \max_{j \geq 2} |f_j(\alpha_0)\beta_0^j| \\ &\leq \max_{j \geq 2} |\beta_0^j| \quad (\text{since } f_j \in \mathcal{O}_K[x]) \\ &= |\beta_0|^2 \quad (\text{by the claim}) \\ &= \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|^2 \\ &< |f(\alpha_0)| \quad (\text{by assumption.}) \end{aligned}$$

We now write

$$f_1(x + y) = f_1(x) + g_1(x)y + g_2(x)y^2 + \cdots.$$

A similar argument yields

$$\begin{aligned} |f_1(\alpha_0) - f_1(\alpha_0 + \beta_0)| &\leq \max_{j \geq 2} |g_j(\alpha_0)\beta_0^j| \\ &< |f(\alpha_0)| \\ &< |f'(\alpha_0)|. \end{aligned}$$

Set $\alpha_1 = \alpha_0 + \beta_0$. This gives:

1. $|f(\alpha_1)| \leq \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|^2 < |f(\alpha_0)|$
2. $|f'(\alpha_1)| = |f_1(\alpha_1)| < |f'(\alpha_0)|$ by applying Lemma 2.17 to the fact that $|f'(\alpha_0) - f'(\alpha_0 + \beta_0)| < |f'(\alpha_0)|$.
3. $|\alpha_1 - \alpha_0| = |\beta_0| = \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$.

We can now repeat this entire argument and inductively define a sequence $\{\alpha_n\}$ with $\alpha_n \in \mathcal{O}_K$ such that

1. $|f(\alpha_n)| < |f(\alpha_{n-1})|$
2. $|f'(\alpha_n)| < |f'(\alpha_{n-1})| < \cdots < |f'(\alpha_0)|$

$$3. |\alpha_n - \alpha_{n-1}| = \left| \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} \right| < \left| \frac{f(\alpha_1)}{f'(\alpha_1)} \right|.$$

Property (1) ensures that $f(\alpha_n) \rightarrow 0$ and property (3) implies that α_n converges to some $\alpha \in \mathcal{O}_K$. Thus, $f(\alpha_n) \rightarrow f(\alpha)$ and by the uniqueness of limits we get that $f(\alpha) = 0$. We also have that $|\alpha_n - \alpha| < \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$ implies that $|\alpha - \alpha_0| < \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$.

It now remains to show the uniqueness of α . Suppose α and $\alpha + \beta$ are two distinct zeroes of f close to α_0 , i.e., $|\alpha + \beta - \alpha_0| < \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$ and $|\alpha - \alpha_0| < \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$. Putting $\alpha + \beta$ into $f(x + y)$ yields

$$\sum f_i(\alpha)\beta^i = 0.$$

Thus, as before we obtain

$$|\beta f_1(\alpha)| = \left| \sum_{j \geq 2} f_j(\alpha)\beta^j \right| \leq |\beta|^2$$

which implies $|f_1(\alpha)| \leq |\beta|$. On the other hand we have

$$\begin{aligned} |f'(\alpha_0)| &> \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right| \\ &> |\alpha + \beta - \alpha_0|. \end{aligned}$$

Now observe that

$$\begin{aligned} |\alpha - \alpha_0| &< \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right| \\ &< |f'(\alpha_0)| \\ &\leq |\beta|. \end{aligned}$$

We can apply Lemma 2.17 to conclude that $|\alpha - \alpha_0| = |\beta|$. Thus, $|f'(\alpha_0)| > |\beta| \geq |f'(\alpha)|$, which is clearly a contradiction. Thus we must have α is unique in the interval $|\alpha - \alpha_0| < \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|$. \square

An immediate corollary, and possibly the more familiar form of what is generally referred to as Hensel's lemma is the following corollary. The power lies in the fact that one can look for a root in the residue field and then if the derivative of f does not vanish at this root we know it lifts to a root in \mathcal{O}_K .

Corollary 2.19. (*Hensel's Lemma*) *Let $f \in \mathcal{O}_K[x]$ and $\alpha_0 \in \mathcal{O}_K$ such that*

$$f(\alpha_0) \equiv 0 \pmod{\mathfrak{m}_K}$$

and

$$f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{m}_K}.$$

Then there exists $\alpha \in \mathcal{O}_K$ so that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\mathfrak{m}_K}$.

We also have another form of Hensel's lemma.

Lemma 2.20. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial, and let $k = \mathcal{O}_K/\mathfrak{m}_K$. If $h', g' \in k[x]$ such that $f \equiv g'h' \pmod{\mathfrak{m}_K}$ and $\gcd(g', h') = 1$, i.e., $(g', h') = k[x]$, then there exists $h, g \in \mathcal{O}_K[x]$ such that $f = hg$ and $g \equiv g' \pmod{\mathfrak{m}_K}$, $h \equiv h' \pmod{\mathfrak{m}_K}$. Moreover, g and h are unique up to scalar multiples.*

Proof. As always, let ϖ be a generator of \mathfrak{m}_K . First we prove existence of g and h . For $n \geq 0$ we will construct, inductively, polynomials g_n, h_n in $\mathcal{O}_K[x]$ with unit leading coefficient such that $f - g_n h_n \equiv 0 \pmod{\varpi^{n+1}}$, $g_n \equiv g', h_n \equiv h' \pmod{\varpi}$, $g_n \equiv g_{n-1}, h_n \equiv h_{n-1} \pmod{\varpi^n}$. Let g_0, h_0 be any lift of g', h' to $\mathcal{O}_K[x]$. One can check that these satisfy the conditions required. Now suppose $n > 0$ and we have constructed g_{n-1}, h_{n-1} with the required properties. Let $l = \frac{f - g_{n-1}h_{n-1}}{\varpi^n} \in \mathcal{O}_K[x]$. Choose $u_n, v_n \in \mathcal{O}_K[x]$ such that $u_n g_0 + v_n h_0 \equiv l \pmod{\varpi}$. This is possible since $\gcd(g', h') = 1$ in $k[x]$. Put $g_n = g_{n-1} + \varpi^n u_n, h_n = h_{n-1} + \varpi^n v_n \in \mathcal{O}_K[x]$. Then $h_n \equiv h_{n-1}, g_n \equiv g_{n-1} \pmod{\varpi^n}$ and we have

$$\begin{aligned} f - g_n h_n &= f - (g_{n-1} + \varpi^n u_n)(h_{n-1} + \varpi^n v_n) \\ &= f - g_{n-1} h_{n-1} - \varpi^n (v_n h_{n-1} + u_n g_{n-1}) \pmod{\varpi^{n+1}} \\ &= \varpi^n l - \varpi^n (\text{something} \equiv l \pmod{\varpi}) \pmod{\varpi^{n+1}} \\ &\equiv 0 \pmod{\varpi^{n+1}}. \end{aligned}$$

Now just take $g = \varprojlim g_n, h = \varprojlim h_n \in \mathcal{O}_K[x]$ so we have $f = gh, g \equiv \bar{g}, h \equiv \bar{h} \pmod{\varpi}$.

It remains to prove uniqueness. Observe that $(g', h') = k[x]$ implies that $(g, h) + \mathfrak{m}_K \mathcal{O}_K[x] = \mathcal{O}_K[x]$. Write $M = \mathcal{O}_K[x]/(g, h)$ so that we have $\mathfrak{m}_K M = M$. Nakayama's Lemma then gives $M = 0$. Suppose $f = gh = \tilde{g}\tilde{h}$, $g \equiv \tilde{g} \pmod{\varpi}, h \equiv \tilde{h} \pmod{\varpi}$. There exists r, s such that $r\tilde{g} + sh = 1$ since the argument above shows $\gcd(\tilde{g}, h) = 1$. Thus

$$\begin{aligned} \tilde{h} &= r\tilde{g}\tilde{h} + sh\tilde{h} \\ &= rgh + sh\tilde{h}. \end{aligned}$$

Hence $h|\tilde{h}$. Similarly, $\tilde{h}|h$. Thus $h = \tilde{h}$ up to multiplication by a unit. The same argument works for g and so we have uniqueness. \square

Example 2.21. Let d be a square-free integer. Let p be a prime so that $p \nmid 2d$. We have that $\sqrt{d} \in \mathbb{Z}_p$ if and only if $f(x) = x^2 - d$ has a root in \mathbb{Z}_p . Applying Hensel's lemma we see that $\sqrt{d} \in \mathbb{Z}_p$ if and only if there is a root α_0 of $f(x)$ in \mathbb{F}_p and $f'(\alpha_0) \not\equiv 0 \pmod{p}$, i.e., $2\alpha_0 \not\equiv 0 \pmod{p}$. The polynomial $f(x)$ having a zero modulo p is equivalent to $\left(\frac{d}{p}\right) = 1$, i.e., d is a quadratic residue modulo p since $p \nmid d$ by assumption. Since $p \nmid 2$, the condition on the derivative is satisfied if such a root exists. Thus we have that if p is a prime so that $p \nmid 2d$ and d is a square-free integer, then $\sqrt{d} \in \mathbb{Z}_p$ if and only if $\left(\frac{d}{p}\right) = 1$.

We can also view this in terms of the factorization of the ideal $p\mathfrak{D}_{\mathbb{Q}(\sqrt{d})}$. We know this splits if and only if $\left(\frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = 1$ where Δ_K is the discriminant of the field. Since the discriminant is either $4d$ or d , we see this is equivalent to our above condition. Thus, we can also phrase the result as $\sqrt{d} \in \mathbb{Z}_p$ if and only if p splits in $\mathbb{Q}(\sqrt{d})$.

Exercise 2.22. Let p be an odd prime and let μ_{p-1} denote the $p-1$ st roots of unity. Prove that $\mu_{p-1} \subset \mathbb{Z}_p^\times$. Use this to construct the Teichmüller character $\omega : \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_p^\times$ where $\omega(a)$ is the unique p th root of unity so that $\omega(a) \equiv a \pmod{p}$.

2.4 Extensions of valuations

We have seen that given a number field K , there are valuations arising from the prime ideals in \mathfrak{D}_K as well as valuations arising from the embeddings of K into \mathbb{R} and \mathbb{C} . We will show in this section that up to equivalence these are the only valuations.

Definition 2.23. Two valuations $|\cdot|_1$ and $|\cdot|_2$ on a field K are said to be *equivalent* if there exists $c \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^c$ for all $x \in K$.

Exercise 2.24. Prove that two evaluations $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if and only if they determine the same topology on K .

The following result of Ostrowski gives our result for the field $K = \mathbb{Q}$.

Proposition 2.25. A non-trivial valuation on \mathbb{Q} is equivalent to either the normal absolute value (which we write as $|\cdot|_\infty$) or $|\cdot|_p$ for some rational prime p .

Proof. Let m, n be integers larger than 1. We can write $m = a_0 + a_1n + \dots + a_r n^r$ with the $a_i \in \mathbb{Z}$, $0 \leq a_i < n$, and $n^r \leq m$. Let $N = \max\{1, |n|\}$. By the triangle inequality we have

$$|m| \leq \sum |a_i| |n|^i \leq \sum |a_i| N^r.$$

Clearly we have $r \leq \frac{\log m}{\log n}$, so another application of the triangle inequality gives that $|a_i| = |1 + \dots + 1| \leq a_i |1| = a_i \leq n$. Combining these we obtain

$$|m| \leq (1+r)nN^r \leq \left(1 + \frac{\log m}{\log n}\right) nN^{\log m / \log n}.$$

In this inequality, replacing m with m^t and taking t^{th} roots gives

$$|m| \leq \left(1 + \frac{t \log m}{\log n}\right)^{1/t} n^{1/t} N^{\log m / \log n}.$$

Letting $t \rightarrow \infty$ we have

$$|m| \leq N^{\log m / \log n}.$$

Case 1: For all $n > 1$, $|n| > 1$.

In this case, $N = |n|$ and so $|m| \leq |n|^{\log m / \log n}$ i.e., $|m|^{1/\log m} \leq |n|^{1/\log n}$. By symmetry we must have equality. So there exists a real number $c > 1$ such that $c = |m|^{1/\log m} = |n|^{1/\log n}$ for all integers $m, n > 1$. Hence, $|n| = c^{\log n} = e^{\log c \log n} = n^{\log c}$ for all $n > 1$. Letting $a = \log c$, we have $|n| = |n|_\infty^a$ for $n > 1$. Since both $|\cdot|$ and $|\cdot|_\infty^a$ are homomorphisms from $\mathbb{Q}^\times \rightarrow \mathbb{R}_{>0}$, the fact that they agree on a set of generators implies they agree on all of \mathbb{Q}^\times .

Case 2: For some $n > 1$, $|n| \leq 1$.

Let n be such that $|n| \leq 1$. In this case $N = 1$, so $|m| \leq 1$ for all integers m . Therefore, we have a nonarchimedean valuation. We know $\mathbb{Z} \subset \mathcal{O}_\mathbb{Q}$ by the definition of $\mathcal{O}_\mathbb{Q}$. Thus $\mathfrak{m}_\mathbb{Q} \cap \mathbb{Z}$ is a prime in \mathbb{Z} and is nonzero since the valuation is not trivial. Thus $\mathfrak{m}_\mathbb{Q} \cap \mathbb{Z} = (p)$ for some rational prime p . If $a \in \mathbb{Z}$ with $p \nmid a$, then $a \notin \mathfrak{m}_\mathbb{Q}$ and so necessarily we have $|a| = 1$. Thus $|np^r| = |p|^r$ if $n = \frac{a}{b}$ with $\gcd(ab, p) = 1$. Now if α is such that $|p| = p^{-\alpha}$, then $|x| = |x|_p^\alpha$ for all $x \in \mathbb{Q}$ and so $|\cdot|$ is equivalent to $|\cdot|_p$. \square

Before we can prove the result for a general number field, we need the following result on extensions of valuations. This will allow us to use Ostrowski's theorem to gain information in the general number field setting.

Theorem 2.26. *Let K be a field complete with respect to a discrete nonarchimedean valuation $|\cdot|$ and L/K a finite separable extension of K .*

1. *There exists a unique valuation $|\cdot|_L$ on L extending $|\cdot|$, necessarily discrete and nonarchimedean.*
2. *For $\beta \in L$, $|\beta|_L = |\mathbb{N}_{L/K}(\beta)|^{1/\deg(L/K)}$.*
3. *L is complete with respect to $|\cdot|_L$.*

Proof. Let ϖ be a uniformizer of K . Let \mathfrak{D}_L be the integral closure of \mathcal{O}_K in L . We break the proof into several steps.

Step 1: The integral closure \mathfrak{D}_L is a Dedekind domain and a finite free \mathcal{O}_K -module.

Pf: By Lemma 2.8, \mathcal{O}_K is a Dedekind domain (even a PID). One now just runs through the same proof as used in basic algebraic number theory to show that \mathfrak{D}_E is a Dedekind domain for E a number field to show that \mathfrak{D}_L is a Dedekind domain.

Step 2: The integral closure \mathfrak{D}_L has a unique maximal ideal.

Pf: Let \mathfrak{m}_L be any maximal ideal of \mathfrak{D}_L . Since \mathcal{O}_K has a unique maximal ideal we must have $\mathfrak{m}_L \cap \mathcal{O}_K = 0$ or \mathfrak{m}_K . Since $\mathfrak{D}_L/\mathfrak{m}_L$ is a field and a free $\mathcal{O}_K/(\mathfrak{m}_L \cap \mathcal{O}_K)$ -module of finite rank, we must have $\mathfrak{m}_L \cap \mathcal{O}_K = \mathfrak{m}_K$. In particular we have that all maximal ideals of \mathfrak{D}_L appear in the factorization of

$\mathfrak{m}_K \mathfrak{D}_L$, i.e., $\mathfrak{m}_K \mathfrak{D}_L = \mathfrak{m}_1^{s_1} \dots \mathfrak{m}_r^{s_r}$ for \mathfrak{m}_i the maximal ideals of \mathfrak{D}_L . We then have

$$\mathfrak{D}_L / \mathfrak{m}_K \mathfrak{O}_L \cong \bigoplus_{i=1}^r \mathfrak{D}_L / \mathfrak{m}_i^{s_i}.$$

Suppose $r \geq 2$. Let $\beta \in \mathfrak{D}_L$ be such that $\beta \in \mathfrak{m}_1$, $\beta \notin \mathfrak{m}_2$. Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of β over K , i.e.,

$$(2.1) \quad \mathcal{O}_K[x][\beta] \cong \mathcal{O}_K[x]/(f).$$

The fact that f is irreducible combines with Hensel's lemma to show that f must be at worst a power of an irreducible polynomial modulo \mathfrak{m}_K . Thus, tensoring equation (2.1) with $\mathcal{O}_K/\mathfrak{m}_K$ we obtain

$$(\mathcal{O}_K[\beta]/\mathfrak{m}_K \mathcal{O}_K[\beta])[x] \cong \mathcal{O}_K[x]/(\mathfrak{m}_K, f) \cong k[x]/(f),$$

which is a local ring. However, this contradicts the fact that $\mathcal{O}_K[\beta]$ has two distinct maximal ideals containing \mathfrak{m}_K , namely $\mathfrak{m}_1 \cap \mathcal{O}_K[\beta]$ and $\mathfrak{m}_2 \cap \mathcal{O}_K[\beta]$. Thus it must be the case that $r = 1$ and \mathfrak{D}_L has a unique maximal ideal.

Step 3: The valuation $|\cdot|$ extends to a discrete valuation on L .

Pf: Let \mathfrak{m}_L be the unique maximal ideal of \mathfrak{D}_L . Since any Dedekind domain with a finite number of prime ideals is a principal ideal domain, \mathfrak{m}_L is principal. Let ϖ_L be a generator of \mathfrak{m}_L . Suppose $\mathfrak{m}_K \mathfrak{D}_L = \mathfrak{m}_L^e$, i.e., $(\varpi) = (\varpi_L)^e$ in \mathfrak{D}_L . Given $x \in L$, define $|x|_L = (|\varpi|)^{\text{ord}_{\mathfrak{m}_L}(x)/e}$. This gives a discrete nonarchimedean valuation. Since $|\varpi|_L = (|\varpi|)^{e/e} = |\varpi|$, the valuation $|\cdot|_L$ agrees with $|\cdot|$ on K .

Step 4: For $\beta \in L$, $|\beta|_L = |\mathbb{N}_{L/K}(\beta)|^{1/\deg(L/K)}$.

Pf: We only need to prove this for $\beta = \pi_L$. We have $\mathbb{N}_{L/K}(\pi_L) = \pi^f \cdot u$ where $f = f(\mathfrak{m}_L/\mathfrak{m}_K)$ and $u \in \mathcal{O}_K^\times$. Thus we have $f e = \deg(L/K)$ and

$$\begin{aligned} |\mathbb{N}_{L/K}(\pi_L)|^{1/f e} &= |\pi^f|^{1/f e} \\ &= |\pi|^{1/e} \\ &= |\pi|^{\deg_{\mathfrak{m}_L}(\pi_L)/e} \\ &= |\pi_L|_L. \end{aligned}$$

Step 5: The field L is complete with respect to $|\cdot|_L$.

Pf: Let $\{\alpha_N\}$ be a Cauchy sequence in L . Let e_1, \dots, e_n be an \mathcal{O}_K -basis of \mathfrak{D}_L . So in particular, a K -basis of L . Write each $\alpha_N = \alpha_{N,1}e_1 + \dots + \alpha_{N,n}e_n$ with $\alpha_{N,i} \in K$ for $1 \leq i \leq n$. For each $r > 0$, let N_r be such that

$$|\alpha_N - \alpha_{N'}| < |\varpi_L|_L^{e r} = |\varpi|_L^r$$

for every $N, N' \geq N_r$. Thus, $\alpha_N - \alpha_{N'} \in \varpi^r \mathfrak{D}_L$. So $\alpha_{N,i} - \alpha_{N',i} \in \varpi^r \mathcal{O}_K$ for every $N, N' \geq N_r$. Thus $\{\alpha_{N,i}\}$ is a Cauchy sequence in K for each i . Let $\alpha_i = \lim_N \alpha_{N,i}$. It is clear that $\alpha = \alpha_1 e_1 + \cdots + \alpha_n e_n$ is the limit of $\{\alpha_N\}$.

Step 7: Suppose $|\cdot|_0$ is some extension of $|\cdot|$ to L . If $x \in \mathfrak{D}_L$, then $|x|_0 \leq 1$. In particular, if $x \in \mathfrak{D}_L^\times$, then $|x|_0 = 1$.

Pf: Let $\mathfrak{D}_L = \mathcal{O}_K e_1 + \cdots + \mathcal{O}_K e_n$. If $x \in \mathfrak{D}_L$ we can write $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ with $\alpha_i \in \mathcal{O}_K$. So there exists $r > 0$ such that $|x|_0^r \leq (|e_1|_0^r + \cdots + |e_n|_0^r)$. For example, take r such that $c^r \leq 2$ where c is as in the definition of valuation. Thus $|x|_0$ is bounded for all $x \in \mathfrak{D}_L$. Hence, $|x|_0 \leq 1$ for otherwise taking powers would contradict the boundedness.

Step 8: Suppose $|\cdot|_0$ is any extension of $|\cdot|$ to L . Then $|\cdot|_0 = |\cdot|_L$.

Pf: It suffices to prove $|\varpi_L|_0 = |\varpi_L|_L$. Let $x = \varpi$. Then $x = \varpi_L^e \cdot u$ for $u \in \mathcal{O}_K^\times$ as above. Thus

$$|\varpi_L|_0^e = |\varpi_L^e|_0 = |\varpi|_0 = |\varpi| = |\varpi_L|_L^e.$$

Thus $|\varpi_L|_0 = |\varpi_L|_L$ as desired. \square

Corollary 2.27. *Let K be a field complete with respect to a discrete nonarchimedean valuation $|\cdot|$. If L/K is any separable algebraic extension of K , not necessarily finite, then $|\cdot|$ extends uniquely to a nonarchimedean valuation on L .*

Proof. To see this, just look at L as a union of finite extensions where the extension of $|\cdot|$ is already known. \square

One should note that in Corollary 2.27 that the extended valuation is not necessarily discrete and L is not necessarily complete with respect to this valuation as we showed was true in the case of finite extensions.

Theorem 2.28. *Let K be a finite separable extension of \mathbb{Q} and L/K a finite separable extension. Let $|\cdot|$ be a valuation on K . Then there exist finitely many extensions $|\cdot|_1, \dots, |\cdot|_r$ of $|\cdot|$ to L . If \widehat{K} is the completion of K with respect to $|\cdot|$ and L_i the completion of L with respect to $|\cdot|_i$, then*

$$L \otimes_K \widehat{K} \xrightarrow{\cong} \prod_{i=1}^r L_i$$

where the map is given by $\alpha \otimes \beta \mapsto (\alpha \beta_i)$ where β_i is the image of β in L_i .

Proof. The fact that L/K is a finite separable extension gives that there exists $\alpha \in L$ so that $L = K(\alpha) \cong K[x]/(f)$ for $f \in K[x]$ the minimal polynomial of α over K . As our extension is separable, $f(x)$ must have distinct roots.

Let $f(x) = f_1(x) \cdots f_r(x)$ be the factorization of $f(x)$ into irreducibles in $\widehat{K}[x]$. Since $f(x)$ has distinct roots the f_i must all be distinct. Thus, we have

$$\begin{aligned} L \otimes_K \widehat{K} &\cong K[x]/(f) \otimes_K \widehat{K} \\ &\cong \widehat{K}[x]/(f) \\ &\cong \prod_{i=1}^r \widehat{K}[x]/(f_i). \end{aligned}$$

Set $L_i = \widehat{K}[x]/(f_i)$.

Each L_i is a finite separable extension of \widehat{K} , so if $|\cdot|$ is a nonarchimedean valuation then $|\cdot|$ extends uniquely to a nonarchimedean valuation on L_i by Theorem 2.26. If $|\cdot|$ is an archimedean valuation, then \widehat{K} is either \mathbb{R} or \mathbb{C} . This is because $|\cdot|$ restricted to \mathbb{Q} must be the normal absolute value, and so $\widehat{\mathbb{Q}} = \mathbb{R}$ and $\widehat{K} \supseteq \widehat{\mathbb{Q}} = \mathbb{R}$. Thus, L_i must be \mathbb{R} or \mathbb{C} and it is clear the valuation $|\cdot|$ extends uniquely in this case as well. Denote the unique extension of $|\cdot|$ to L_i by $|\cdot|_i$. Note that since we can embed L into L_i , the valuation $|\cdot|_i$ restricts to a valuation on L which we also denote at $|\cdot|_i$.

It remains to show that if $|\cdot|'$ is any extension of $|\cdot|$ to L then $|\cdot|' = |\cdot|_i$ for some $1 \leq i \leq r$ and $|\cdot|_i = |\cdot|_j$ if $i \neq j$. Let $|\cdot|'$ be any extension of $|\cdot|$ to L and let L' be the completion of L with respect to $|\cdot|'$. Recall that L is dense in L' by Proposition 2.12. Thus, we have $L = K(\alpha) \subseteq \widehat{K}(\alpha) \subseteq L'$ since $\widehat{K} \subseteq L'$ and $\alpha \in L'$. We have that $\widehat{K}(\alpha) \cong \widehat{K}[x]/(g)$ where g is the minimal polynomial of α over \widehat{K} . This implies that g must be equal to f_i for some i and so $L \subseteq L_i \subseteq L'$. Thus, the restriction of $|\cdot|'$ to L_i is $|\cdot|_i$ by the uniqueness of the extension of $|\cdot|$ to L_i . However, the completion of L with respect to $|\cdot|_i$ is just L_i and so we must have $L_i = L'$.

Now suppose that $|\cdot|_i = |\cdot|_j$ for $i \neq j$. This gives that $L_i \cong L_j$. However, we know that $K[x]/(f) \not\cong K[x]/(g)$ if $f \neq g$. Thus it must be that $|\cdot|_i \neq |\cdot|_j$ for $i \neq j$ as claimed. \square

Corollary 2.29. *Let K be a number field and L/K a finite separable extension of fields. Let $|\cdot|$ be a valuation on K , \widehat{K} the completion of K with respect to $|\cdot|$, and L_i defined as in Theorem 2.28. Then for $x \in L$ we have*

$$\begin{aligned} \text{Nm}_{L/K}(x) &= \prod_{i=1}^r \text{Nm}_{L_i/\widehat{K}}(x) \\ \text{Tr}_{L/K}(x) &= \sum_{i=1}^r \text{Tr}_{L_i/\widehat{K}}(x). \end{aligned}$$

Proof. Exercise. \square

We are now able to combine Ostrowski's result with Theorems 2.26 and 2.28 to classify the possible valuations on a number field K .

Theorem 2.30. *Let K be a number field and $|\cdot|$ a valuation on K . The valuation $|\cdot|$ is equivalent to either:*

1. $|\cdot|_\sigma$ for some $\sigma : K \hookrightarrow \mathbb{C}$ or
2. $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p} \subseteq \mathfrak{O}_K$ a prime.

Proof. Ostrowski's theorem implies that $|\cdot|$ restricted to \mathbb{Q} is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p . Since K is a finite separable extension of \mathbb{Q} , there are only finitely many possibilities for $|\cdot|$ and they are given as in Theorem 2.28.

Suppose $|\cdot| = |\cdot|_\infty$ on \mathbb{Q} . Write the number field K as $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Then we have $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[x]/(f)$. Write the factorization of $f(x)$ as

$$f(x) = \prod_{i=1}^r (x - \alpha_i) \prod_{j=1}^s ((x - \beta_j)(x - \bar{\beta}_j))$$

for $\alpha_i \in \mathbb{R}$ and $\beta_j \in \mathbb{C}$. Then we have $\mathbb{R}[x]/(f) \cong \mathbb{R}^r \oplus \mathbb{C}^s$ by the map $x \mapsto (\alpha_i) \oplus (\beta_j)$. Thus, we have

$$K \longrightarrow \mathbb{R}^r \oplus \mathbb{C}^s \longrightarrow \mathbb{R} \text{ or } \mathbb{C}$$

by $\alpha \mapsto \alpha_i$ or β_j . Thus, for each i we get an embedding $\sigma_i : K \hookrightarrow \mathbb{R}$ given by $\sigma_i(\alpha) = \alpha_i$ and for each j we get an embedding $\sigma_j : K \hookrightarrow \mathbb{C}$ given by $\sigma_j(\alpha) = \beta_j$. This gives that the only extensions of $|\cdot|_\infty$ to K are the ones given by $|\cdot|_{\sigma_i}$ for σ_i one of the embeddings arising from α_i or β_j .

Now suppose that $|\cdot| = |\cdot|_p$ when restricted to \mathbb{Q} where p is some rational prime. Again we write $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$. Let $f(x) = f_1(x) \dots f_r(x)$ be the factorization of f into irreducibles in \mathbb{Q}_p and write $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i=1}^r K_i$ as in the proof of Theorem 2.28. Let $|\cdot|_i$ be the unique extension of $|\cdot|$ to K_i . We saw in Theorem 2.28 that the valuations $|\cdot|_i$ are precisely the possible extensions of $|\cdot|_p$ to a valuation on K . Thus it only remains to show they are equivalent to $|\cdot|_{\mathfrak{p}}$ for a prime $\mathfrak{p} \subseteq \mathfrak{O}_K$.

Let $\zeta \in \mathfrak{O}_K$. Then there exists $a_i \in \mathbb{Z}$ so that

$$\zeta^n + a_1 \zeta^{n-1} + \dots + a_n = 0.$$

We have

$$|\zeta|_i^n = |a_1 \zeta^{n-1} + \dots + a_n|_i \leq \max_{0 \leq j \leq n-1} |a_j \zeta^j|_i \leq \max_{0 \leq j \leq n-1} |\zeta^j|_i$$

where we use that $|m|_i = |m|_p \leq 1$ for $m \in \mathbb{Z}$. Thus we must have $|\zeta|_i \leq 1$. Thus, $\mathfrak{O}_K \subseteq \mathcal{O}_{K_i}$ for $1 \leq i \leq r$. This implies that $\mathfrak{m}_i \cap \mathfrak{O}_K$ is a prime ideal of \mathfrak{O}_K , call it \mathfrak{p}_i where we write \mathfrak{m}_i to denote the maximal ideal of \mathcal{O}_{K_i} . We know that $\mathfrak{m}_i \cap \mathbb{Z} = (p)$ so we must have $\mathfrak{p}_i | p \mathfrak{O}_K$. Now for $z \in K^\times$, we have

$$|z|_i = |\varpi_i|_i^{\text{ord } \mathfrak{m}_i(z)}$$

where $\text{ord}_{\mathfrak{m}_i}(z)$ is the minimal m so that $z \in \varpi_{K_i}^m \mathcal{O}_{K_i}$, i.e., the minimal m so that $z \in \mathfrak{p}_i^m \mathfrak{D}_K$. Thus we have $|z|_i = |\varpi_i|_i^{\text{ord}_{\mathfrak{p}_i}(z)}$. This gives that $|\cdot|_i$ is equivalent to $|\cdot|_{\mathfrak{p}_i}$ since $|z|_{\mathfrak{p}_i} = (\mathfrak{D}_K/\mathfrak{p}_i)^{-\text{ord}_{\mathfrak{p}_i}(z)}$ and there exists a c so that $|\varpi_i|_i = (\mathfrak{D}_K/\mathfrak{p}_i)^{-c}$. \square

Definition 2.31. 1. Let K be a field complete with respect to a valuation $|\cdot|$ so that the residue field of K is finite. We say the valuation $|\cdot|$ is *normalized* if $|\varpi_K| = (\#k)^{-1}$.

2. Let L be a finite separable extension of \mathbb{Q} . We say a valuation $|\cdot|$ on L is *normalized* if either $|\cdot|$ is nonarchimedean and the extension of $|\cdot|$ to \widehat{L} is normalized or if $|\cdot|$ is archimedean and $|\cdot| = |\cdot|_{\sigma}$ for $\sigma : L \hookrightarrow \mathbb{R}$ if L embeds into \mathbb{R} or $|\cdot| = |\cdot|_{\sigma}^2$ for $\sigma : L \hookrightarrow \mathbb{C}$ when L does not embed into \mathbb{R} . We write $\|\cdot\|$ to denote the valuation is normalized.

Example 2.32. The valuation $\|\cdot\|_p = |\cdot|_p$ is a normalized valuation as $|p|_p = p^{-1}$.

Definition 2.33. Let K be a field. An equivalence class of valuations on K is called a *place of K* or just a *place* if K is clear from context. An equivalence class of archimedean valuations is called an *infinite place* and an equivalence class of nonarchimedean valuations is called a *finite place*. The set of places of K is denoted M_K .

We will often denote a place by v and the completion of K with respect to v by K_v . We will denote the valuation ring of K_v by \mathcal{O}_v , the maximal ideal by \mathfrak{m}_v , and the residue field by k_v . If we need to be careful to indicate that $|\cdot|$ corresponds to v we will write $|\cdot|_v$. The reader should be aware that in some texts the term “place” is referred to as “prime of K ” instead. If L is a finite separable extension of a field K_v , then we have seen that v extends uniquely to a valuation on L . In general we will write v for the extended valuation as well. The reader should be careful not to confuse this with the situation where we begin with a number field K and a finite separable extension L/K . In this case for the valuation v , we have seen that there are finitely many valuations ω of L sitting over v and we write L_{ω} for the completion of L with respect to one of these valuations.

One should note that if K is a number field then Theorem 2.30 gives a bijection between the places and the set containing

1. $\mathfrak{p} \subseteq \mathfrak{D}_K$ a nonzero prime,
2. $\sigma : K \hookrightarrow \mathbb{R}$,
3. pairs $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$.

Places will be of paramount importance when we study adeles and ideles in global class field theory. For now we note the following two results that are important in their own right. Theorems 2.34 and 2.37 are known as the product formulas.

Theorem 2.34. *Let $x \in \mathbb{Q}$. Then*

$$\|x\|_\infty \prod_p \|x\|_p = 1.$$

Proof. Note that the product is actually well-defined as $\|x\|_p = 1$ for all but finitely many p . As valuations are multiplicative, it is enough to show the result when x is a prime. Let $x = q$ be a prime. Then we have

$$\begin{aligned} \|x\|_\infty \prod_p \|x\|_p &= \|q\|_\infty \|q\|_q \\ &= qq^{-1} = 1. \end{aligned}$$

□

Definition 2.35. Let L/K be a finite separable extension of number fields. For $\omega \in M_L$ and $v \in M_K$ we write $\omega | v$ if

1. $\omega = \mathfrak{p}$ and $\mathfrak{p} \cap \mathfrak{O}_K = v$ or
2. $\omega = \sigma$ and $\sigma|_K = v$.

Lemma 2.36. *Let L/K be a finite separable extension of number fields. For $v \in M_K$ and $x \in L$ we have*

$$\prod_{\substack{\omega|v \\ \omega \in M_L}} \|x\|_\omega = \|\mathrm{Nm}_{L/K}(x)\|_v.$$

Proof. Let $\omega | v$. Let $|\cdot|_\omega$ be the extension of $\|\cdot\|_v$ to L equivalent to $\|\cdot\|_\omega$. Let K_v be the completion of K with respect to $\|\cdot\|_v$ and L_ω the completion of L with respect to $\|\cdot\|_\omega$. For $x \in L$ Corollary 2.29 gives

$$\|\mathrm{Nm}_{L/K}(x)\|_v = \left\| \prod_{\omega|v} \mathrm{Nm}_{L_\omega/K_v}(x) \right\|_v.$$

Since $\mathrm{Nm}_{L_\omega/K_v}(x) \in K_v$ we have

$$\left\| \prod_{\omega|v} \mathrm{Nm}_{L_\omega/K_v}(x) \right\|_v = \prod_{\omega|v} |\mathrm{Nm}_{L_\omega/K_v}(x)|_v.$$

We saw in Theorem 2.26 that for $x \in L$ we have

$$|\mathrm{Nm}_{L_\omega/K_v}(x)|_v = |x|_\omega^{\deg(L_\omega/K_v)}.$$

Now observe that if we set $f = \deg(\ell_\omega/k_v)$ and e such $\varpi_v = \varpi_\omega^e$, then

$$\begin{aligned}
 |\varpi_v|_\omega &= \|\varpi_v\|_v \\
 &= (\#k_v)^{-1} \\
 &= (\#\ell_\omega)^{-\frac{1}{f}} \\
 &= \|\varpi_\omega\|_\omega^{\frac{1}{f}} \\
 &= \|\varpi_\omega^e\|_\omega^{\frac{1}{fe}} \\
 &= \|\varpi_v\|_\omega^{\frac{1}{fe}} \\
 &= \|\varpi_v\|_\omega^{\frac{1}{\deg(L_\omega/K_v)}}.
 \end{aligned}$$

Thus, we have

$$\begin{aligned}
 \|\mathrm{Nm}_{L/K}(x)\|_v &= \prod_{\omega|v} |x|_\omega^{\deg(L_\omega/K_v)} \\
 &= \prod_{\omega|v} \|x\|_\omega,
 \end{aligned}$$

as desired. □

Theorem 2.37. *Let K be a number field and $x \in K$. Then*

$$\prod_{\omega \in M_K} \|x\|_\omega = 1.$$

Proof. Essentially all of the work for this proof has been carried out in proving Theorem 2.34 and Lemma 2.36. Let $x \in K$. Then we have

$$\begin{aligned}
 \prod_{\omega \in M_K} \|x\|_\omega &= \prod_{v \in M_\mathbb{Q}} \prod_{\omega|v} \|x\|_\omega \\
 &= \prod_{v \in M_\mathbb{Q}} \|\mathrm{Nm}_{K/\mathbb{Q}}(x)\|_v \\
 &= 1.
 \end{aligned}$$

□

Chapter 3

Local Fields

3.1 Definitions and basic facts

In this chapter we study local fields. These fields and their abelian extensions will be the objects of study in local class field theory and so are very important to our subject.

Definition 3.1. A field K_v is a *local field* if it is locally compact with respect to a valuation v . (Unless otherwise noted all of our local fields have characteristic 0.)

In the case that the valuation v is an archimedean valuation, one can show that the field K_v must be either \mathbb{R} or \mathbb{C} . As we feel we understand these fields fairly well, we will focus on the case when v is discrete and nonarchimedean.

Proposition 3.2. *Let K_v be complete with respect to a discrete nonarchimedean valuation v . We have that \mathcal{O}_v is compact if and only if k_v is finite.*

Proof. Let S be a set of representatives for k_v . Suppose that \mathcal{O}_v is compact. As \mathcal{O}_v is the disjoint union of the sets $s + \mathfrak{m}_v$ for $s \in S$ and each of these is open, it must be that S is finite.

Now suppose that k_v is finite. We begin by observing that \mathcal{O}_v is both open and closed. It is open because there exists $\delta > 0$ so that $\mathcal{O}_v = \{x \in K_v : |x| < 1 + \delta\}$ since the valuation $|\cdot|$ is discrete. It is closed because $\mathcal{O}_v = \{x \in K_v : |x| \leq 1\}$.

Observe that we have

$$\mathcal{O}_v \cong \varprojlim_n \mathcal{O}_v / \varpi_v^n \mathcal{O}_v \subseteq \prod_n \mathcal{O}_v / \varpi_v^n \mathcal{O}_v.$$

Each set $\mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ is a finite set (since k_v is finite) and so is compact. Thus, the product $\prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ is a compact set since it is a product of compact sets.

We now show that \mathcal{O}_v is closed in $\prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ and since this product is compact, this will force \mathcal{O}_v to be compact as well. Let $(x_n) \in \prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ be

a point that is not in \mathcal{O}_v . Since this point is not in \mathcal{O}_v , there exists r, s so that $x_r \not\equiv x_s \pmod{\varpi_v^r}$ for $r < s$. Set \mathcal{U} to be the set defined by

$$\mathcal{U} = \prod_{n>s} \mathcal{O}_v / \varpi_v^n \mathcal{O}_v \times \{x_s\} \times \cdots \times \{x_1\}.$$

Any point in \mathcal{U} must contain x_r and x_s and so $\mathcal{U} \cap \mathcal{O}_v = \emptyset$. Thus, the point (x_n) has a neighborhood \mathcal{U} that does not meet \mathcal{O}_v . If we show that \mathcal{U} is open then every point in $\prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v - \mathcal{O}_v$ will have an open neighborhood that does not meet \mathcal{O}_v . This will imply that \mathcal{O}_v is closed as we will have $\prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v - \mathcal{O}_v$ is open. Since each $\mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ is finite, the sets $\{x_i\} \subset \mathcal{O}_v / \varpi_v^i \mathcal{O}_v$ are open. Thus, we must have that \mathcal{U} is open. Thus, \mathcal{O}_v is closed in the compact set $\prod \mathcal{O}_v / \varpi_v^n \mathcal{O}_v$ and so is compact. \square

Corollary 3.3. *If K_v is a local field with v a discrete nonarchimedean valuation, then k_v is finite.*

Proof. Observe that the open sets $\varpi^n \mathcal{O}_v$ form a fundamental system of open neighborhoods of 0. The fact that K_v is locally compact implies there exists a m so that $\varpi^m \mathcal{O}_v$ is compact. Multiplying by ϖ^{-m} we see that \mathcal{O}_v is compact which allows us to apply the previous proposition to conclude that k_v is finite. \square

We call a field K_v a nonarchimedean local field if v is a discrete nonarchimedean valuation and K_v is a local field with respect to this valuation.

Exercise 3.4. *Let K_v be a nonarchimedean local field. The fractional ideals of K_v are all compact as is \mathcal{O}_v^\times .*

Exercise 3.5. *Let K_v be a nonarchimedean local field (of characteristic 0). Prove that K_v is a finite extension of \mathbb{Q}_p for some prime p .*

We end this section with a useful decomposition of the multiplicative group of a nonarchimedean local field.

Proposition 3.6. *Let K_v be a nonarchimedean local field and let $q = \#k_v$. Then we have*

$$K_v^\times = \varpi_v^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)}$$

where $\varpi_v^{\mathbb{Z}} = \{\varpi_v^k : k \in \mathbb{Z}\}$, μ_{q-1} is the group of $(q-1)^{\text{st}}$ roots of unity, and $U^{(1)} = 1 + \mathfrak{m}_v$.

Proof. Let $\alpha \in K_v^\times$. We know that α has a unique representation in the form $\alpha = u\varpi_v^r$ for some $r \in \mathbb{Z}$ and $u \in \mathcal{O}_v^\times$. Thus, we have that $K_v^\times = \varpi_v^{\mathbb{Z}} \times \mathcal{O}_v^\times$ so it only remains to analyze \mathcal{O}_v^\times . Consider the polynomial $f(x) = x^{q-1} - 1$. This polynomial splits into linear factors in k_v and hence splits into linear factors in \mathcal{O}_v^\times by Hensel's lemma. Thus, \mathcal{O}_v^\times must contain μ_{q-1} . The surjective homomorphism $\mathcal{O}_v^\times \rightarrow k_v^\times$ given by $x \mapsto x \pmod{\mathfrak{m}_v}$ has kernel $U^{(1)}$ and so we obtain the result. \square

3.2 Krasner's Lemma

Let K_v be a nonarchimedean local field. Given $h = a_n x^n + \cdots + a_1 x + a_0 \in K_v[x]$, define $\|h\| = \max |a_i|$. Let $f, g \in K_v[x]$ be monic and irreducible with $\|f - g\|$ small. We will show that the roots of f and g yield the same extensions of K_v . We will conclude the section by showing that $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ injects into $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Lemma 3.7. *Let K_v be a nonarchimedean local field, $\alpha \in K_v^{\text{sep}}$ and $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$. Then $|\alpha|_{K_v^{\text{sep}}} = |\sigma(\alpha)|_{K_v^{\text{sep}}}$.*

Proof. The valuations $x \mapsto |x|_{K_v^{\text{sep}}}$ and $x \mapsto |\sigma(x)|_{K_v^{\text{sep}}}$ are both extensions of $|\cdot|$ to K_v^{sep} . Thus the extensions must be equal by the uniqueness statement in Corollary 2.27. \square

The following lemma is known as Krasner's lemma and forms a basis for the rest of the results in this section.

Lemma 3.8. *Let K_v be a nonarchimedean local field. Suppose there exists $\alpha, \beta \in K_v^{\text{sep}}$ so that*

$$|\alpha - \beta| < |\alpha - \sigma(\alpha)|$$

for all $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ with $\sigma(\alpha) \neq \alpha$, i.e., β is closer to α than all of its nontrivial Galois-conjugates. Then $K_v(\alpha) \subseteq K_v(\beta)$.

Proof. We know from Corollary 3.7 that for all $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ we have

$$|\alpha - \beta| = |\sigma(\alpha) - \sigma(\beta)|.$$

Let σ be such that $\sigma(\beta) = \beta$. This gives

$$|\alpha - \beta| = |\sigma(\alpha) - \beta|$$

for all such σ . Thus, we have

$$\begin{aligned} |\sigma(\alpha) - \alpha| &= |\sigma(\alpha) - \beta + \beta - \alpha| \\ &\leq |\alpha - \beta| \end{aligned}$$

which contradicts our assumption that β is closer to α than any of its conjugates unless $\sigma(\alpha) = \alpha$ for all σ fixing β . Thus it must be the case that if $\sigma(\beta) = \beta$ then $\sigma(\alpha) = \alpha$, i.e., we must have $K_v(\alpha) \subseteq K_v(\beta)$ by Galois theory. \square

One should note that the above lemma is clearly false if one does not require K_v to be a nonarchimedean local field. For example, if one looks at \mathbb{Q} with $\alpha = \sqrt{2}$ then one can satisfy the hypotheses of the theorem with $\beta = 1$ but clearly $\mathbb{Q}(\sqrt{2})$ is not a subfield of \mathbb{Q} .

Definition 3.9. Let K_v be a nonarchimedean local field and let $\alpha, \beta \in K_v^{\text{sep}}$. We say that β *belongs to* α if $|\alpha - \beta| < |\sigma(\alpha) - \alpha|$ for every $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ with $\sigma(\alpha) \neq \alpha$.

Lemma 3.10. *Let K_v be a nonarchimedean local field, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K_v[x]$ be separable and irreducible, and $\alpha \in K_v^{\text{sep}}$ a root of f . There exists $c(f) > 0$ such that if $g(x) \in K_v[x]$ is any monic polynomial such that $\|g - f\| \leq c(f)$, then g has a root β that belongs to α . Moreover, g is irreducible, $\deg(g) = \deg(f)$, and $K_v(\alpha) = K_v(\beta)$.*

Proof. Pick $c(f)$ such that

1. $c(f) < \min(1, \|f\|)$
2. $c(f) < \min_{\sigma(\alpha) \neq \alpha} (c_1^{-1} |\sigma(\alpha) - \alpha|^n)$ where $c_1 = \max_{\substack{0 \leq m \leq n-1 \\ 0 \leq j \leq n-1}} \|f\|^{\frac{m}{n-j}}$.

Suppose that g is such that $\|g - f\| \leq c(f)$. If $\deg(f) \neq \deg(g)$, the fact that f and g are monic would give that $c(f) \geq 1$. Thus it must be that $\deg(g) = \deg(f) = n$. We also have

$$\begin{aligned} \|g\| &= \|f + (g - f)\| \\ &\leq \max(\|f\|, \|g - f\|) \\ &\leq \|f\| \end{aligned}$$

since $\|g - f\| \leq c(f)$ and $c(f) \leq \|f\|$.

Let $g = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ and let β_0 be any root of g . We have

$$\begin{aligned} |\beta_0^n| &= \left| \sum_{i=0}^{n-1} b_i \beta_0^i \right| \\ &\leq \max_{0 \leq i \leq n-1} |b_i| |\beta_0|^i. \end{aligned}$$

Thus, for some j we have

$$\begin{aligned} |\beta_0|^{n-j} &\leq \|g\| \\ &\leq \|f\|. \end{aligned}$$

If we write $(f - g)(x) = \sum_{m=0}^{n-1} c_m x^m$, then

$$\begin{aligned} |f(\beta_0)| &= |(f - g)(\beta_0)| \\ &\leq \max_{0 \leq m \leq n-1} |c_m| |\beta_0|^m \\ &\leq c(f) \max_{0 \leq m \leq n-1} |\beta_0|^m \\ &\leq c(f) \max_{0 \leq m \leq n-1} (\|f\|)^{m/(n-j)} \quad (\text{for some } j) \\ &< \min_{\sigma(\alpha) \neq \alpha} |\sigma(\alpha) - \alpha|^n. \end{aligned}$$

On the other hand, if we let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of f , then we have

$$\prod_{i=1}^n |\beta_0 - \alpha_i| = |f(\beta_0)| < \min_{\sigma(\alpha) \neq \alpha} |\sigma(\alpha) - \alpha|^n$$

for every σ such that $\sigma(\alpha) \neq \alpha$. Thus, there exists $1 \leq i \leq n$ so that $|\beta_0 - \alpha_i| < |\sigma(\alpha) - \alpha|$ for every σ such that $\sigma(\alpha) \neq \alpha$. Since f is irreducible, there exists $\sigma_i \in \text{Gal}(K_v^{\text{sep}}/K_v)$ such that $\sigma_i(\alpha_i) = \alpha$. Put $\beta_i = \sigma_i(\beta_0)$. Then for every $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ such that $\sigma(\alpha) \neq \alpha$ we have

$$\begin{aligned} |\beta_i - \alpha| &= |\sigma_i(\beta_0) - \sigma_i(\alpha_i)| \\ &= |\beta_0 - \alpha_i| \\ &< |\sigma(\alpha) - \alpha|. \end{aligned}$$

Thus, β_i belongs to α .

It only remains to show that $K_v(\alpha) = K_v(\beta_i)$. Once we have shown this we will know that g must be irreducible. Suppose $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ with $\sigma(\alpha) \neq \alpha$ and $\sigma(\beta) = \beta$. We have seen that $|\beta_i - \alpha| < |\sigma(\alpha) - \alpha|$, so by Lemma 3.8 we have $K_v(\alpha) \subseteq K_v(\beta_i)$. On the other hand,

$$\begin{aligned} \deg(f) &= \deg(K_v(\alpha)/K_v) \\ &\leq \deg(K_v(\beta_i)/K_v) \\ &= \deg(g). \end{aligned}$$

However, we have already seen that $\deg(f) = \deg(g)$ and so we must have $K_v(\alpha) = K_v(\beta_i)$. \square

Corollary 3.11. *Let f, g and $c(f)$ be as in Lemma 3.10. Then every root of g belongs to exactly one root of f . So, in particular, the roots of g yield the same extensions as the roots of f .*

Proof. Let α be a root of f . Then by Lemma 3.10 there exists a root β of g belonging to α . Let $\beta = \beta_1, \dots, \beta_n$ be the roots of g . Since g is irreducible by Lemma 3.10, there exists $\sigma \in \text{Gal}(K_v^{\text{sep}}/K_v)$ so that $\beta_i = \sigma_i(\beta)$. Thus, β_i belongs to $\sigma(\alpha_i)$, which is also a root of f . Suppose now that β is a root of g belonging to two roots of f , say α and $\sigma(\alpha)$. Then $|\alpha - \beta| < |\tau(\alpha) - \alpha|$ for all $\tau \in \text{Gal}(K_v^{\text{sep}}/K_v)$ so that $\tau(\alpha) \neq \alpha$, and $|\sigma(\alpha) - \beta| < |\eta(\sigma(\alpha)) - \sigma(\alpha)|$ for all $\eta \in \text{Gal}(K_v^{\text{sep}}/K_v)$ so that $\eta(\sigma(\alpha)) \neq \sigma(\alpha)$. In particular, if we set $\tau = \sigma$ and $\eta = \sigma^{-1}$ then we have $|\sigma(\alpha) - \beta| < |\sigma(\alpha) - \alpha|$ and $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Thus,

$$\begin{aligned} |\sigma(\alpha) - \alpha| &= |(\sigma(\alpha) - \beta) + (\beta - \alpha)| \\ &< |\sigma(\alpha) - \alpha|. \end{aligned}$$

This is clearly a contradiction and finishes the proof. \square

Corollary 3.12. *Let K/\mathbb{Q}_p be a finite separable extension. Fix $\overline{\mathbb{Q}_p}$ an algebraic closure of \mathbb{Q}_p and an embedding $\mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}_p}$. Then there exists a finite extension F/\mathbb{Q} such that $K = F \cdot \mathbb{Q}_p \subseteq \overline{\mathbb{Q}_p}$.*

Proof. Suppose $K = \mathbb{Q}_p(\alpha)$ with α having $f \in \mathbb{Q}_p[x]$ as its minimal monic polynomial. Choose $g \in \mathbb{Q}[x] \subset \mathbb{Q}_p[x]$ such that $\|f - g\| < c(f)$ where $c(f)$ is as in Lemma 3.10. Note that this is possible because \mathbb{Q} is dense in \mathbb{Q}_p . Thus, g has a root $\beta \in \overline{\mathbb{Q}}$ such that $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha)$ by Lemma 3.10. However, $\mathbb{Q}_p(\beta) = \mathbb{Q}(\beta) \cdot \mathbb{Q}_p$ since $\beta \in \overline{\mathbb{Q}}$. Thus, if we set $F = \mathbb{Q}(\beta)$ we are done. \square

Fix algebraic closures $\overline{\mathbb{Q}}, \overline{\mathbb{Q}_p}$ and compatible embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}, \mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}, \mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}_p}$, and $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Any automorphism of $\overline{\mathbb{Q}_p}$ fixing \mathbb{Q}_p restricts to an automorphism of $\overline{\mathbb{Q}}$ fixing \mathbb{Q} . In other words, the restriction yields a homomorphism

$$\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

We claim that this map is injective. Let $\sigma \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and let $\alpha \in \overline{\mathbb{Q}_p}$ such that $\sigma(\alpha) \neq \alpha$. Set $L = \mathbb{Q}_p(\alpha)$. Then by Corollary 3.12 there exists $F/\mathbb{Q}, F \subseteq \overline{\mathbb{Q}}$ such that $L = F \cdot \mathbb{Q}_p$. Since σ acts non-trivially on α , hence on L , σ cannot fix F . So the image of σ is non-trivial. The fact that this map is an injection will be very important in our study of global class field theory and is very important in general as we will see that $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is isomorphic to the decomposition group at p .

3.3 Eisenstein Extensions

We begin by recalling the Eisenstein irreducibility criterion from elementary abstract algebra.

Lemma 3.13. *Let R be a ring and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$. If there exists a prime ideal $\mathfrak{p} \subseteq R$ such that $a_n \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ for $i = 1, \dots, n$, and $a_0 \notin \mathfrak{p}^2$, then f is irreducible. Moreover, if f is monic and R is integrally closed, then (f) is a prime ideal in $R[x]$.*

Definition 3.14. Let K be any field and let \mathfrak{p} be a prime ideal of \mathfrak{O}_K . If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathfrak{O}_K[x]$, $a_i \in \mathfrak{p}$, and $a_0 \notin \mathfrak{p}^2$, then we call f an *Eisenstein polynomial*.

Observe that an Eisenstein polynomial is necessarily an irreducible polynomial by Lemma 3.13.

Definition 3.15. An extension L/K_v is *Eisenstein* if $L = K_v(\alpha)$ with α a root of an Eisenstein polynomial.

Lemma 3.16. *If K_v is a nonarchimedean local field, then there are only finitely many Eisenstein extensions of K_v of fixed degree. (If we wanted to include positive characteristic, one would get finitely many Eisenstein extensions of fixed degree prime to $\text{char}(K_v)$.)*

Proof. Let $\mathcal{A} = \mathfrak{m}_v \times \cdots \times \mathfrak{m}_v \times (\mathfrak{m}_v - \mathfrak{m}_v^2)$ where there are $n - 1$ factors \mathfrak{m}_v . If $\mathbf{a} = (a_{n-1}, \dots, a_0) \in \mathcal{A}$, then $f_{\mathbf{a}}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_v[x]$ is irreducible because it is an Eisenstein polynomial. Every Eisenstein extension of

K_v of degree n arises from adjoining a root of some $f_{\mathbf{a}}$ with $\mathbf{a} \in \mathcal{A}$. We can apply Corollary 3.11 to conclude that for each $\mathbf{a} \in \mathcal{A}$, there exists a neighborhood $U_{\mathbf{a}} \subseteq \mathcal{A}$ of \mathbf{a} such that if $\mathbf{b} \in U_{\mathbf{a}}$, then the roots of $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$ yield the same extensions of K_v . We have that \mathfrak{m}_v is compact as it is a closed subset of the compact set \mathcal{O}_v by the discreteness of v , \mathfrak{m}_v^2 is both open and closed because $\mathfrak{m}_v^2 = \{x : |x| \leq |\varpi|^2\} = \{x : |x| < |\varpi|\}$. Thus $\mathfrak{m}_v - \mathfrak{m}_v^2$ is closed in \mathfrak{m}_v , a compact set and hence is compact itself. The set \mathcal{A} is the product of compact sets, so is also compact. Thus there exist $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathcal{A}$ such that $\mathcal{A} = \bigcup_{i=1}^m U_{\mathbf{a}_i}$.

So every Eisenstein extension of K_v of degree n is of the form $K_v(\alpha)$ with α a root of $f_{\mathbf{a}_i}$ for some $i \in \{1, \dots, m\}$. Thus there can be only finitely many such extensions. \square

Recall that given Dedekind domains $\mathfrak{o} \subseteq \mathfrak{D}$ we say a prime ideal \wp of \mathfrak{D} is *totally ramified* over a prime ideal $\mathfrak{p} \subset \mathfrak{o}$ if $\wp \mid \mathfrak{p}$ and $f(\wp/\mathfrak{p}) = [\mathfrak{D}/\wp : \mathfrak{o}/\mathfrak{p}] = 1$. In the case of an extension of nonarchimedean local fields L/K_v , the extension is said to be *totally ramified* if \mathfrak{m}_L is totally ramified over \mathfrak{m}_v .

Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathcal{O}_v[x]$ be a separable Eisenstein polynomial. Let $\alpha_1, \dots, \alpha_n$ be the roots of f and let ϖ_v be a uniformizer of K_v . By Lemma 3.7 $|\alpha_i| = |\alpha_j|$ for every i, j where $|\cdot|$ is the extension of $|\cdot|$ to K_v^{sep} . We have that $a_0 = (-1)^n \prod \alpha_i$ and so $|\alpha_i|^n = \prod |\alpha_i| = |a_0| = |\varpi_v|$ since $a_0 \in \mathfrak{m}_v - \mathfrak{m}_v^2$. So in particular we have that $|\alpha_i| = |\varpi_v|^{1/n}$ for each i . Let $L_i = K_v(\alpha_i)$ and let ϖ_{L_i} be a uniformizer of \mathcal{O}_{L_i} . Write $\varpi_v = \varpi_{L_i}^{e_i} \cdot u_i$ and $\alpha_i = \varpi_{L_i}^{m_i} \cdot v_i$ for some $u_i, v_i \in \mathcal{O}_{L_i}^\times$ and some $e_i, m_i \geq 0$. We know that $\deg(L_i/K_v) = n$ and so $e_i \leq e_i f_i = n$. We have

$$\begin{aligned} |\varpi_v|^{1/n} &= |\alpha_i| \\ &= |\varpi_{L_i}|^{m_i} \\ &= (|\varpi_v|^{1/e_i})^{m_i} \\ &= |\varpi_v|^{m_i/e_i}. \end{aligned}$$

Thus, $n = \frac{e_i}{m_i} \leq e_i$ and so we must have $m_i = 1$ and $e_i = n$. Hence α_i is a uniformizer of \mathcal{O}_{L_i} since $\alpha_i = \varpi_{L_i} \cdot v_i$.

Lemma 3.17. *Let K_v be a nonarchimedean local field. Suppose L/K_v is separable and Eisenstein. Then*

1. L is totally ramified over K_v , i.e., (ϖ_v) is totally ramified in \mathcal{O}_L .
2. If $L = K_v(\alpha)$ with α a root of an Eisenstein polynomial over K_v , then α is a uniformizer of L .
3. If ϖ_L is any uniformizer of L , then $\mathcal{O}_L = \mathcal{O}_{K_v}[\varpi_L]$.

Proof. We have already shown the first two claims above so it only remains to prove the third claim. Let $n = \deg(L/K_v)$. Since L/K_v is totally ramified we

must have $f(\varpi_L/\varpi_v) = 1$, i.e., $\mathcal{O}_v/(\varpi_v) \xrightarrow{\cong} \mathcal{O}_L/(\varpi_L)$. Thus we have

$$(3.1) \quad \mathcal{O}_L = \mathcal{O}_v + \varpi_L \mathcal{O}_L = \mathcal{O}_v[\varpi_L] + \varpi_L \mathcal{O}_L.$$

Let $\alpha \in \mathcal{O}_L$. Write $\alpha = \alpha_1 + \beta_1$ for some $\alpha_1 \in \mathcal{O}_v[\varpi_L]$ and $\beta_1 \in \varpi_L \mathcal{O}_L$. Multiplying equation (3.1) by ϖ_L we obtain

$$(3.2) \quad \varpi_L \mathcal{O}_L = \varpi_L \mathcal{O}_v[\varpi_L] + \varpi_L^2 \mathcal{O}_L.$$

We can now write $\beta_1 = \varpi_L \alpha_2 + \varpi_L^2 \beta_2$ with $\alpha_2 \in \mathcal{O}_v[\varpi_L]$ and $\beta_2 \in \mathcal{O}_L$. Continuing in this fashion we produce α_i and β_i so that

$$\alpha = \alpha_1 + \alpha_2 \varpi_L + \cdots + \alpha_m \varpi_L^{m-1} + \beta_m \varpi_L^m$$

with $\alpha_1 + \alpha_2 \varpi_L + \cdots + \alpha_{m+1} \varpi_L^m \in \mathcal{O}_v[\varpi_L]$ and $\beta_{m+1} \in \mathcal{O}_L$ for all $m \in \mathbb{N}$. Thus, for all $m \in \mathbb{N}$ we have $\mathcal{O}_L = \mathcal{O}_v[\varpi_L] + \varpi_L^m \mathcal{O}_L$.

Observe that the discriminant is given by

$$\begin{aligned} \Delta &= \Delta_{\mathcal{O}_L/\mathcal{O}_v}(1, \varpi_L, \dots, \varpi_L^{n-1}) \\ &= \varpi_v^M \cdot u \end{aligned}$$

for some $M \geq 0$ and some $u \in \mathcal{O}_v^\times$ since the discriminant is necessarily in \mathcal{O}_v . However, we know that $\varpi_v \mathcal{O}_L = \varpi_L^n \mathcal{O}_L$ and so we have $\Delta_{\mathcal{O}_L} = \varpi_L^{Mn} \mathcal{O}_L$.

Let $\gamma \in \mathcal{O}_L$ and write $\gamma = a_0 + a_1 \varpi_L + \cdots + a_{n-1} \varpi_L^{n-1}$ with $a_i \in L$. We have

$$(\mathrm{Tr}_{L/K_v}(\varpi_L^i \varpi_L^j)) \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{L/K_v}(\gamma) \\ \vdots \\ \mathrm{Tr}_{L/K_v}(\varpi_L^{n-1} \gamma) \end{pmatrix}$$

where we have used that the trace map is linear. We have that $\mathrm{Tr}_{L/K_v}(\varpi_L^i \varpi_L^j) \in \mathcal{O}_v$ for all $1 \leq i, j \leq n-1$ since $\varpi_L \in \mathcal{O}_L$ and $\mathrm{Tr}_{L/K_v}(\varpi_L^i \gamma) \in \mathcal{O}_v$ for all $1 \leq i \leq n-1$ as $\varpi_L^i \gamma \in \mathcal{O}_L$ for all $1 \leq i \leq n-1$. Thus we apply Cramer's rule to conclude that $\Delta_{\mathcal{O}_L} \subseteq \mathcal{O}_v$.

Using this exercise if we choose m so that $m \geq Mn$ then we have $\mathcal{O}_L = \mathcal{O}_v[\varpi_L] + \varpi_L^m \mathcal{O}_L \subseteq \mathcal{O}_v[\varpi_L]$ and thus $\mathcal{O}_L = \mathcal{O}_v[\varpi_L]$. \square

Theorem 3.18. *Let K_v be a nonarchimedean local field. A finite separable extension L/K_v is totally ramified if and only if L/K_v is Eisenstein.*

Proof. We have just shown that Eisenstein extensions are totally ramified, so it only remains to show that all totally ramified extensions are Eisenstein. Let L/K_v be totally ramified with $\deg(L/K_v) = n$. Consider the intermediate field $L_1 = K_v(\varpi_L)$. Since L/K_v is totally ramified, L_1/K_v must also be totally ramified. Thus, we have $|\varpi_v| = |\varpi_L|^n$ since L/K_v is totally ramified and $|\varpi_v| = |\varpi_L|^{\deg(L_1/K_v)}$ since L_1/K_v is totally ramified and $\varpi_L \in L_1$. Thus, we must have $\deg(L_1/K_v) = n$ and so $L_1 = L$.

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_v[x]$ be the minimal polynomial of ϖ_L over K_v . Let $\varpi_L = \varpi_1, \dots, \varpi_n$ be the roots of f . We have that $|\varpi_i| = |\varpi_j|$ for

every i, j and $|\varpi_1| < 1$ since it is a uniformizer, i.e., $\mathfrak{m}_L = \varpi_L \mathcal{O}_L$. Thus $|a_i| < 1$ since the a_i 's are symmetric polynomials in the ϖ_i . Hence we have $a_i \in \mathfrak{m}_v$. We also have

$$|a_0| = \prod_{i=1}^n |\varpi_i| = |\varpi_L|^n = |\varpi_v|$$

again using that L/K_v is totally ramified. Thus $a_0 = u\varpi_v$ for some $u \in \mathcal{O}_v^\times$. Hence $a_0 \in \mathfrak{m}_v - \mathfrak{m}_v^2$ and so f is Eisenstein. \square

Corollary 3.19. *If K_v is a nonarchimedean local field then there are only finitely many extensions of K_v of a fixed degree that are totally ramified. (Again, if one wants to include the case of positive characteristic, one gets extensions of fixed degree prime to $\text{char}(K_v)$.)*

Exercise 3.20. (a) *Show that there is a totally ramified extension of \mathbb{Q}_7 of degree n for any integer $n > 1$.*

(b) *Find two nonisomorphic totally ramified extensions of \mathbb{Q}_5 of degree 2. Can you do the same for degree 3?*

3.4 Unramified Extensions

Now that we have characterized the totally ramified extensions of nonarchimedean local fields, the next natural step is to consider unramified extensions. Let $\mathfrak{o} \subseteq \mathfrak{D}$ be Dedekind domains and \mathfrak{p} a prime ideal in \mathfrak{o} . Let \wp_1, \dots, \wp_r be prime ideals of \mathfrak{D} and e_1, \dots, e_r be positive integers so that $\mathfrak{p}\mathfrak{D} = \wp_1^{e_1} \cdots \wp_r^{e_r}$. We say \wp_i is *unramified* over \mathfrak{p} if $e_i = 1$. In the case of an extension of nonarchimedean local fields L/K_v , we say the extension is *unramified* if \mathfrak{m}_L is unramified over \mathfrak{m}_v . The following theorem classifies the finite separable unramified extensions of a nonarchimedean local field in terms of finite extensions of its residue field.

Theorem 3.21. *Let K_v be a local field with residue field k_v . There is a bijection*

$$\{L/K_v \text{ finite, separable, unramified}\} \longleftrightarrow \{l/k_v \text{ finite}\}.$$

where $L \mapsto l = \mathcal{O}_L/\mathfrak{m}_L$.

This satisfies:

1. *If L_1 and L_2 are finite separable unramified extensions of K_v with residue fields l_1 and l_2 respectively, then $L_1 \subseteq L_2$ if and only if $l_1 \subseteq l_2$;*
2. *$\text{Gal}(L/K_v) \cong \text{Gal}(l/k_v)$ by $\sigma \mapsto \sigma|_{\mathcal{O}_L}$.*

Proof. Let $p = \text{char}(k_v)$. We break the proof into several steps.

Step 1: Let m be a positive integer so that $\text{gcd}(p, m) = 1$. The irreducible factors of $x^m - 1$ in $k_v[x]$ are the reductions modulo \mathfrak{m}_v of the irreducible factors of $x^m - 1$ in $\mathcal{O}_v[x]$.

Pf: Write $x^m - 1 = g_1^{n_1}(x) \cdots g_r^{n_r}(x)$ in $\mathcal{O}_v[x]$. We need to show that if $\bar{g}_i(x) \in k_v[x]$ is the reduction of $g_i(x)$ modulo \mathfrak{m}_v , then $\bar{g}_i(x)$ is still irreducible. The fact that $\gcd(p, m) = 1$ gives that $x^m - 1$ is separable and hence so are the g_i and \bar{g}_i .

Let $\bar{f} \in k_v[x]$ be a monic irreducible factor of \bar{g}_i and let $f \in \mathcal{O}_v[x]$ be a monic polynomial such that the reduction of f modulo \mathfrak{m}_v is \bar{f} . Note that f is necessarily irreducible for otherwise \bar{f} would be reducible. Let α be any root of f and put $E = K_v(\alpha)$. We have

$$\deg(E/K_v) = \deg(f) = \deg(\bar{f}) \leq \deg(\bar{g}_i) = \deg(g_i).$$

On the other hand, \bar{g}_i has a root in k_E . Namely, since $f(\alpha) = 0$, we have that $\bar{f}(\bar{\alpha}) = 0$ in k_v . Since $\bar{f} \mid \bar{g}_i$, we must have that $\bar{g}_i(\bar{\alpha}) = 0$ in k_v . The fact that \bar{g}_i is separable implies that we can apply Hensel's lemma to conclude that g_i has a root $\beta \in \mathcal{O}_E$. This gives $K_v(\beta) \subseteq E$. In particular,

$$\deg(g_i) = \deg(K_v(\beta)/K_v) \leq \deg(E/K_v) \leq \deg(g_i)$$

i.e., $\deg(g_i) = \deg(E/K_v)$. Thus we have $\deg(\bar{f}) = \deg(\bar{g}_i)$ and so \bar{g}_i is irreducible as claimed.

Step 2: Let l/k_v be a separable extension of degree n . Then there exists a unique unramified extension K_n/K_v that is separable, finite, and has residue field l .

Pf: We have that there exists $\bar{\alpha}$ such that $l = k_v(\bar{\alpha})$. Set $m = \#l - 1$. Then $\bar{\alpha}$ is a root of $x^m - 1 \in k_v[x]$ as l^\times is a cyclic group of order m . Let \bar{f} be the minimal monic polynomial of $\bar{\alpha}$ over k_v , i.e., \bar{f} is some irreducible factor of $x^m - 1$ in $k_v[x]$. By Step 1 there exists an irreducible factor $f \in \mathcal{O}_v[x]$ of $x^m - 1$ reducing to \bar{f} modulo \mathfrak{m}_v . Let β be any root of f . Set $K_n = K_v(\beta)$. Then

$$\deg(K_n/K_v) = \deg(f) = \deg(\bar{f}) = \deg(l/k_v) = n.$$

We always have that

$$n \geq f(K_n/K_v) = \deg_{k_v}(\mathcal{O}_{K_n}/\mathfrak{m}_{K_n})$$

by general results on the residue class degree. Thus

$$n \geq f(K_n/K_v) = \deg_{k_v}(\mathcal{O}_{K_n}/\mathfrak{m}_{K_n}) \geq \deg(k_v(\bar{\beta})/k_v) = n$$

as $k_v(\bar{\beta}) \subseteq \mathcal{O}_{K_n}/\mathfrak{m}_{K_n}$. Thus $f(K_n/K) = n$ which gives that K_n/K_v is unramified and $l = \mathcal{O}_{K_n}/\mathfrak{m}_{K_n}$ since they are the same degree field extension of the finite field k_v .

It remains to prove uniqueness. Suppose L/K_v is such that the residue field of L is l . Since \bar{f} has a root $\bar{\alpha}$ in l and \bar{f} is necessarily separable, f has a root α in \mathcal{O}_L by Hensel's Lemma. Thus we have $K_v(\alpha) \subseteq L$ and $K_v(\alpha) \cong K_n$. Now if L is unramified, then $n = \deg(L/K_v)$ and so $L = K_v(\alpha) \cong K_n$. This gives

the uniqueness. The same argument also gives part (1) of the theorem.

Step 3: Let l/k_v be a finite separable extension of degree n . Then $\text{Gal}(K_n/K_v) \cong \text{Gal}(l/k_v)$.

Pf: Let f and \bar{f} be as in Step 2. By Hensel's Lemma any root of \bar{f} in l lifts to a root of f in \mathcal{O}_{K_n} . Let $\alpha_1, \dots, \alpha_n$ be the roots of f and $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ be in k_v such that $\bar{\alpha}_i = \alpha_i \pmod{\mathfrak{m}_{K_n}}$. Let $\sigma \in \text{Gal}(K_n/K_v)$ be such that $\sigma \neq 1$. Then there exists i, j such that $\sigma(\alpha_i) = \alpha_j$ with $i \neq j$. Set $\bar{\sigma}$ to be the image of σ in $\text{Gal}(l/k_v)$. Then $\bar{\sigma}(\bar{\alpha}_i) = \bar{\sigma}(\alpha_i) = \bar{\alpha}_j \neq \bar{\alpha}_i$. Thus $\bar{\sigma} \neq 1$. Hence the kernel of the map $\text{Gal}(K_n/K_v) \rightarrow \text{Gal}(l/k_v)$ is $\{1\}$. The fact that both Galois groups are of order n allows us to conclude that this is an isomorphism. \square

The following corollary is implicit in the arguments given in the previous proof. We state and prove it here for clarity as it will be needed in the future.

Corollary 3.22. *Let $f(x) \in \mathcal{O}_v[x]$ be a monic polynomial so that its reduction $\bar{f}(x) \in k_v[x]$ is a monic separable polynomial. Let $\alpha \in \bar{K}_v$ be a root of $f(x)$ and set $L = K_v(\alpha)$. Then the extension L/K_v is unramified and the residue field ℓ of L is given by $\ell = k_v(\bar{\alpha})$.*

Proof. Note that since \bar{f} is separable, f is necessarily separable as well. Let $f(x) = \prod_i f_i(x)$ be the irreducible factorization of f in $K_v[x]$. By Gauss' lemma we know that the $f_i \in \mathcal{O}_v[x]$ and so we can consider their reductions in $k_v[x]$. Without loss of generality we can assume that α is a root of f_1 . We have that \bar{f}_1 is a monic separable polynomial in $k_v[x]$ with root $\bar{\alpha}$. Thus, we can apply Hensel's lemma to conclude that \bar{f}_1 is irreducible and $\alpha \in \mathcal{O}_L$. We have that $\ell \supset k_v(\bar{\alpha})$ and so

$$\begin{aligned} \deg f_1(x) &= \deg(L/K_v) \\ &\geq f(L/K_v) \\ &= \deg(\ell/k_v) \\ &\geq \deg(k_v(\bar{\alpha})/k_v) \\ &= \deg \bar{f}_1 \\ &= \deg f_1. \end{aligned}$$

Thus, we must have $\deg(L/K_v) = f(L/K_v)$ and so the extension is unramified. We also obtain that $\deg(\ell/k_v) = \deg(k_v(\bar{\alpha})/k_v)$ and so $\ell = k_v(\bar{\alpha})$. \square

Let m be a positive integer and let k be the finite field with q elements. There exists a unique extension k_m of k of degree m . The field k_m is the splitting field of the polynomial $f(x) = x^{q^m} - x$. The Galois group $\text{Gal}(k_m/k)$ is cyclic of degree m generated by the Frobenius automorphism $x \mapsto x^q$. Thus, given a positive integer m and a nonarchimedean local field K_v , there is a unique unramified extension K_m of K_v with $\text{Gal}(K_m/K_v) \cong \text{Gal}(k_m/k) \cong \mathbb{Z}/m\mathbb{Z}$. There is a canonical generator Frob_{K_m/K_v} of $\text{Gal}(K_m/K_v)$; namely, the element that

maps to the Frobenius automorphism $x \mapsto x^q$ in $\text{Gal}(k_m/k_v)$. The following corollary is immediate from our discussion and the previous theorem.

Corollary 3.23. *Let K_v be a nonarchimedean local field.*

1. *The compositum of two finite separable unramified extensions is unramified.*
2. *If L/K_v is any separable algebraic extension, possibly of infinite degree, then there exists a unique maximal unramified subextension $K_v \subseteq L_{\text{ur}} \subseteq L$.*
3. *Given any integer m there exists a unique unramified extension K_m of K_v of degree m . Moreover, $\text{Gal}(K_m/K_v) \cong \mathbb{Z}/m\mathbb{Z}$.*

Exercise 3.24. *Show that the compositum of two totally ramified extensions need not be totally ramified.*

Corollary 3.25. *Let n be a positive integer. If K_v is a nonarchimedean local field (of characteristic 0), then there are finitely many extensions of K_v of degree n .*

Proof. Suppose L/K_v is such an extension of degree n . Then by part (2) of Corollary 3.23 we have $K_v \subseteq L_{\text{ur}} \subseteq L$ where L/L_{ur} is totally ramified and L_{ur}/K_v is unramified. The extension L_{ur}/K is uniquely determined by Theorem 3.21. Thus, by Corollary 3.19 there are finitely many possibilities for L/L_{ur} . \square

Example 3.26. Let p be a prime. We consider the quadratic extensions of the field \mathbb{Q}_p .

Let L/\mathbb{Q}_p be a quadratic extension given by $L = \mathbb{Q}_p(\alpha)$ where α is a root of $x^2 - a$ for some $a \in \mathbb{Q}_p^\times$. One can check that $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b})$ if and only if $\frac{a}{b} \in (\mathbb{Q}_p^\times)^2$. Thus, the number of quadratic extensions of \mathbb{Q}_p is equal $\#(\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2) - 1$ as the trivial element does not give a quadratic extension. For $\beta \in \mathbb{Q}_p^\times$ we write $\beta = up^r$ where $r \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. We have an isomorphism

$$\mathbb{Q}_p^\times \xrightarrow{\cong} \mathbb{Z}_p^\times \times \mathbb{Z}$$

given by $\beta \mapsto (u, r)$ and

$$(\mathbb{Q}_p^\times)^2 \xrightarrow{\cong} (\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}$$

given by $\beta^2 \mapsto (u^2, 2r)$. Thus we have

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times \times \mathbb{Z}) / ((\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}) \cong \mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \times \mathbb{Z}/2\mathbb{Z}.$$

In order to classify the quadratic extensions of \mathbb{Q}_p we need to look at $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. We know that $p\mathbb{Z}_p$ is a maximal ideal and so $1 + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$. Note

that for $p \neq 2$ we have $(1 + p\mathbb{Z}_p)^2 = 1 + p\mathbb{Z}_p$. Now $\mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ with $\ker = 1 + p\mathbb{Z}_p$. Thus

$$\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times / ((\mathbb{Z}/p\mathbb{Z})^\times)^2 \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z}$$

and so for $p \neq 2$ we have

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Thus there are 3 distinct quadratic extensions of \mathbb{Q}_p when $p \neq 2$; namely, the unique unramified extension of degree 2 and two totally ramified extensions.

We now deal with the case of $p = 2$. In this case we have $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$ and $(\mathbb{Z}_2^\times)^2 = 1 + 8\mathbb{Z}_2$. Thus,

$$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

since

$$(1 + 2\mathbb{Z}_2) / (1 + 8\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

under the map

$$1 + a_1 2 + a_2 2^2 \mapsto (a_1, a_2).$$

We can now use this isomorphism to determine representatives in \mathbb{Q}_2^\times . Given $(a, b, c) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we see that under the isomorphism this maps to $(1 + a \cdot 2 + b \cdot 2^2)2^c$. Thus, we have that $1, 2, 3, 5, 6, 7, 10, 14 \in \mathbb{Q}_2$ are representatives. Thus there are 7 extensions of \mathbb{Q}_2 given by $\mathbb{Q}_2(\sqrt{a})$ for $a \in \{2, 3, 5, 6, 7, 10, 14\}$. The field $\mathbb{Q}_2(\sqrt{5})$ has discriminant 5, and since $2 \nmid 5$, 2 is unramified in this extension. Thus 5 corresponds to the unique unramified extension.

Exercise 3.27. Give a similar characterization for the quadratic extensions of \mathbb{Q}_5 as was done for \mathbb{Q}_2 .

3.5 Ramification and Galois theory

In this section we give a better description of the totally ramified part of an extension L/K_v ; namely we split the totally ramified part into tame and wild ramification.

Throughout this section we let K_v be a nonarchimedean local field, k_v the residue field, $p = \text{char}(k_v)$, L/K_v a finite and separable extension, and ϖ_v a uniformizer of K_v . We write $e(L/K_v)$ for the ramification index of ϖ_L over ϖ_v .

Definition 3.28. We say L/K_v is *tamely ramified* if $p \nmid e(L/K_v)$ and $e(L/K_v) \neq 1$. We say L/K_v has *wild ramification* if $p \mid e(L/K_v)$.

Lemma 3.29. Let L/K_v be totally ramified. Let $\beta_0 \in L^\times$ so that $|\beta_0|^n = |\varpi_v|$ for some integer n with $p \nmid n$. Then there exists $\beta \in L$ and a uniformizer α of K_v such that $\beta^n = \alpha$.

Proof. Write $\beta_0^n = u\varpi_v$ where $u \in \mathcal{O}_L^\times$. Let $u_0 \in \mathcal{O}_v^\times$ be such that $u_0 \pmod{\mathfrak{m}_v} \equiv u \pmod{\mathfrak{m}_L}$. This is possible since L/K_v is totally ramified so that $\mathcal{O}_v/\mathfrak{m}_v \cong \mathcal{O}_L/\mathfrak{m}_L$. Set $\alpha = u_0\varpi_v$. Then we have

$$|\beta_0^n - \alpha| = |\beta_0^n - u_0\varpi_v| = |\varpi_v(u - u_0)| < |\varpi_v| = |\alpha|$$

where we have used that $|u - u_0| < 1$ since $u - u_0 \in \mathfrak{m}_L$. Let $\beta_1, \dots, \beta_n \in K_v^{\text{sep}}$ be the roots of $f(x) = x^n - \alpha$. Observe that $|\alpha| > |\beta_0^n - \alpha| = \prod |\beta_0 - \beta_i|$ and so $|\beta_0 - \beta_{i_0}| < |\alpha|^{1/n}$ for some i_0 . The fact that $p \nmid n$ (and so $|n| = 1$) implies that

$$|\beta_{i_0}|^{n-1} = |n||\beta_{i_0}|^{n-1} = |f'(\beta_{i_0})| = \prod_{j \neq i_0} |\beta_{i_0} - \beta_j|.$$

Thus, $|\beta_{i_0} - \beta_j| = |\beta_{i_0}|$ for every $j \neq i_0$ since $|\beta_{i_0} - \beta_j| \leq \max\{|\beta_{i_0}|, |\beta_j|\} = |\beta_{i_0}|$ and there are $n - 1$ terms that multiply to give $|\beta_{i_0}|^{n-1}$. Now we can apply Krasner's Lemma to conclude that $K_v(\beta_{i_0}) \subseteq K_v(\beta_0) \subseteq L$. Thus $\beta_{i_0} \in L$ is a root of f and so $\beta_{i_0}^n = \alpha$. \square

Corollary 3.30. *The extension L/K_v is totally tamely ramified if and only if there exists uniformizers ϖ_v and ϖ_L of K_v and L such that $\varpi_L^{\deg(L/K_v)} = \varpi_v$ with $p \nmid \deg(L/K_v)$.*

Proof. Let L/K_v be totally tamely ramified. Lemma 3.29 implies that there exists such uniformizers. On the other hand, if there are such uniformizers our study of Eisenstein extensions shows that L/K_v is totally tamely ramified. \square

Corollary 3.31. *If L_1/K_v and L_2/K_v are tamely ramified, then so is L_1L_2 .*

Proof. We begin by reducing to the case where L_1 and L_2 are totally ramified over K_v . Consider the maximal unramified subextension $(L_1L_2)_{\text{ur}}$ of L_1L_2 . Then we have the following diagram of fields

$$\begin{array}{ccc}
 & L_1L_2 & \\
 & / \quad \backslash & \\
 L_1(L_1L_2)_{\text{ur}} & & L_2(L_1L_2)_{\text{ur}} \\
 & \backslash \quad / & \\
 & (L_1L_2)_{\text{ur}} & \\
 & | & \\
 & K_v &
 \end{array}$$

where $L_1(L_1L_2)_{\text{ur}}/(L_1L_2)_{\text{ur}}$ and $L_2(L_1L_2)_{\text{ur}}/(L_1L_2)_{\text{ur}}$ are totally ramified since they are subextensions of $L_1L_2/(L_1L_2)_{\text{ur}}$ which is totally ramified. Thus by

considering the extensions $L_1(L_1L_2)_{\text{ur}}/(L_1L_2)_{\text{ur}}$ and $L_2(L_1L_2)_{\text{ur}}/(L_1L_2)_{\text{ur}}$ we reduce to the case of considering totally ramified extensions.

The fact that we may assume L_1 and L_2 are totally ramified over K_v gives that there exists uniformizers ϖ_{L_1} and ϖ_{L_2} and ϖ_1 and ϖ_2 such that $\varpi_{L_i}^{\deg(L_i/K_v)} = \varpi_i$. Write $\varpi_2 = u\varpi_1$ for $u \in \mathcal{O}_v^\times$. Lemma 3.17 gives that $L_1 \subseteq K_1 = K_v(\zeta_{e_1}, \varpi_1^{1/e_1})$ and $L_2 \subseteq K_2 = K_v(\zeta_{e_2}, u^{1/e_2}, \varpi_1^{1/e_2})$ where $e_i = \deg(L_i/K_v) = e(L_i/K_v)$ and ζ_{e_i} is a e_i th root of unity. The fact that $p \nmid e_i$ along with Corollaries 3.22 and 3.23 imply that K_1 and K_2 are unramified over K_v . Thus, $K_i(\varpi_1^{1/e_i})/K_i$ is tamely ramified. Set $K_3 = K_1K_2$, which is an unramified extension of K_v . Now $L_1L_2 \subseteq K_4 = K_v(\zeta_{e_1}, \zeta_{e_2}, \varpi_1^{1/e_1}, \varpi_2^{1/e_2})$ and $e(K_4/K_3) \mid e_1e_2$, and so is relatively prime to p . Then since K_3/K_v is unramified, we have the result. \square

Combining what we have done so far we have the following result.

Proposition 3.32. *Let L/K_v be a finite separable extension of nonarchimedean local fields. Then there exists unique subfields $K_v \subseteq L_{\text{ur}} \subseteq L_t \subseteq L$ such that*

1. L_{ur}/K_v is unramified,
2. L_t/L_{ur} is totally tamely ramified,
3. L/L_t is totally wildly ramified.

Proof. The only part that remains to prove is that L/L_t has degree a power of p . Write $\deg(L/L_t) = e'p^r$ for $p \nmid e'$. Let ϖ_L be a uniformizer of L . Then $|\varpi_L^{p^r}|^{e'} = |\varpi_{L_t}|$. Now we apply Lemma 3.29 to get β and ϖ' such that $\beta^{e'} = \varpi'$. The fact that $L_t(\beta)$ is totally ramified implies $e' = 1$. \square

We now turn our attention to the Galois theory of these extensions. The fact that the subfields L_{ur} and L_t are unique implies that if L/K_v is Galois, then so are L_{ur}/K_v and L_t/K_v . From now on we assume that L/K_v is Galois. The group $\text{Gal}(L/L_{\text{ur}})$ is the *inertia group* and is denoted by $I(L/K_v)$, the group $\text{Gal}(L_t/L_{\text{ur}})$ is referred to as the *tame inertia* and denoted $\Gamma^t(L/K_v)$ and the group $\text{Gal}(L/L^t)$ is the wild inertia and is denoted $\Gamma^w(L/K_v)$. One can easily check we have the following exact sequences:

$$0 \longrightarrow I(L/K_v) \longrightarrow \text{Gal}(L/K_v) \longrightarrow \text{Gal}(L_{\text{ur}}/K_v) \longrightarrow 0$$

and

$$0 \longrightarrow \Gamma^w(L/K_v) \longrightarrow I(L/K_v) \longrightarrow \Gamma^t(L/K_v) \longrightarrow 0.$$

Set $K_v^t = \bigcup L_t$ and $K_v^{\text{ur}} = \bigcup L_{\text{ur}}$ where the unions are over all finite separable extensions of K_v . We have $K_v^{\text{ur}} \subseteq K_v^t \subseteq K_v^{\text{sep}}$ where K_v^{ur} is the maximal

unramified subfield of K_v^{sep} and K_v^{t} is the maximal tamely ramified subfield of K_v^{sep} . If $K_v \subseteq L \subseteq K_v^{\text{ur}}$ and L/K_v is finite and separable, then L/K_v is necessarily unramified. If $K_v^{\text{ur}} \subseteq L \subseteq K_v^{\text{t}}$ and L/K_v^{ur} is finite and separable, then L/K_v^{ur} is necessarily totally tamely ramified. Note that K_v^{ur}/K_v and K_v^{t}/K_v are Galois extensions.

Infinite Galois theory enables us to conclude that

$$\text{Gal}(K_v^{\text{ur}}/K_v) \cong \varprojlim_{L/K_v \text{ fin. sep. Galois}} \text{Gal}(L_{\text{ur}}/K_v),$$

$$I(K_v) := \text{Gal}(K_v^{\text{sep}}/K_v^{\text{ur}}) \cong \varprojlim_{L/K \text{ fin. sep. Galois}} \text{Gal}(L/L_{\text{ur}}),$$

and

$$I^{\text{t}}(K_v) := \text{Gal}(K_v^{\text{t}}/K_v^{\text{ur}}) \cong \varprojlim_{L/K \text{ fin. sep. Galois}} \text{Gal}(L_{\text{t}}/L_{\text{ur}}).$$

Thus there is a filtration on $\text{Gal}(K_v^{\text{sep}}/K_v)$ given by

$$0 \longrightarrow I(K_v) \longrightarrow \text{Gal}(K_v^{\text{sep}}/K_v) \longrightarrow \text{Gal}(K_v^{\text{ur}}/K_v) \longrightarrow 0$$

and we have the following exact sequence

$$0 \longrightarrow I^{\text{w}}(K_v) \longrightarrow I(K_v) \longrightarrow I^{\text{t}}(K_v) \longrightarrow 0$$

where

$$I^{\text{w}}(K_v) := \text{Gal}(K_v^{\text{sep}}/K_v^{\text{t}}) \cong \varprojlim_{L/K \text{ fin. sep. Galois}} \text{Gal}(K_v^{\text{sep}}/L_{\text{t}}).$$

The group $I^{\text{w}}(K_v)$ is a pro- p group as the degree of L/L_{t} is a power of p for each L/K_v finite, separable and Galois. The tame inertia groups $I^{\text{t}}(L/K_v)$ must all have order prime to p as $\deg(L_{\text{t}}/L_{\text{ur}})$ is prime to p . Let K_n/K_v be the unique unramified extension of K_v of degree n . We know from our study of unramified extensions that $\text{Gal}(K_n/K_v) \cong \mathbb{Z}/n\mathbb{Z}$. Set $k_n = \mathcal{O}_{K_n}/\mathfrak{m}_{K_n}$. We have that k_n is a finite extension of k_v of degree n and the Galois group $\text{Gal}(k_n/k_v)$ is generated by the map $\sigma_{k_n/k_v} : k_n \rightarrow k_n$ given by $\sigma_{k_n/k_v}(x) = x^p$. The fact that $\text{Gal}(K_n/K_v) \cong \text{Gal}(k_n/k_v)$ gives that there is a unique element $\text{Frob}_{K_n/K_v} \in \text{Gal}(K_n/K_v)$ generating $\text{Gal}(K_n/K_v)$ that maps to σ_{k_n/k_v} . This element Frob_{K_n/K_v} is called the *Frobenius element*.

We have

$$\text{Gal}(K_v^{\text{ur}}/K_v) \cong \varprojlim_n \text{Gal}(K_n/K_v)$$

where the projective limit is given by

$$\text{Gal}(K_n/K_v) \twoheadrightarrow \text{Gal}(K_m/K_v) \quad (m \mid n)$$

by restriction. Thus,

$$\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \cong \varprojlim_n \mathrm{Gal}(K_n/K_v) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Hence $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \cong \hat{\mathbb{Z}}$ by $\mathrm{Frob}_{K_v} \mapsto 1$ where Frob_{K_v} is the element of $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$ that restricts to Frob_{L/K_v} for L/K_v any finite unramified extension of K_v . Using that $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, we have that $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \cong \prod_p \mathbb{Z}_p$.

The importance of the structure of these Galois groups will become apparent as we begin our study of local class field theory. For those interested in further study of nonarchimedean local fields, Serre's book *Local Fields* ([S79]) provides much more information and in much greater generality than has been provided here.

Chapter 4

Group Cohomology

In proving the main theorems of local class field theory, we will make use of the theory of group cohomology. The reader who is familiar with group cohomology is safe to skip this chapter and return to parts of it as needed. There are many excellent sources for this material. We use Milne ([Mi97]) as our source, which follows [CF67] very closely for the material of interest to us. We omit many of the proofs, preferring to let the interested reader look these proofs up on his/her own.

4.1 Definitions

Throughout this section we will let G be a group and M a G -module, i.e., M is an abelian group with a map

$$G \times M \longrightarrow M : (g, m) \mapsto gm$$

satisfying

1. $g(m_1 + m_2) = gm_1 + gm_2$;
2. $(g_1g_2)m = g_1(g_2m)$

for all $g, g_1, g_2 \in G$ and all $m, m_1, m_2 \in M$. Recall that a homomorphism of G -modules M and N is a map $\varphi : M \rightarrow N$ so that

1. φ is a homomorphism of abelian groups;
2. $\varphi(gm) = g\varphi(m)$ for all $g \in G, m \in M$.

We denote the set of all G -module homomorphisms from M to N by $\text{Hom}_G(M, N)$.

In order to define cohomology groups, we need the notion of an injective module and an injective resolution of a module.

Definition 4.1. A G -module I is called an *injective module* if $\text{Hom}_G(\cdot, I)$ is an exact functor.

Recall that this means given an exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

one has that the sequence

$$0 \longrightarrow \text{Hom}_G(M_3, I) \longrightarrow \text{Hom}_G(M_2, I) \longrightarrow \text{Hom}_G(M_1, I) \longrightarrow 0$$

is exact. Note that the sequence

$$0 \longrightarrow \text{Hom}_G(M_3, I) \longrightarrow \text{Hom}_G(M_2, I) \longrightarrow \text{Hom}_G(M_1, I)$$

is always exact, so being an injective module is equivalent to saying given an injection $M_1 \rightarrow M_2$, any homomorphism $M_1 \rightarrow I$ lifts to a homomorphism $M_2 \rightarrow I$.

Theorem 4.2. *Given a G -module M , there exists an injective module I so that $M \hookrightarrow I$.*

An *injective resolution* of a G -module M is an exact sequence

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \dots$$

where I^j are injective modules. It is customary to write this exact sequence as $M \rightarrow I$.

Corollary 4.3. *Given a G -module M there exists an injective resolution of M .*

We can define a left-exact functor from the category of G -modules to the category of abelian groups by sending M to M^G where we define

$$M^G = \{m \in M : gm = m \text{ for all } g \in G\}.$$

Given an injective resolution $M \rightarrow I$ of M , we can apply this functor to the exact sequence to obtain a sequence

$$0 \longrightarrow (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} \dots$$

which is no longer necessarily an exact sequence. We define the r th cohomology group of G with coefficients in M to be

$$H^r(G, M) = \frac{\ker(d^r)}{\text{Im}(d^{r-1})}.$$

Proposition 4.4. *Let M and N be G -modules. Then we have*

1. $H^0(G, M) = M^G$;
2. For an injective G -module I , one has $H^r(G, I) = 0$ for all $r > 0$;
3. Let $M \rightarrow I$ and $N \rightarrow J$ be injective resolutions. Then any homomorphism $\varphi : M \rightarrow N$ extends to a map of complexes $\tilde{\varphi} : I \rightarrow J$ and the maps $H^r(\tilde{\varphi}) : H^r(G, M) \rightarrow H^r(G, N)$ are independent of the choice of $\tilde{\varphi}$. In particular, applying this to the identity map $M \rightarrow M$ shows that the cohomology groups are well-defined;
4. A short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

gives rise to a long exact sequence of cohomology

$$0 \longrightarrow M_1^G \longrightarrow M_2^G \longrightarrow M_3^G \xrightarrow{\delta^0} H^1(G, M_1) \longrightarrow H^1(G, M_2) \longrightarrow \cdots$$

The proof of this proposition is not difficult, and in any case can be found in any standard source.

Exercise 4.5. *Let M_i be a finite collection of G -modules. Show that $\prod M_i$ is a G -module and that $H^r(G, \prod M_i) \cong \prod H^r(G, M_i)$ for all $r \geq 0$.*

This formulation of the cohomology groups is useful for proving general results, but is not easy to calculate with and so is not useful in many instances. One can remedy this problem by instead considering a projective resolution of the module M . For an appropriate projective resolution this leads to the description of the cohomology groups in terms of cochains, which are more useful for calculations.

For $r \geq 0$, let P_r be the free \mathbb{Z} -module with basis consisting of $r + 1$ -tuples (g_0, g_1, \dots, g_r) with $g_i \in G$. The module P_r has a natural G -action given by $g \cdot (g_0, g_1, \dots, g_r) = (gg_0, gg_1, \dots, gg_r)$. Define a homomorphism $d_r : P_r \rightarrow P_{r-1}$ by

$$d_r(g_0, \dots, g_r) = \sum_{i=0}^r (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_r)$$

where the $\hat{}$ indicates that entry is omitted. These maps are referred to as the *boundary maps*. Let P be the sequence

$$\cdots \longrightarrow P_r \xrightarrow{d_r} P_{r-1} \xrightarrow{d_{r-1}} \cdots \xrightarrow{d_1} P_0.$$

Viewing \mathbb{Z} as a G -module with trivial G -action we can define a map $\varepsilon : P_0 \rightarrow \mathbb{Z}$ given by sending generators to 1, and so we have the sequence

$$\cdots \longrightarrow P_r \xrightarrow{d_r} P_{r-1} \xrightarrow{d_{r-1}} \cdots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Exercise 4.6. Check that $d_{r-1} \circ d_r = 0$ and so this defines a complex. In fact, show that the sequence is an exact sequence.

The following theorem follows immediately from the fact that P is a projective resolution of M . One can see ([Mi97], Appendix to Chapter 4) for a proof of this fact.

Theorem 4.7. For any G -module M one has

$$H^r(G, M) \cong H^r(\text{Hom}_G(P, M))$$

where $H^r(\text{Hom}_G(P, M))$ indicates the cohomology groups arising from the complex

$$0 \longrightarrow \text{Hom}_G(P_0, M) \longrightarrow \text{Hom}_G(P_1, M) \longrightarrow \cdots.$$

This theorem shows that we can compute the cohomology groups by working with this projective resolution rather than the injective resolution. We will now see how this is advantageous.

An element $f \in \text{Hom}_G(P_r, M)$ can be identified with a function $f : G^{r+1} \rightarrow M$ so that $f(gg_0, \dots, gg_r) = gf(g_0, \dots, g_r)$ for all $g, g_0, \dots, g_r \in G$. Such a function is determined by its values on elements of the form $(1, g_1, g_1g_2, \dots, g_1 \cdots g_r)$ in G^{r+1} . (Looking at our functions on such elements will make things work out nicer.) Set

$$\phi(g_1, \dots, g_r) = f(1, g_1, g_1g_2, \dots, g_1 \cdots g_r).$$

The boundary maps are then given by

$$\begin{aligned} d^r \phi(g_1, \dots, g_{r+1}) &= g_1 \phi(g_2, \dots, g_{r+1}) + \sum_{j=1}^r (-1)^j \phi(g_1, \dots, g_j g_{j+1}, \dots, g_{r+1}) \\ &\quad + (-1)^{r+1} \phi(g_1, \dots, g_r). \end{aligned}$$

Exercise 4.8. We say a homomorphism $\phi : G \rightarrow M$ is a crossed homomorphism if $\phi(g_1g_2) = g_1\phi(g_2) + \phi(g_1)$ for all $g_1, g_2 \in G$.

1. Let $m \in M$. Show that the map $g \mapsto gm - m$ is a crossed homomorphism. These are called the principle crossed homomorphisms.

2. Show that

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms } G \rightarrow M\}}{\{\text{principle crossed homomorphisms } G \rightarrow M\}}.$$

3. Let G act on M trivially. Prove that $H^1(G, M) = \text{Hom}_G(G, M)$.

4.2 Hilbert's Theorem 90

In this section we will prove one of the most useful results about group cohomology, Hilbert's Theorem 90. Let L/K be a finite Galois extension of fields and let $G = \text{Gal}(L/K)$. We can view L^\times as a G -module. When viewed as an additive group, L is also a G -module. We will calculate the first cohomology groups of L and L^\times in this section. First, we begin with some more preliminaries.

Let G be a group and H a subgroup of G . Let M be a H -module. We now describe how to associate a G -module to M . Let $\text{Ind}_H^G(M)$ be the set of maps $\psi : G \rightarrow M$ so that $\psi(hg) = h\psi(g)$ for all $h \in H, g \in G$. Note that these maps are not required to be homomorphisms. The set $\text{Ind}_H^G(M)$ is a G -module with operations $(\psi_1 + \psi_2)(g) = \psi_1(g) + \psi_2(g)$ and $g_1\psi(g_2) = \psi(g_2g_1)$ for all $g, g_1, g_2 \in G, \psi, \psi_1, \psi_2 \in \text{Ind}_H^G(M)$. We call $\text{Ind}_H^G(M)$ the module induced from H . The following exercise is an important result and should be worked out in detail.

Exercise 4.9. Let H be a subgroup of G , M a G -module, and N a H -module. Prove that

$$\text{Hom}_G(M, \text{Ind}_H^G(N)) \cong \text{Hom}_H(M, N).$$

Let M be a G -module and consider \mathbb{Z} as a G -module with trivial action. Observe that

$$(4.1) \quad \text{Hom}_G(\mathbb{Z}, M) \cong M^G$$

as any homomorphism from \mathbb{Z} into M is determined by the image of 1 and conversely, something is the image of 1 if and only if it is fixed by G .

Proposition 4.10. (*Shapiro's Lemma*) Let G be a group and H a subgroup. For any H -module N , there is a canonical isomorphism

$$H^r(G, \text{Ind}_H^G(N)) \xrightarrow{\cong} H^r(H, N)$$

for all $r \geq 0$.

Proof. The case of $r = 0$ follows from equation (4.1) along with the previous exercise. For $r > 0$, the result follows from the fact that Ind_H^G is an exact functor and preserves injectives. \square

Corollary 4.11. Let M be an induced G -module, i.e., $M = \text{Ind}_1^G(M_0)$ for some abelian group M_0 . Then $H^r(G, M) = 0$ for all $r > 0$.

Proof. We have

$$H^r(G, M) = H^r(\{1\}, M_0) = 0$$

for all $r > 0$. □

We will also need the Normal Basis Theorem. For a proof of this theorem, see ([Mi97], pages 50-51.)

Theorem 4.12. (*Normal Basis Theorem*) *Let L/K be a finite Galois extension with Galois group G . There exists $\alpha \in L$ so that $\{\sigma\alpha : \sigma \in G\}$ is a basis for L as a K -vector space.*

Proposition 4.13. *Let L/K be a finite Galois extension with Galois group G . Then $H^r(G, L) = 0$ for all $r > 0$.*

Proof. As a G -module, we have that $L \cong K[G]$ by the Normal Basis Theorem where $K[G]$ is the group algebra. However, we have that $\text{Ind}_1^G(K) \cong K[G]$ under the map $\varphi \mapsto \sum_{g \in G} \varphi(g^{-1})g$ and so $H^r(G, L) = H^r(\{1\}, K) = 0$ for all $r > 0$. □

We will also need Dedekind's theorem on the independence of characters.

Theorem 4.14. *Let L be a field and H a group. Then any finite set $\{\chi_i\}$ of distinct homomorphisms $H \rightarrow L^\times$ is linearly independent over L .*

The next theorem and its corollary are both often referred to as Hilbert's Theorem 90.

Theorem 4.15. (*Hilbert's Theorem 90*) *Let L/K be a finite Galois extension with Galois group G . Then $H^1(G, L^\times) = 0$.*

Proof. First, note that since L^\times is a group under multiplication, our notation here will reflect this fact. Let $\phi \in H^1(G, L^\times)$, i.e., $\phi(g_1g_2) = g_2\phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. For any $x \in L^\times$, set

$$y = \sum_{g \in G} \phi(g)g(x).$$

Observe that we can apply Theorem 4.14 to this situation with $H = L^\times$ and the g 's as our χ_i 's to obtain that there exists $x \in L^\times$ so that $y \neq 0$.

Let $g_1 \in G$. Then we have

$$\begin{aligned} g_1y &= \sum_{g \in G} g_1\phi(g)g_1g(x) \\ &= \sum_{g \in G} \phi(g_1)^{-1}\phi(g_1g)g_1g(x) \\ &= \phi(g_1)^{-1}y. \end{aligned}$$

Now we use that $y \neq 0$ to conclude that

$$\phi(g_1) = y/g_1(y) = g_1(y^{-1})/y^{-1}.$$

Thus we have that ϕ is trivial in $H^1(G, L^\times)$, completing the proof. □

Corollary 4.16. *Let L/K be a finite cyclic Galois extension, i.e., L/K is a Galois extension with a finite cyclic Galois group G . Let g generate G . If $\text{Nm}_{L/K} x = 1$, then x is of the form gy/y .*

Proof. This follows immediately from the fact that $H^1(G, L^\times) \cong \text{Ker}(\text{Nm}_{L/K})/(g-1)L^\times$ in this case, which we now prove.

Consider the map $\Phi : H^1(G, L^\times) \rightarrow \text{Ker}(\text{Nm}_{L/K})/(gL^\times/L^\times)$ given by $\phi \mapsto \phi(g)$. (One should note that often this is written as $\text{Ker}(\text{Nm}_{L/K})/(g-1)L^\times$, mixing the multiplicative and additive notation in one equation!) Let $\phi \in H^1(G, L^\times)$. Note that $\phi(1) = \phi(1 \cdot 1) = 1\phi(1)\phi(1)$ and so $\phi(1) = 1$. Thus, we have

$$\begin{aligned} 1 &= \phi(g^m) \\ &= \phi(g^{m-1}g) \\ &= g\phi(g^{m-1})\phi(g) \\ &= g^2\phi(g^{m-2})\phi(g)^2 \\ &= \dots \\ &= \text{Nm}_{L/K}(\phi(g)). \end{aligned}$$

Thus, $\phi(g) \in \text{Ker}(\text{Nm}_{L/K})$. Finally, we note that ϕ is trivial in $H^1(G, L^\times)$ if and only if $\phi(g) = g(x)/x$ for some $x \in L^\times$, i.e., if and only if $\phi(g) \in (gL^\times/L^\times)$. \square

Before returning to more general results, we give an application of Hilbert's Theorem 90 to Kummer Theory, i.e., classifying the finite abelian extensions of a field K of degree dividing n when $\mu_n \subset K^\times$. First we need the following result.

Exercise 4.17. *Show that given an exact sequence of G -modules*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

one has that the connecting homomorphism $\delta_0 : M_3^G \rightarrow H^1(G, M_1)$ given in the long exact sequence of cohomology is given as follows: for $m_3 \in M_3^G$, let $m_2 \in M_2$ be an element mapping to m_3 and define $\delta_0(m_3)$ to be the class in $H^1(G, M_1)$ defined by sending $g \mapsto gm_2 - m_2$.

Let n be a positive integer and let K be a field containing μ_n , the n th roots of unity. Let $G = \text{Gal}(\overline{K}/K)$. One has that the following sequence is exact:

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{n} \overline{K}^\times \longrightarrow 1$$

where the n denotes the n th power map. The long exact sequence of cohomology gives

$$1 \longrightarrow \mu_n^G \longrightarrow (\overline{K}^\times)^G \xrightarrow{n} (\overline{K}^\times)^G \longrightarrow H^1(G, \mu_n) \longrightarrow H^1(G, \overline{K}^\times) \longrightarrow \cdots$$

The fact that $\mu_n \subset K$ gives that $\mu_n^G = \mu_n$ and $(\overline{K}^\times)^G = K^\times$ by Galois theory. We have that $H^1(G, \overline{K}^\times) = 0$ by using Hilbert's Theorem 90 to get the result for all finite extensions of K and then using that $H^1(G, \overline{K}^\times)$ is the inverse limit of trivial groups. Thus, the sequence becomes

$$1 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{n} K^\times \longrightarrow H^1(G, \mu_n) \longrightarrow 0,$$

i.e., we have an isomorphism

$$H^1(G, \mu_n) \cong K^\times / (K^\times)^n.$$

The previous exercise (keeping in mind we are using multiplicative notation here!) gives that for every $x \in K^\times$ and $g \in G$, the element $\sqrt[n]{x}$ in \overline{K}^\times maps to x in the long exact sequence and

$$\phi(g) = g(\sqrt[n]{x}) / \sqrt[n]{x}$$

defines an element in $H^1(G, \mu_n)$. The kernel of this homomorphism is $K(\sqrt[n]{x})$.

Observe that since $\mu_n \subset K$ we have that G acts trivially on μ_n and so $H^1(G, \mu_n) = \text{Hom}_G(G, \mu_n)$. Since the action is trivial, as a G -module $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ and so $H^1(G, \mu_n) \cong \text{Hom}_G(G, \mathbb{Z}/n\mathbb{Z})$. Given a G -module homomorphism $\phi \in \text{Hom}_G(G, \mathbb{Z}/n\mathbb{Z})$, we have that $\ker \phi \subset G$ is a closed normal subgroup and so corresponds via Galois theory to a finite extension L_ϕ of K . Moreover, $\text{Gal}(L_\phi/K) \cong \text{Im}(\phi) \subset \mathbb{Z}/n\mathbb{Z}$ and so is necessarily a cyclic group of order dividing n . Conversely, every such cyclic extension of K of order dividing n gives a G -module homomorphism in $\text{Hom}_G(G, \mathbb{Z}/n\mathbb{Z})$. Thus, we have a bijection between $H^1(G, \mu_n)$ and cyclic extensions of K of degree dividing n . Combining with what we showed above gives that the Kummer extensions (finite cyclic of order dividing n) are given by $L = K(\sqrt[n]{x})$ for some $x \in K^\times$. Moreover, the class of $x \in K^\times / (K^\times)^n$ is unique.

4.3 Changing the group

It is often valuable to have a way to compare the cohomology of different groups as it may be easier to calculate for one of the groups. We have already seen this applied several times in the context of Exercise 4.9. We will describe three more comparison maps in this section: the restriction, corestriction, and inflation maps.

Let G and H be a groups and let M be a G -module. Let $f : H \rightarrow G$ be a homomorphism of groups. We can view M as a H -module via the map f . Let P_G and P_H be the standard projective resolutions we used above to define the

cohomology groups in terms of cocycles. The map f induces a homomorphism of complexes $P_H \rightarrow P_G$, which in turn gives a homomorphism $H^r(G, M) \rightarrow H^r(H, M)$. (Note that the order of G and H is reversed here, be sure you understand why!)

If we set H to be a subgroup of G and f to be the inclusion map, then the induced map on cohomology is known as the restriction map:

$$\text{Res} : H^r(G, M) \rightarrow H^r(H, M).$$

Another natural map to consider is the projection map $G \rightarrow G/H$. In this case, given a G -module M , we have that M^H is a G/H -module. Thus, we have a map on cohomology $H^r(G/H, M^H) \rightarrow H^r(G, M^H)$. We obtain the inflation map by composing this map with the one induced by the natural map $M^H \rightarrow M$:

$$\text{Inf} : H^r(G/H, M^H) \rightarrow H^r(G, M).$$

The importance of these two maps follows from the following important theorem.

Theorem 4.18. (*Inflation-Restriction Sequence*) *Let H be a normal subgroup of G and let M be a G -module. The sequence*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)$$

is exact.

Proof. Our first step is to show that the inflation map is an injection. Let $\phi \in H^1(G/H, M^H)$ so that $\text{Inf}(\phi) = 0$ in $H^1(G, M)$, i.e., there exists $m \in M$ so that $\text{Inf}(\phi)(g) = gm - m$ for all $g \in G$. Recall that $\text{Inf}(\phi)$ is in the map induced from $\phi : G/H \rightarrow M^H$ via $G \rightarrow G/H \rightarrow M^H \rightarrow M$. Thus, we have that $\text{Inf}(\phi)$ is constant on the cosets of H in G and so $ghm - m = gm - m$ for all $g \in G, h \in H$. Taking g to be the identity we see that $hm = m$ for all $h \in H$. Thus, $m \in M^H$ and so ϕ must be trivial in $H^1(G/H, M^H)$ as claimed.

The next step is to show that $\text{Res} \circ \text{Inf} = 0$. Let $\phi \in H^1(G/H, M^H)$. This is clear. If $\psi \in H^1(G, M)$, then $\text{Res}(\psi) = \psi|_H$. If $\phi \in H^1(G/H, M^H)$, then $\text{Inf}(\phi)$ is trivial on H and so $\text{Res}(\text{Inf}(\phi)) = 0$.

Finally, we need to show that the image of Inf is the kernel of Res . We have just seen that the image is contained in the kernel, so it remains to show that in fact that kernel is contained in the image. Let $\psi \in H^1(G, M)$ be such that $\text{Res}(\psi) = 0$, i.e., there exists $m \in M$ so that $\text{Res}(\psi)(h) = hm - m$ for all $h \in H$. Our goal is to show that there exists $\phi \in H^1(G/H, M^H)$ so that $\text{Inf}(\phi) = \psi$. Recall that the map $\delta \in H^1(G, M)$ given by $\delta(g) = gm - m$ for all $g \in G$ is trivial in $H^1(G, M)$. Thus, by looking at $\psi - \delta$, we can assume that $\psi|_H = 0$. We know that for all $g_1, g_2 \in G$ we have

$$\psi(g_1g_2) = \psi(g_1) + g_1\psi(g_2).$$

If we take $g \in G$ and $h \in H$, then we have

$$\psi(gh) = \psi(g) + g\psi(h) = \psi(g).$$

Thus, we have that ψ gives a map $G/H \rightarrow M$. On the other hand, we also have

$$\psi(hg) = \psi(h) + h\psi(g) = h\psi(g).$$

We have that H is a normal subgroup of G , so for any $g \in G, h \in H$ there exists an $h_g \in H$ so that $g^{-1}hg = h_g$. Using this we have

$$\begin{aligned} h\psi(g) &= \psi(hg) \\ &= \psi(gh_g) \\ &= \psi(g). \end{aligned}$$

Thus, we have that $\psi : G/H \rightarrow M^H$ and so ψ is in the image of the inflation map, as desired. \square

One should note that even though we have only shown the result for $r = 1$, the sequence is also exact for the r th cohomology groups if one adds the assumption that $H_T^i(H, M) = 0$ for all $1 \leq i \leq r - 1$. We will use the more general result later. The general case follows from the case $r = 1$ by induction.

The last functorial map of cohomology groups we will need is the corestriction map. Let H be a finite index subgroup of G and let $\{g_1, \dots, g_n\}$ be a set of left coset representatives. Let M be a G -module and for any $m \in M^H$ define the norm from G to H of m by

$$\text{Nm}_{G/H} m = \sum_{i=1}^n g_i m.$$

This is independent of the coset representatives chosen and is easily seen to be fixed by G . Thus, the map $\text{Nm}_{G/H}$ is a homomorphism $M^H \rightarrow M^G$. We now see how this map can be extended to a map $H^r(H, M) \rightarrow H^r(G, M)$ for all r .

Exercise 4.19. Show that the map $\psi \mapsto \sum_{i=1}^n g_i \psi(g_i^{-1})$ is a homomorphism from $\text{Ind}_H^G(M)$ to M .

Using this homomorphism, we have an induced map on the cohomology

$$H^r(G, \text{Ind}_H^G(M)) \longrightarrow H^r(G, M).$$

Combining this map with the isomorphism $H^r(H, M) \cong H^r(G, \text{Ind}_H^G(M))$ given by Shapiro's lemma gives the corestriction map

$$\text{Cor} : H^r(H, M) \longrightarrow H^r(G, M).$$

Proposition 4.20. Let H be a subgroup of G of finite index with coset representatives $\{g_1, \dots, g_n\}$. The composite map $\text{Cor} \circ \text{Res}$ is multiplication by $[G : H]$.

Proof. There is a natural map $m \mapsto \psi_m$ from M to $\text{Ind}_H^G(M)$ where $\psi_m(g) = gm$. The map $\text{Cor} \circ \text{Res}$ is the map induced from the maps $M \rightarrow \text{Ind}_H^G(M) \rightarrow M$ given by

$$m \mapsto \psi_m \mapsto \sum_{i=1}^n g_i \psi_m(g_i^{-1}).$$

It is easy to see that

$$\begin{aligned} \sum_{i=1}^n g_i \psi_m(g_i^{-1}) &= \sum_{i=1}^n m \\ &= [G : H]m. \end{aligned}$$

□

Exercise 4.21. If $\#G = n$, then $nH^r(G, M) = 0$ for $r > 0$.

Corollary 4.22. If G is a finite group and M is finitely generated as an abelian group, then $H^r(G, M)$ is finite.

Proof. From the definition of $H^r(G, M)$ it is clear that it is finitely generated. We now use the fact that it is killed by the order of G to conclude that it must be finite. □

For any abelian group G , the p -primary component of G is the set of elements of G killed by some power of p . This group is denoted by $G[p^\infty]$.

Corollary 4.23. Let G be a finite group and let G_p be the p -Sylow subgroup of G . For any G -module M , the restriction map

$$\text{Res} : H^r(G, M) \longrightarrow H^r(G_p, M)$$

is injective on $H^r(G, M)[p^\infty]$.

Proof. By definition we have that $[G : G_p]$ is relatively prime to p . Since the composite

$$\text{Cor} \circ \text{Res} : H^r(G, M) \longrightarrow H^r(G_p, M) \longrightarrow H^r(G, M)$$

is multiplication by $[G : G_p]$, it is necessarily injective on $H^r(G, M)[p^\infty]$ by definition of the p -primary component. Thus, Res must also be injective on $H^r(G, M)[p^\infty]$ as well. □

4.4 Cup Products

Let M and N be G -modules. We write $M \otimes N$ for $M \otimes_{\mathbb{Z}} N$ considered as a G -module with action given by $g(m \otimes n) = gm \otimes gn$ for $g \in G$, $m \in M$ and $n \in N$.

Theorem 4.24. *There exists a unique family of bi-additive pairings*

$$(\phi, \psi) \mapsto \phi \cup \psi : H^r(G, M) \times H^s(G, N) \longrightarrow H^{r+s}(G, M \otimes N)$$

defined for all G -modules M and N and all integers $r, s \geq 0$ satisfying the following conditions:

1. these maps become morphisms of functors when the two sides are regarded as covariant bifunctors on (M, N) ;
2. for $r = s = 0$, the pairing is

$$(m, n) \mapsto m \otimes n : M^G \otimes N^G \longrightarrow (M \otimes N)^G;$$

3. if

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is an exact sequence of G -modules so that

$$0 \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is exact, then

$$(\delta\phi_3) \cup \psi = \delta(\phi_3 \cup \psi)$$

for $\phi_3 \in H^r(G, M_3)$ and $\psi \in H^s(G, N)$ where δ denotes the appropriate connecting homomorphism;

4. if

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

is an exact sequence of G -modules so that

$$0 \longrightarrow M \otimes N_1 \longrightarrow M \otimes N_2 \longrightarrow M \otimes N_3 \longrightarrow 0$$

is exact, then

$$\phi \cup \delta\psi_3 = (-1)^r \delta(\phi \cup \psi_3)$$

for $\phi \in H^r(G, M)$ and $\psi_3 \in H^s(G, N_3)$ where δ denotes the appropriate connecting homomorphism.

Proof. See Theorem 4 in the Cohomology of Groups section of [CF67]. \square

Proposition 4.25. *We have the following formulas:*

1. $(\phi \cup \psi) \cup \chi = \phi \cup (\psi \cup \chi)$;
2. $\phi \cup \psi = (-1)^{rs} \psi \cup \phi$;
3. $\text{Res}(\phi \cup \psi) = \text{Res}(\phi) \cup \text{Res}(\psi)$;
4. $\text{Cor}(\phi \cup \text{Res}(\psi)) = \text{Cor}(\phi) \cup \psi$.

Proof. Again, one can see [CF67] for a complete proof. \square

4.5 Profinite Groups

Let G be a profinite group, i.e., G is a compact topological group for which the open normal subgroups form a fundamental system of open neighborhoods of 1. For example, let L/K be a Galois extension of fields (not necessarily finite), then $G = \text{Gal}(L/K)$ is a profinite group. In this case the open subgroups are precisely those that fix a finite extension of K sitting in L . A finite group given the discrete topology is also a profinite group. In this section we give a brief account of how our notions of cohomology can be adapted to handle profinite groups as well. This will be important so that we can extend the results we obtain about finite Galois groups to those of infinite Galois groups.

When given a profinite group, we consider only the G -modules for which the action of G on M is a continuous map when M is given the discrete topology. Such a G -module is referred to as a discrete module. The category of discrete modules is an abelian category with enough injectives, so we can define cohomology groups just as before, writing $H_{\text{cts}}^r(G, M)$. Note that if G is finite the continuous cohomology groups coincide with the cohomology groups we have been using up to this point. The continuous cohomology groups behave much the same as the cohomology groups we have been dealing with. For example, one still has the Res, Cor, and Inf maps. The following propositions will be particularly important for us.

Proposition 4.26. *The maps*

$$\text{Inf} : H^r(G/H, M^H) \longrightarrow H_{\text{cts}}^r(G, M)$$

realize the continuous cohomology group as the direct limit of the groups $H^r(G/H, M^H)$ where the H run over the open normal subgroups of G , i.e., we have

$$\varinjlim H^r(G/H, M^H) = H_{\text{cts}}^r(G, M).$$

Proposition 4.27. *Let G be a profinite group and M a discrete G -module. If $M = \varinjlim M_i$ where $M_i \subset M$, then*

$$H^r(G, M) = \varinjlim H^r(G, M_i).$$

We omit the proofs of these facts, but they follow readily from the fact that direct limits commute with the formation of cohomology groups. From now on we deal strictly with continuous cohomology. As such, we drop the cts from the notation. As there is no difference for finite groups, the fact that we are using continuous cohomology will not become important until the next chapter.

4.6 Homology Groups

Though cohomology is our main tool for proving the results of local class field theory, it will be necessary to use homology groups to define the “Tate Groups”, which will be very important in our proofs. The notion of homology groups is dual to that of cohomology groups, and since we studied those in some detail the study of homology will very cursory at best.

Let G be a group and M a G -module. Let $I_G = \{g - 1 : g \in G\}$, i.e., I_G fits into the exact sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

where the map $\mathbb{Z}[G] \rightarrow \mathbb{Z}$ is given by $\sum n_g g \mapsto \sum n_g$, and consider the submodule $M_G = M/I_G M$ of M . This is the largest quotient of M on which G acts trivially, the dual notion to that of M^G . The functor sending M to M_G is a right exact functor. To define the homology groups, we take a projective resolution

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow M \longrightarrow 0$$

of M . The complex

$$\cdots \longrightarrow (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \longrightarrow M_G \longrightarrow 0$$

is no longer exact, and so we define the homology groups as

$$H_r(G, M) = \text{Ker}(d_r) / \text{Im}(d_{r+1}).$$

These groups have the same properties as the cohomology groups, just dualized. For example, given a short exact sequence of G -modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

one obtains a long exact sequence of homology groups

$$\cdots \longrightarrow H_r(G, M_2) \longrightarrow H_r(G, M_3) \xrightarrow{\delta_r} H_{r-1}(G, M_1) \longrightarrow \cdots \longrightarrow H_0(G, M_3) \longrightarrow 0.$$

In some instances it may be easiest to use the resolution P we used to give the description of the cohomology groups in terms of cocycles to define the homology as well. This can be done as follows. Recall that P was the exact sequence

$$\cdots \longrightarrow P_r \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

defined as in section 4.1. We can tensor this sequence with M and it remains exact giving

$$\cdots \longrightarrow P_r \otimes M \longrightarrow \cdots \longrightarrow P_1 \otimes M \longrightarrow P_0 \otimes M \longrightarrow M \longrightarrow 0.$$

Now we can apply the above construction to this resolution of M to define the homology groups.

As in the case of cohomology groups, one can show that $H^r(G, M) = 0$ for $r > 0$ if M is an induced module. This shows that $H^r(G, \mathbb{Z}[G]) = 0$ for $r > 0$ with \mathbb{Z} having a trivial G -action since we saw before that $\mathbb{Z}[G] = \text{Ind}_1^G \mathbb{Z}$. Using the long exact sequence defining I_G , we have the following long exact sequence of homology

$$0 \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow I_G/I_G^2 \longrightarrow \mathbb{Z}[G]/I_G\mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The map $I_G/I_G^2 \rightarrow \mathbb{Z}[G]/I_G\mathbb{Z}[G]$ is induced from the inclusion map $I_G \rightarrow \mathbb{Z}[G]$, and so has image 0. Thus, we obtain that $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$ and $\mathbb{Z}[G]/I_G\mathbb{Z}[G] \cong \mathbb{Z}$.

Exercise 4.28. Let G^{ab} be the largest abelian quotient of G , i.e., it is $G/[G, G]$. Show that the map $g \mapsto (g-1) + I_G^2$ induces an isomorphism

$$G^{\text{ab}} \xrightarrow{\cong} I_G/I_G^2.$$

Corollary 4.29. There is a canonical isomorphism

$$H_1(G, \mathbb{Z}) \xrightarrow{\cong} G^{\text{ab}}.$$

4.7 The Tate Groups

Throughout this section we let G be a finite group. Recall that for any G -module M , we defined the norm map $\text{Nm}_G : M \rightarrow M$ by

$$m \mapsto \sum_{g \in G} gm.$$

Given $g_1 \in G$, it is clear that as G runs through all elements of G , so does g_1g . Thus, we have

$$\mathrm{Nm}_G(gm) = \mathrm{Nm}_G(m) = g(\mathrm{Nm}_G(m)).$$

In particular, this shows that $\mathrm{Im}(\mathrm{Nm}_G) \subset M^G$. We also see that $(g-1)\mathrm{Nm}_G = 0$ and so $I_G M \subset \mathrm{Ker}(\mathrm{Nm}_G)$. Combining these two facts shows that the norm map defines a homomorphism

$$\mathrm{Nm}_G : H_0(G, M) \longrightarrow H^1(G, M).$$

Let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of G -modules. We then obtain a diagram

$$\begin{array}{ccccccccc} H_1(G, M_3) & \longrightarrow & H_0(G, M_1) & \longrightarrow & H_0(G, M_2) & \longrightarrow & H_0(G, M_3) & \longrightarrow & 0 \\ & & \downarrow \mathrm{Nm}_G & & \downarrow \mathrm{Nm}_G & & \downarrow \mathrm{Nm}_G & & \\ 0 & \longrightarrow & H^0(G, M_1) & \longrightarrow & H^0(G, M_2) & \longrightarrow & H^0(G, M_3) & \longrightarrow & H^1(G, M_1) \longrightarrow \cdots \end{array}$$

Applying the Snake lemma to the middle of this diagram gives the long exact sequence of Tate cohomology groups

$$\cdots \longrightarrow H_T^r(G, M_1) \longrightarrow H_T^r(G, M_2) \longrightarrow H_T^r(G, M_3) \xrightarrow{\delta_r} H_T^{r+1}(G, M_1) \longrightarrow \cdots$$

for all $-\infty < r < \infty$ where the Tate cohomology groups are defined by

$$H_T^r(G, M) := \begin{cases} H^r(G, M) & r > 0 \\ M^G / \mathrm{Nm}_G(M) & r = 0 \\ \mathrm{Ker}(\mathrm{Nm}_G) / I_G M & r = -1 \\ H_{-r-1}(G, M) & r < -1. \end{cases}$$

It turns out that most of the results we have talked about for the groups $H^r(G, M)$ apply to $H_T^r(G, M)$ as well. (Of course, all of them for $r > 0$ apply!) For instance, we still have restriction, corestriction, and inflation maps and $\mathrm{Cor} \circ \mathrm{Res}$ is still multiplication by $[G : H]$. Cup products also extend in a natural way to the Tate cohomology groups, see [CF67] for example.

We now consider \mathbb{Z} , \mathbb{Q} , and \mathbb{Q}/\mathbb{Z} as G -modules with a trivial G -action and compute the relevant Tate groups that we will need for the proofs of the local class field theory results in Chapter 5.

Lemma 4.30. *Let G be a finite group.*

1. $H_T^r(G, \mathbb{Q}) = 0$ for all r ;
2. $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/[G : 1]\mathbb{Z}$ and $H_T^1(G, \mathbb{Z}) = 0$;
3. there is a canonical isomorphism

$$\mathrm{Hom}_G(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow H_T^2(G, \mathbb{Z}).$$

Proof. Note that for any positive integer m the multiplication by m map $m : \mathbb{Q} \rightarrow \mathbb{Q}$ is an isomorphism. Thus, for any integer r we have that $H^r(m) : H_T^r(G, \mathbb{Q}) \rightarrow H_T^r(G, \mathbb{Q})$ is also an isomorphism (it is also just multiplication by m .) Since G is assumed to be finite, we can set $m = \#G$. However, this gives that multiplication by m is an isomorphism and also the zero map. This implies that we must have $H_T^r(G, \mathbb{Q}) = 0$.

We now consider the case of $M = \mathbb{Z}$. Observe that since $\mathbb{Z}^G = \mathbb{Z}$, the norm map on \mathbb{Z} is just multiplication by $m = \#G$. Thus, $H_T^0(G, \mathbb{Z}) = \mathbb{Z}^G / \mathrm{Nm}_G(\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$, as claimed. We have seen before that $H^1(G, \mathbb{Z}) = \mathrm{Hom}_G(G, \mathbb{Z})$. Let $\phi \in \mathrm{Hom}_G(G, \mathbb{Z})$. Let $g \in G$ be an element other than the identity. We have that $g^m = e$, and so $0 = \phi(e) = \phi(g^m) = m\phi(g)$. However, \mathbb{Z} is torsion free so it must be that $\phi(g) = 0$.

Finally, consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

If we look at the associated long exact sequence of cohomology we get

$$H_T^1(G, \mathbb{Q}) \longrightarrow H_T^1(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow H_T^2(G, \mathbb{Z}) \longrightarrow H_T^2(G, \mathbb{Q}).$$

Using that $H_T^r(G, \mathbb{Q}) = 0$ and $H_T^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_G(G, \mathbb{Q}/\mathbb{Z})$, we get the final claim. \square

Proposition 4.31. *Let G be a finite cyclic group and M a G -module. Then for all r there exists an isomorphism*

$$H_T^r(G, M) \xrightarrow{\cong} H_T^{r+2}(G, M)$$

depending only on the choice of generator of G .

Proof. Let g generate G with $\#G = m$. Let $N = 1 + g + g^2 + \cdots + g^{m-1}$. The fact that G is cyclic of order m gives that $N(g-1) = (g-1)N = g^m - 1 = 0$. Thus, we obtain a particularly simply resolution

$$\cdots \xrightarrow{g^{-1}} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{g^{-1}} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

We can use that $\text{Hom}_G(\mathbb{Z}[G], M) \cong M$ to get the complex

$$\cdots \xrightarrow{N} M \xrightarrow{g^{-1}} M \xrightarrow{N} M \xrightarrow{g^{-1}} M \longrightarrow 0.$$

From this it is clear that

$$\begin{aligned} H^{2r}(G, M) &\cong M^G/NM, \\ H^{2r+1}(G, M) &\cong \text{Ker}(N)/I_G M, \end{aligned}$$

for $r > 0$ where $\text{Ker}(N)$ is the kernel of the map $N : M \rightarrow M$.

To calculate the homology groups, we use the above projective resolution and tensor up first with M obtaining

$$\cdots \xrightarrow{g^{-1}} \mathbb{Z}[G] \otimes M \xrightarrow{N} \mathbb{Z}[G] \otimes M \xrightarrow{g^{-1}} \mathbb{Z}[G] \otimes M \longrightarrow M \longrightarrow 0.$$

We now apply the functor used to define homology

$$\cdots \xrightarrow{g^{-1}} (\mathbb{Z}[G] \otimes M)_G \xrightarrow{N} (\mathbb{Z}[G] \otimes M)_G \xrightarrow{g^{-1}} (\mathbb{Z}[G] \otimes M)_G \longrightarrow 0.$$

Observe that $(\mathbb{Z}[G] \otimes M)_G \cong \mathbb{Z}[G] \otimes_G M \cong M$, and so we obtain the complex used to define the cohomology. Thus, we have

$$\begin{aligned} H_T^{2r}(G, M) &\cong M^G/NM, \\ H_T^{2r+1}(G, M) &\cong \text{Ker}(N)/I_G M \end{aligned}$$

for all $r \neq 0, -1$. The following exercise then completes the proof. \square

Exercise 4.32. *Show that the result holds true for $r = 0, -1$ by using the connecting homomorphism Nm_G .*

In fact, we can specify the map between cohomology groups. Recall that $H^2(G, \mathbb{Z}) \cong \text{Hom}_G(G, \mathbb{Q}/\mathbb{Z})$. Let $\gamma \in H^2(G, \mathbb{Z})$ be the element that maps to the map sending g (the generator of G) to $1/m$. Then the map $H_T^r(G, M) \rightarrow H_T^{r+2}(G, M)$ is $\phi \mapsto \phi \cup \gamma$.

For G a finite cyclic group and M a G -module, if $H_T^0(G, M)$ and $H_T^1(G, M)$ are both finite, we define the *Herbrand quotient* to be

$$h(M) = \frac{\# H_T^0(G, M)}{\# H_T^1(G, M)}.$$

Proposition 4.33. *Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be an exact sequence of G -modules with G a finite cyclic group. If two of the three Herbrand quotients $h(A)$, $h(B)$, $h(C)$ are defined, then so is the third and

$$h(B) = h(A)h(C).$$

Proof. We apply the previous proposition to turn the long exact sequence of Tate cohomology groups into the following exact hexagon:

$$\begin{array}{ccc} & \mathrm{H}_T^0(G, A) \longrightarrow \mathrm{H}_T^0(G, B) & \\ & \nearrow & \searrow \\ \mathrm{H}_T^1(G, C) & & \mathrm{H}_T^0(G, C) \\ & \nwarrow & \swarrow \\ & \mathrm{H}_T^1(G, B) \longleftarrow \mathrm{H}_T^1(G, A) & \end{array}$$

Suppose for example that $\mathrm{H}_T^i(G, A)$ and $\mathrm{H}_T^i(G, B)$ are finite for $i = 0, 1$. Let M_1 be the image of $\mathrm{H}_T^0(G, A)$ in $\mathrm{H}_T^0(G, B)$, and so on around the hexagon. We have that M_2 and M_3 are finite groups, M_2 because it is the homomorphic image of a finite group and M_3 because it sits in a finite group. We have that sequence

$$0 \longrightarrow M_2 \longrightarrow \mathrm{H}_T^0(G, C) \longrightarrow M_3 \longrightarrow 0$$

is exact. Thus, we have that $\mathrm{H}_T^0(G, C)$ is finite. Similarly we obtain that $\mathrm{H}_T^1(G, C)$ is finite. If we set m_i to be the order of M_i , then we have that the orders of the group $\mathrm{H}_T^0(G, A) = m_6 m_1$, etc. This gives the claim that $h(B) = h(A)h(C)$. \square

Proposition 4.34. *Let G be as above and let M be a finite G -module, i.e., it is a finitely generated G -module. Then $h(M) = 1$.*

Proof. Recall that we saw for a finite group and a finitely generated module that all the cohomology groups are finite, so this statement makes sense. Consider the exact sequences

$$0 \longrightarrow M^G \longrightarrow M \xrightarrow{g-1} M \longrightarrow M_G \longrightarrow 0,$$

$$0 \longrightarrow H_T^1(G, M) \longrightarrow M_G \xrightarrow{\text{Nm}_G} M^G \longrightarrow H_T^0(G, A) \longrightarrow 0.$$

The first shows that M^G and M_G have the same order and the second shows that $H_T^0(G, M)$ and $H_T^1(G, M)$ have the same order. \square

Exercise 4.35. *Let M_1 and M_2 be G -modules, $f : M_1 \rightarrow M_2$ a G -module homomorphism with finite kernel and cokernel. If either $h(M_1)$ or $h(M_2)$ is defined, then so is the other and they are equal.*

Our reason for introducing the Tate cohomology groups is Tate's theorem. In order to prove Tate's theorem we will need the following exact sequence. Let M be a G -module and let M_0 be M considered only as an abelian group, i.e., we ignore the G -action. We can then consider the induced module $M_* = \text{Ind}_1^G(M_0)$.

Exercise 4.36. 1. *Show that $M_* \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ via the map $\varphi \mapsto \sum_{g \in G} g \otimes \varphi(g^{-1})$.*

2. *Show that M_* surjects onto M via the map $\varphi \mapsto \sum_{g \in G} g\varphi(g^{-1})$.*

Let M' be the kernel of the surjective homomorphism M_* onto M , i.e., we have the exact sequence

$$0 \longrightarrow M' \longrightarrow M_* \longrightarrow M \longrightarrow 0.$$

We will use this exact sequence in the proof of the following theorem.

Theorem 4.37. *Let G be a finite group and M a G -module. If*

$$H_T^1(H, M) = H_T^2(H, M) = 0$$

for all subgroups H of G , then $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$.

Proof. The result follows from the assumption and Proposition 4.31 if G is a cyclic group. We now consider the case when G is a solvable group and proceed by induction on the order of G . The base case is true. Thus, assume the result is true for all groups of order less than G . Since G is a solvable group by definition there exists a proper normal subgroup H so that G/H is cyclic. The fact that H has order less than G gives that we can apply the induction hypothesis to (H, M) and so $H_T^r(H, M) = 0$ for all $r \in \mathbb{Z}$. We have that $H_T^1(G, M) = H_T^2(G, M) = 0$ by assumption. We can now consider the Inflation-Restriction exact sequence:

$$0 \longrightarrow H_T^r(G/H, M^H) \xrightarrow{\text{Inf}} H_T^r(G, M) \xrightarrow{\text{Res}} H_T^r(H, M)$$

for all $r \geq 1$. This shows that $H_T^1(G/H, M^H) = H_T^2(G/H, M^H) = 0$. Now we use Proposition 4.31 and the fact that G/H is cyclic to conclude that

$H_T^r(G/H, M^H) = 0$ for all $r \geq 1$. We again use the Inflation-Restriction sequence to conclude that $H_T^r(G, M) = 0$ for all $r \geq 1$.

We now show that $H_T^0(G, M) = M^G / \text{Nm}_G(M) = 0$. Let $x \in M^G$. We know that $H_T^0(G/H, M^H) = 0$ and so there exists a $y \in M^H$ so that $\text{Nm}_{G/H}(y) = x$ by the definition of $H_T^0(G/H, M^H)$. Similarly, since $H_T^0(H, M) = 0$ we know that there exists a $z \in M$ so that $\text{Nm}_H(z) = x$. We now just use the fact that

$$\text{Nm}_G(z) = (\text{Nm}_{G/H} \circ \text{Nm}_G)(z) = x$$

to see that $H_T^0(G, M) = 0$.

It remains to deal with the case of negative r . Consider the exact sequence discussed above:

$$0 \longrightarrow M' \longrightarrow M_* \longrightarrow M \longrightarrow 0.$$

The fact that M_* is an induced module we know that $H_T^r(G, M_*) = 0$ for all r and all subgroups H of G . Thus, we obtain

$$H_T^r(H, M') = H_T^{r-1}(H, M)$$

for all r and all subgroups H of G . We can now apply what we have shown above, i.e., that $H_T^r(G, M) = 0$ for all $r \geq 0$ to conclude that $H_T^r(G, M') = 0$ for all $r \geq 1$. In particular, this shows that the pair (G, M') satisfies the hypotheses of the theorem and so by what we have shown above, $H_T^r(G, M') = 0$ for all $r \geq 0$. We now use that $H_T^0(G, M') = H_T^{-1}(G, M)$ to obtain that $H_T^{-1}(G, M) = 0$. Thus, our induction now shows that for (G, M) satisfying the hypotheses of the theorem that $H_T^r(G, M) = 0$ for $r \geq -1$. Apply this result again to (G, M') to obtain $H_T^{-2}(G, M) = 0$. Continuing like this we obtain $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$.

It now remains to deal with the general case. Let G be an arbitrary finite group. Let p be a prime and G_p the p -Sylow subgroup of G . If (G, M) satisfies the hypotheses of the theorem, then so does (G_p, M) . The fact that G_p is a p -group gives that it is a solvable group, and so we can apply what we have just shown to conclude that $H_T^r(G_p, M) = 0$ for all $r \in \mathbb{Z}$. We now apply Corollary 4.23 (in the case of Tate cohomology, it generalizes easily) to conclude that for every $r \in \mathbb{Z}$ and every prime p , $H_T^r(G, M)[p^\infty] = 0$. Thus, for each prime p the p -part of the group $H_T^r(G, M) = 0$ and so necessarily we have $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$. \square

Theorem 4.38. (*Tate's Theorem*) *Let G be a finite group and M a G -module. Suppose that for all subgroups H of G we have*

1. $H_T^1(H, M) = 0$ and
2. $H_T^2(H, M)$ is cyclic of order $[H : 1]$.

Then for every $r \in \mathbb{Z}$ there is an isomorphism

$$\mathbf{H}_T^r(G, \mathbb{Z}) \longrightarrow \mathbf{H}_T^{r+2}(G, M)$$

depending only on the choice of a generator for $\mathbf{H}_T^2(G, M)$.

Before we prove this theorem, we see how it will be useful for us in proving the results of local class field theory. Let K_v be a local field, L a finite extension of K_v , and $G = \text{Gal}(L/K_v)$. In the next chapter we will show that $\mathbf{H}_T^2(G, L^\times)$ is cyclic of order $[L : K]$ with a canonical generator $u_{L/K}$. Hilbert's theorem 90 gives that $\mathbf{H}_T^1(G, L^\times) = 0$, so Tate's theorem gives that the cup product with $u_{L/K}$ gives an isomorphism between $\mathbf{H}_T^{-2}(G, \mathbb{Z}) \xrightarrow{\cong} \mathbf{H}_T^0(G, L^\times)$. In particular, combining this with what we've already shown will give

$$G^{\text{ab}} \cong \mathbf{H}_1(G, \mathbb{Z}) = \mathbf{H}_T^{-2}(G, \mathbb{Z}) \xrightarrow{\cong} \mathbf{H}_T^0(G, L^\times) = K_v^\times / \text{Nm}(L^\times).$$

In particular, if $\text{Gal}(L/K_v)$ is abelian, then this shows that $K_v^\times / \text{Nm}(L^\times) \cong \text{Gal}(L/K_v)$.

Proof. (of Tate's Theorem) Let $\gamma \in \mathbf{H}_T^2(G, M)$ be a generator. For any subgroup H of G , we have that $\text{Res}(\gamma)$ is a generator of $\mathbf{H}_T^2(H, M)$. This follows from the fact that $\text{Cor} \circ \text{Res} = [G : H]$ and the assumption that $\mathbf{H}_T^2(H, M)$ is cyclic of order $[H : 1]$ for all subgroups H .

Let ϕ be a cocycle representing γ . Let Z be the free abelian group having the symbols x_σ as a basis where $\sigma \in G$, $\sigma \neq 1$. Set $M(\phi) = M \oplus Z$ and extend the action of G to an action on $M(\phi)$ by setting

$$\sigma(m, x_\tau) = (\sigma m + \phi(\sigma, \tau), x_{\sigma\tau} - x_\sigma)$$

and then extending linearly. One can check this is an action by first observing that

$$\sigma\tau(m, x_\rho) = (\sigma\tau m + \phi(\sigma\tau, \rho), x_{\sigma\tau\rho} - x_{\sigma\tau})$$

and

$$\begin{aligned} \sigma(\tau(m, x_\rho)) &= \sigma(\tau m + \phi(\tau, \rho), x_{\tau\rho} - x_\tau) \\ &= \sigma(\tau m + \phi(\tau, \rho), x_{\tau\rho}) - \sigma(0, x_\tau) \\ &= (\sigma\tau m + \sigma\phi(\tau, \rho) + \phi(\sigma, \tau\rho), x_{\sigma\tau\rho} - x_\sigma) - (\phi(\sigma, \tau), x_{\sigma\tau} - x_\sigma) \\ &= (\sigma\tau m + \sigma\phi(\tau, \rho) + \phi(\sigma, \tau\rho) - \phi(\sigma, \tau), x_{\sigma\tau\rho} - x_{\sigma\tau}). \end{aligned}$$

Thus, we have

$$\sigma\tau(m, x_\rho) - \sigma(\tau(m, x_\rho)) = (\phi(\sigma\tau, \rho) - \sigma\phi(\tau, \rho) - \phi(\sigma, \tau\rho) + \phi(\sigma, \tau), 0).$$

We now just use that $\phi \in \mathbf{H}_T^2(G, M) = \mathbf{H}^2(G, M)$ to see that

$$\phi(\sigma\tau, \rho) - \sigma\phi(\tau, \rho) - \phi(\sigma, \tau\rho) + \phi(\sigma, \tau) = 0$$

(this is the cocycle condition for the second cohomology group!)

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Recall the exact sequence

We know that $H_T^r(H, \mathbb{Z}[G]) = 0$ for all $r \in \mathbb{Z}$ as $\mathbb{Z}[G]$ is an induced module, and so the long exact sequence of Tate cohomology groups gives

$$\begin{aligned} H_T^1(H, I_G) &\cong H_T^0(H, \mathbb{Z}) \cong \mathbb{Z}/[H : 1]\mathbb{Z}, \\ H_T^2(H, I_G) &\cong H_T^1(H, \mathbb{Z}) = 0 \end{aligned}$$

where we use that $H_T^1(H, \mathbb{Z}) = 0$ for all finite groups H . Set $f : M(\phi) \rightarrow \mathbb{Z}[G]$ to be the linear extension of the map given by $f((m, x_\tau)) = \tau - 1$ for all $m \in M$, $x_\tau \in \mathbb{Z}$. This map gives an exact sequence of G -modules:

$$0 \longrightarrow M \longrightarrow M(\phi) \xrightarrow{f} I_G \longrightarrow 0.$$

We can use the associated long exact sequence of Tate cohomology groups to show that

$$H_T^1(H, M(\phi)) = H_T^2(H, M(\phi)) = 0.$$

The long exact sequence is given by

$$0 \longrightarrow H_T^1(H, M(\phi)) \longrightarrow H_T^1(H, I_G) \longrightarrow H_T^2(H, M) \longrightarrow H_T^2(H, M(\phi)) \longrightarrow 0$$

where we obtain the zeroes on the end by virtue of the fact that $H_T^1(H, M) = 0$ by assumption and $H_T^2(H, I_G) = 0$ by what we have shown above. We claim that the map $H_T^2(H, M) \rightarrow H_T^2(H, M(\phi))$ is the zero map. Consider the map $\psi : G \rightarrow M(\phi)$ given by $\psi(\sigma) = (0, x_\sigma)$. One has that

$$\begin{aligned} d^1\psi(\sigma, \tau) &= \sigma\psi(\tau) - \psi(\sigma\tau) + \psi(\sigma) \\ &= (\phi(\sigma, \tau), 0). \end{aligned}$$

This shows that ϕ is in the image of the boundary map d^1 used to define the cohomology groups $H^r(G, M(\phi))$. In particular, this shows that ϕ is trivial in $H_T^2(G, M(\phi))$. However, we know that $H_T^2(H, M)$ is generated by $\text{Res}(\gamma)$, which maps to the restriction of γ in $H_T^2(H, M(\phi))$, which is zero. Thus, we must have that $H_T^1(H, I_G) \rightarrow H_T^2(H, M)$ is an onto map. Since each of these groups has order $[H : 1]$, it must be that this map is an isomorphism and so the kernel and cokernel must both be 0, namely, $H_T^1(H, M(\phi))$ and $H_T^2(H, M(\phi))$. This fact, combined with Theorem 4.37 gives that $H_T^r(G, M(\phi)) = 0$ for all $r \in \mathbb{Z}$.

To finish the proof, we combine the two short exact sequences used above to conclude that $H_T^r(G, \mathbb{Z}) \cong H_T^{r+1}(G, I_G)$ and $H_T^{r+1}(G, I_G) \cong H_T^{r+2}(G, M)$. Thus, we have

$$H_T^r(G, \mathbb{Z}) \cong H_T^{r+2}(G, M)$$

for all $r \in \mathbb{Z}$.

□

Chapter 5

Main Results of Local Class Field Theory

5.1 Statements of the theorems

We briefly state here the main results of local class field theory. In the next section we will use the group cohomology theory developed in the previous chapter to give proofs of these results. The notation here is that of Chapter 3.

For K_v a nonarchimedean local field, let K_v^{ab} be the maximal abelian extension of K_v , i.e., the union of all finite abelian extensions of K_v contained in \overline{K}_v . The first theorem is generally referred to as the “Local Reciprocity Law”.

Theorem 5.1. *Let K_v be a nonarchimedean local field. There is a unique group homomorphism*

$$\phi_{K_v} : K_v^\times \longrightarrow \text{Gal}(K_v^{\text{ab}}/K_v)$$

satisfying the following properties:

1. *for ϖ_v a uniformizer of K_v , $\phi_{K_v}(\varpi_v)$ acts on K_v^{ur} as Frob_{K_v} ;*
2. *for any finite abelian extension L of K_v , the kernel of $x \mapsto \phi_{K_v}(x)|_L$ contains $\text{Nm}_{L/K_v}(L^\times)$ and ϕ_{K_v} induces an isomorphism*

$$\phi_{L/K_v} : K_v^\times / \text{Nm}(L^\times) \longrightarrow \text{Gal}(L/K_v).$$

Given L/K_v a finite abelian extension, the Local Reciprocity Law gives that $\phi_{L/K_v}(\varpi_v) = \text{Frob}_{L/K_v}$ for any uniformizer ϖ_v of K_v . In fact, one could phrase part (1) in terms of the restriction of $\phi_{K_v}(\varpi_v)$ to L if one wished. The map ϕ_{K_v} is known as the *local Artin map*, the *local reciprocity map*, or the *norm residue symbol*.

Let $u \in \mathcal{O}_v^\times$. The fact that $u\varpi_v$ is still a uniformizer for any uniformizer ϖ_v combines with part (1) of the Local Reciprocity Law to show that \mathcal{O}_v^\times lies in the kernel of $x \mapsto \phi_{K_v}(x)|_{K_v^{\text{ur}}}$. In particular, this shows that the map $\phi_{K_v} : K_v^\times \rightarrow \text{Gal}(K_v^{\text{ur}}/K_v)$ factors through the maps

$$K_v^\times \xrightarrow{\text{ord}_{K_v}} \mathbb{Z} \xrightarrow{n \mapsto \text{Frob}_{K_v}^n} \text{Gal}(K_v^{\text{ur}}/K_v).$$

Theorem 5.2. *Let N be a subgroup of K_v^\times . The subgroup N is of the form $\text{Nm}_{L/K_v}(L^\times)$ for some finite abelian extension L/K_v if and only if N is of finite index and open.*

Exercise 5.3. *Prove that if K_v has characteristic 0, then every subgroup of K_v^\times that is of finite index is necessarily open. (This is not the case if $\text{char}(K_v) = p > 0$.)*

Exercise 5.4. *The map $L \mapsto \text{Nm}_{L/K_v}(L^\times)$ gives a bijection between the set of finite abelian extensions of K_v and the set of open subgroups of finite index in K_v^\times . Moreover, one has*

1. $L_1 \subset L_2$ if and only if $\text{Nm}_{L_1/K_v}(L_1^\times) \supset \text{Nm}_{L_2/K_v}(L_2^\times)$;
2. $\text{Nm}_{L_1 L_2/K_v}(L_1 L_2) = \text{Nm}_{L_1/K_v}(L_1^\times) \cap \text{Nm}_{L_2/K_v}(L_2^\times)$;
3. $\text{Nm}_{(L_1 \cap L_2)/K_v}(L_1 \cap L_2) = \text{Nm}_{L_1/K_v}(L_1) \text{Nm}_{L_2/K_v}(L_2^\times)$.

(Hint: First consider a finite abelian extension E/K_v and subfields of E . One can use the Local Reciprocity Law to phrase this exercise in terms of Galois theory. From there, just let E grow to get the final result.)

The following theorem shows that while local class field theory classifies the abelian extensions of a local field in terms of norm groups, this approach cannot be extended to obtain results about nonabelian extensions.

Theorem 5.5. (Norm Limitation Theorem) *Let E be a finite Galois extension of K_v and let L be the largest abelian extension of K_v contained in E . Then*

$$\text{Nm}_{E/K_v}(E^\times) = \text{Nm}_{L/K_v}(L^\times).$$

Proof. We know that $\text{Nm}_{E/K_v} = \text{Nm}_{E/L} \circ \text{Nm}_{L/K_v}$ and so $\text{Nm}_{E/K_v}(E^\times) \subset \text{Nm}_{L/K_v}(L^\times)$. However, we also have that $\text{Gal}(E/K_v)^{\text{ab}} = \text{Gal}(L/K_v)$ and so we have

$$K_v^\times / \text{Nm}_{L/K_v}(L^\times) = \text{Gal}(L/K_v) = \text{Gal}(E/K_v)^{\text{ab}} = K_v^\times / \text{Nm}_{E/K_v}(E^\times).$$

Since we have $\text{Nm}_{E/K_v}(E^\times) \subset \text{Nm}_{L/K_v}(L^\times)$ and both of the norm groups have the same index in K_v^\times , we must have equality. \square

5.2 The fundamental class

Our first goal in this section is to prove the following theorem.

Theorem 5.6. *Let L/K_v be a finite Galois extension of degree n with Galois group G . Then $H_1^2(L/K_v)$ is cyclic of order n .*

We begin by showing that the cohomology of the units is trivial. To prove this we need several lemmas.

Lemma 5.7. *Let L/K_v be a finite unramified extension and let $m > 0$. Then we have*

$$\begin{aligned} \mathcal{O}_L^\times / (1 + \mathfrak{m}_L) &\xrightarrow{\cong} l^\times \\ (1 + \mathfrak{m}_L^m) / (1 + \mathfrak{m}_L^{m+1}) &\xrightarrow{\cong} l \end{aligned}$$

as G -modules where l is the residue field of L .

Proof. Note that since L/K_v is unramified, ϖ_v is also a uniformizer of L and so we can write

$$(1 + \mathfrak{m}_L^m) = \{1 + a\varpi_v^m : a \in \mathcal{O}_L\}.$$

The isomorphisms then follow readily from the maps

$$\begin{aligned} \mathcal{O}_L^\times &\rightarrow l^\times \\ u &\mapsto u \pmod{\mathfrak{m}_L} \end{aligned}$$

and

$$\begin{aligned} (1 + \mathfrak{m}_L^m) &\rightarrow l \\ (1 + a\varpi_v^m) &\mapsto a \pmod{\mathfrak{m}_L}. \end{aligned}$$

□

Lemma 5.8. *Let L/K_v be a finite unramified extension. For all $r \in \mathbb{Z}$, $H_{\mathbb{T}}^r(G, l^\times) = 0$.*

Proof. We know that $H_{\mathbb{T}}^1(G, l^\times) = 0$ by Hilbert's Theorem 90. The fact that l^\times is finite, so in particular it is a finite G -module implies that the Herbrand quotient $h(l^\times) = 1$ (see Proposition 4.34.) Thus, by the definition of the Herbrand quotient we see that $H_{\mathbb{T}}^0(G, l^\times) = 0$. However, since L/K_v is unramified, it is necessarily cyclic and so we can apply Proposition 4.31 to conclude that $H_{\mathbb{T}}^r(G, l^\times) = 0$ for all $r \in \mathbb{Z}$. □

Note that the previous lemma implies that the norm map from $l^\times \rightarrow k_v^\times$ is surjective. To see this, recall that since L/K_v is unramified we have $\text{Gal}(L/K_v) \cong \text{Gal}(l/k_v)$. Thus, the norm map $\text{Nm}_G : H_0(G, l^\times) \rightarrow H^0(G, l^\times)$ is precisely the usual norm map. We have that $H_{\mathbb{T}}^0(G, l^\times) = 0$ from the previous lemma, but we also know that $H_{\mathbb{T}}^0(G, l^\times) = (l^\times)^G / \text{Nm}_G(l^\times) = k_v^\times / \text{Nm}_G(l^\times)$. Thus, we must have $k_v^\times = \text{Nm}_G(l^\times)$ as claimed.

Lemma 5.9. *Let L/K_v be a finite unramified extension. The groups $H_{\mathbb{T}}^r(G, l) = 0$ for all $r \in \mathbb{Z}$.*

Proof. We begin by observing again that since L/K_v is unramified, we have $G \cong \text{Gal}(l/k_v)$. This allows us to use Proposition 4.13 to conclude that $H_{\mathbb{T}}^r(G, l) = 0$ for all $r \geq 0$. Now we just use that G is cyclic along with Proposition 4.31 to finish the proof. □

Exercise 5.10. For L/K_v finite and unramified, show that the trace map $l \rightarrow k_v$ is surjective.

Proposition 5.11. Let L/K_v be a finite unramified extension. The norm map $\text{Nm}_{L/K_v} : \mathcal{O}_L^\times \rightarrow \mathcal{O}_v^\times$ is surjective.

Proof. Let $u \in \mathcal{O}_v^\times$. We have shown that the norm map from $l^\times \rightarrow k_v^\times$ is surjective. We also have that $l^\times \cong \mathcal{O}_L^\times / (1 + \mathfrak{m}_L)$ and similarly for k_v^\times . This allows us to find $v_0 \in \mathcal{O}_L^\times$ so that $\text{Nm}(v_0)(1 + \mathfrak{m}_v) = u \pmod{1 + \mathfrak{m}_v}$, i.e., $u/\text{Nm}(v_0) \in (1 + \mathfrak{m}_v)$. We also showed that $l \cong (1 + \mathfrak{m}_L^i)/(1 + \mathfrak{m}_L^{i+1})$ for all $i \geq 1$ and similarly for k_v . Combining this with the surjectivity of the trace map gives that the norm map $(1 + \mathfrak{m}_L)/(1 + \mathfrak{m}_L^2) \rightarrow (1 + \mathfrak{m}_v)/(1 + \mathfrak{m}_v^2)$ is surjective. As such, we can find $v_1 \in (1 + \mathfrak{m}_L)$ so that $\text{Nm}(v_1)(1 + \mathfrak{m}_v^2) = u/\text{Nm}(v_0)(1 + \mathfrak{m}_v^2)$, i.e., $u/\text{Nm}(v_0 v_1) \in (1 + \mathfrak{m}_v^2)$. We now continue in this pattern to form a sequence $v_0, v_1, \dots, v_n \in (1 + \mathfrak{m}_v^n)$ so that $u/\text{Nm}(v_0 \cdots v_n) \in (1 + \mathfrak{m}_v^{n+1})$. Now just set $v = \prod_{i=0}^\infty v_i$ and observe that $u/\text{Nm}(v) \in \bigcap_{i=0}^\infty (1 + \mathfrak{m}_v^i) = \{1\}$. Thus, the norm map is surjective. \square

Corollary 5.12. Let L/K_v be an arbitrary unramified extension with Galois group G (we no longer require finite!) We have

$$\mathrm{H}_T^r(G, \mathcal{O}_L^\times) = 0$$

for all $r \in \mathbb{Z}$ when G is finite and for all $r > 0$ when G is infinite.

Proof. First suppose that L/K_v is a finite unramified extension. Recall that

$$L^\times \cong \mathcal{O}_L^\times \times \varpi_v^{\mathbb{Z}}$$

where we use that ϖ_v is a uniformizer of L since L/K_v is unramified. Thus, we have $\mathrm{H}_T^r(G, L^\times) = \mathrm{H}_T^r(G, \mathcal{O}_L^\times) \oplus \mathrm{H}_T^r(G, \varpi_v^{\mathbb{Z}})$. However, Hilbert's theorem 90 gives that $\mathrm{H}_T^1(G, L^\times) = 0$ and so $\mathrm{H}_T^1(G, \mathcal{O}_L^\times) = 0$. We now use the previous proposition that the norm map from \mathcal{O}_L^\times to \mathcal{O}_v^\times is surjective to obtain that $\mathrm{H}_T^0(G, \mathcal{O}_L^\times) = 0$. The fact that G is necessarily cyclic combines with Proposition 4.31 to give the result for finite unramified extensions.

Suppose now that L/K_v is unramified and possibly infinite. We no longer have well-defined Tate cohomology groups for $r < 0$, but we can work with continuous cohomology groups for $r > 0$. In this case we have that

$$\mathrm{H}^r(G, \mathcal{O}_L^\times) = \varinjlim_{K'} \mathrm{H}_T^r(\mathrm{Gal}(K'/K), \mathcal{O}_{K'}^\times)$$

where the limit is over finite unramified extensions of K contained in L . Since each term of the limit is 0, we have the result. \square

Note that the previous result shows that $\mathrm{H}^r(\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v), \mathcal{O}_{K_v^{\mathrm{ur}}}^\times) = 0$ for K_v^{ur} the maximal unramified extension of K_v .

The decomposition $L^\times \cong \mathcal{O}_L^\times \times \varpi_v^{\mathbb{Z}}$ can be rewritten as an exact sequence

$$0 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{\text{ord}_L} \mathbb{Z} \longrightarrow 0.$$

The long exact sequence of cohomology along with Corollary 5.12 gives that

$$H_{\mathbb{T}}^2(G, L^\times) \cong H_{\mathbb{T}}^2(G, \mathbb{Z}).$$

Recall we also have an isomorphism

$$H_{\mathbb{T}}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H_{\mathbb{T}}^2(G, \mathbb{Z})$$

given in Lemma 4.30. Since the G -action on \mathbb{Q}/\mathbb{Z} is the trivial one, we have

$$H_{\mathbb{T}}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z}).$$

Let L/K_v have degree $n < \infty$. Recall that G is then a finite cyclic group of order n generated by Frob_{L/K_v} . One can then see that the map

$$f \mapsto f(\text{Frob}_{L/K_v}) : \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is an isomorphism from $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ onto the unique cyclic subgroup $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ of order n of \mathbb{Q}/\mathbb{Z} .

Now suppose that L/K_v has infinite degree. In this case we have that G is the closure of the group $\{\text{Frob}_{L/K_v}^i : i \in \mathbb{Z}\}$ and the map

$$(5.1) \quad f \mapsto f(\text{Frob}_{L/K_v}) : \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is an isomorphism from $\text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z})$ onto an infinite subgroup of \mathbb{Q}/\mathbb{Z} .

Exercise 5.13. Let $L = K_v^{\text{ur}}$. Show that the map given in equation (5.1) gives an isomorphism between $\text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z})$ and \mathbb{Q}/\mathbb{Z} .

Set $H_{\mathbb{T}}^2(L/K_v) = H_{\mathbb{T}}^2(\text{Gal}(L/K_v), L^\times)$ for any extension of fields L/K_v . We can now define the *invariant map* $\text{inv}_{L/K_v} : H_{\mathbb{T}}^2(G, L^\times) \longrightarrow \mathbb{Q}/\mathbb{Z}$ by

$$H_{\mathbb{T}}^2(L/K_v) \xrightarrow{\cong} H_{\mathbb{T}}^2(G, \mathbb{Z}) \xrightarrow[\cong]{\delta^{-1}} H_{\mathbb{T}}^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma_{L/K_v}} \mathbb{Q}/\mathbb{Z}$$

where γ_{L/K_v} is the map given by $\gamma_{L/K_v} : f \mapsto f(\text{Frob}_{L/K_v})$. Note that for $L = K_v^{\text{ur}}$, the invariant map $\text{inv}_{K_v} := \text{inv}_{K_v^{\text{ur}}/K_v}$ is a canonical isomorphism between $H_{\mathbb{T}}^2(K_v^{\text{ur}}/K_v)$ and \mathbb{Q}/\mathbb{Z} so such that if E/K_v is a finite unramified extension of degree n , then inv_{K_v} induces an isomorphism $H_{\mathbb{T}}^2(E/K_v) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Exercise 5.14. Let $K_v \subset E \subset F$ be a tower of fields with both E and F contained in K_v^{ur} . Prove that the diagram

commutes.

Proposition 5.15. Let L/K_v be a finite extension of degree n . (We are not assuming unramified here!) The following diagram commutes:

$$\begin{array}{ccc}
\mathrm{H}_{\mathrm{T}}^2(E/K_v) & \xrightarrow{\mathrm{inv}_{E/K_v}} & \mathbb{Q}/\mathbb{Z} \\
\mathrm{Inf} \downarrow & & \downarrow = \\
\mathrm{H}_{\mathrm{T}}^2(F/K_v) & \xrightarrow{\mathrm{inv}_{F/K_v}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

$$\begin{array}{ccc}
\mathrm{H}_{\mathrm{T}}^2(K_v^{\mathrm{ur}}/K_v) & \xrightarrow{\mathrm{Res}} & \mathrm{H}_{\mathrm{T}}^2(L^{\mathrm{ur}}/L) \\
\mathrm{inv}_{K_v} \downarrow & & \downarrow \mathrm{inv}_L \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

$$\begin{array}{ccccccc}
\mathrm{H}_{\mathrm{T}}^2(K_v^{\mathrm{ur}}/K_v) & \xrightarrow{\mathrm{ord}_{K_v}} & \mathrm{H}_{\mathrm{T}}^2(\Gamma_{K_v}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}_{\mathrm{cts}}(\Gamma_{K_v}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_{K_v}} & \mathbb{Q}/\mathbb{Z} \\
\mathrm{Res} \downarrow & & e \cdot \mathrm{Res} \downarrow & & e \cdot \mathrm{Res} \downarrow & & n \downarrow \\
\mathrm{H}_{\mathrm{T}}^2(L^{\mathrm{ur}}/L) & \xrightarrow{\mathrm{ord}_L} & \mathrm{H}_{\mathrm{T}}^2(\Gamma_L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}_{\mathrm{cts}}(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_L} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

Proof. Set $\Gamma_{K_v} = \mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$ and similarly for Γ_L . Let $f = [l : k_v]$ and e the ramification index. Set $\gamma_{K_v} := \gamma_{K_v^{\mathrm{ur}}/K_v}$ and similarly for γ_L . Consider the following diagram

Call the leftmost square (1), the middle one (2), and the third one (3). We claim that each of these squares commutes. Square (1) commutes because of the fact that ord_L is equal to $e \cdot \mathrm{ord}_{K_v}$ on K_v^{ur} . The fact that square (2) commutes is clear. Square (3) commutes because of the fact that $\mathrm{Frob}_L = \mathrm{Frob}_{K_v}^f$. The result is now clear from the definition of inv_{K_v} and inv_L . \square

Corollary 5.16. *Let L/K_v be a finite extension of degree n and set $\mathrm{H}_{\mathrm{T}}^2(L/K_v)_{\mathrm{ur}} = \mathrm{H}_{\mathrm{T}}^2(L/K_v) \cap \mathrm{H}_{\mathrm{T}}^2(K_v^{\mathrm{ur}}/K_v)$. Then $\mathrm{H}_{\mathrm{T}}^2(L/K_v)_{\mathrm{ur}}$ is cyclic of order n and is generated by the element $u_{L/K_v} \in \mathrm{H}_{\mathrm{T}}^2(K_v^{\mathrm{ur}}/K_v)$ such that $\mathrm{inv}_{K_v}(u_{L/K_v}) = \frac{1}{n}$.*

Proof. Observe that we have an exact sequence

$$0 \longrightarrow \mathrm{H}_{\mathrm{T}}^2(L/K_v)_{\mathrm{ur}} \longrightarrow \mathrm{H}_{\mathrm{T}}^2(K_v^{\mathrm{ur}}/K_v) \xrightarrow{\mathrm{Res}} \mathrm{H}_{\mathrm{T}}^2(L^{\mathrm{ur}}/L).$$

We can combine this with the previous proposition to obtain the following commuting diagram

We now use the fact that inv_{K_v} is an isomorphism to obtain that $\mathrm{H}_{\mathrm{T}}^2(L/K_v)_{\mathrm{ur}} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ and the corollary follows. \square

Exercise 5.17. *Let L/K_v be a finite extension of degree n . Show that n divides the order of $\mathrm{H}_{\mathrm{T}}^2(L/K_v)$.*

$$\begin{array}{ccccccc}
0 & \longrightarrow & H_{\mathbb{T}}^2(L/K_v)_{\text{ur}} & \longrightarrow & H_{\mathbb{T}}^2(K_v^{\text{ur}}/K_v) & \xrightarrow{\text{Res}} & H_{\mathbb{T}}^2(L^{\text{ur}}/L) \\
& & & & \downarrow \text{inv}_{K_v} & & \downarrow \text{inv}_L \\
0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

We have shown that for L/K_v a finite unramified extension with Galois group G that we have $H_{\mathbb{T}}^r(G, \mathcal{O}_L^\times) = 0$ for all $r \in \mathbb{Z}$. Now let L/K_v be an arbitrary finite Galois extension with Galois group G . We do not get such a strong result in this case, but we do have the following results which are enough for what is needed.

Lemma 5.18. *Let L/K_v be a finite Galois extension with Galois group G . There exists an open subgroup U of \mathcal{O}_L stable under the action of G so that $H_{\mathbb{T}}^r(G, U) = 0$ for all $r \in \mathbb{Z}$.*

Proof. Let $\{x_\sigma : \sigma \in G\}$ be a basis of L over K_v as given in the Normal Basis Theorem. Since G is finite, the x_σ have a common denominator d in \mathcal{O}_v . We can replace each x_σ with dx_σ to obtain a basis with elements in \mathcal{O}_L . Set $U = \sum \mathcal{O}_L x_\sigma$. Then we have

$$U \cong \mathcal{O}_L[G] = \text{Ind}_1^G \mathcal{O}_L.$$

From this it is clear that $H_{\mathbb{T}}^r(G, U) = 0$ for all $r \in \mathbb{Z}$. \square

Proposition 5.19. *Let L/K_v be a finite Galois extension with Galois group G . There exists an open subgroup $U \subset \mathcal{O}_L^\times$ stable under the action of G so that*

$$H_{\mathbb{T}}^r(G, U) = 0$$

for all $r \in \mathbb{Z}$.

Before we can prove this proposition we need the following exercise.

Exercise 5.20. *Let K_v be a nonarchimedean local field with residue characteristic p . The power series*

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

gives an isomorphism

$$\mathfrak{m}_v^n \xrightarrow{\exp} 1 + \mathfrak{m}_v^n$$

for $n > \frac{e}{p-1}$ where $e = e(K_v/\mathbb{Q}_p)$ with inverse map

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots.$$

Proof. (of Proposition 5.19) From the previous exercise we have that the map \exp defines an isomorphism between an open neighborhood of 0 in L onto an open neighborhood of 1 in L^\times with inverse given by \log . It is also clear that both of these maps commute with the G -action. Let V be an open neighborhood of 0 as in the previous proposition. Then we can take $\varpi_v^M V$ as an open and it will also be an open neighborhood of 0 with $H_{\mathbb{T}}^r(G, \varpi_v^M V) = 0$ for all $r > 0$. Now just take $U = \varpi_v^M V$ with M chosen sufficiently large so that \exp is a local isomorphism. The result then follows. \square

Corollary 5.21. *Let L/K_v be a cyclic extension of degree n with Galois group G . Then we have $h(\mathcal{O}_L^\times) = 1$ and $h(L^\times) = n$.*

Proof. Let U be an open subgroup of \mathcal{O}_L^\times so that $H_{\mathbb{T}}^r(G, U) = 0$ for all r . We have seen that the Herbrand quotient is multiplicative, so we have $h(\mathcal{O}_K^\times) = h(U)h(\mathcal{O}_L^\times/U)$. We know that \mathcal{O}_L^\times is compact, and so \mathcal{O}_L^\times/U is a finite set. Thus, $h(\mathcal{O}_L^\times/U) = 1$. We have that $h(U) = 1$ by the choice of U and so $h(\mathcal{O}_L^\times) = 1$.

We have that $L^\times/\mathcal{O}_L^\times \cong \mathbb{Z}$ and so $h(L^\times) = h(\mathbb{Z})h(\mathcal{O}_L^\times) = h(\mathbb{Z})$. However, we have already seen that $\#H_{\mathbb{T}}^0(G, \mathbb{Z}) = n$ and $H_{\mathbb{T}}^1(G, \mathbb{Z})$ is trivial, so we have $h(\mathbb{Z}) = n$ and thus $h(L^\times) = n$ as claimed. \square

Corollary 5.22. *Let L/K_v be a cyclic extension of degree n with Galois group G . Then $H_{\mathbb{T}}^2(L/K_v)$ is of order n .*

Proof. We have that $h(L^\times) = n$ and so

$$n = \frac{\#H_{\mathbb{T}}^0(G, L^\times)}{\#H_{\mathbb{T}}^1(G, L^\times)}.$$

However, we know by Hilbert theorem 90 that $H_{\mathbb{T}}^1(G, L^\times)$ is trivial. Applying the periodicity we obtain from the fact that L/K_v is cyclic gives the result. \square

In order to finish proving Theorem 5.6, we need the following messy lemma.

Lemma 5.23. *Let G be a finite group and M a G -module. Let $q, r \in \mathbb{Z}_{\geq 0}$. Assume that:*

1. $H_{\mathbb{T}}^i(H, M) = 0$ for all $0 < i < r$ and all subgroups H of G ;
2. if $H \subset K \subset G$, with H normal in K and K/H cyclic of prime order, then the order of $H_{\mathbb{T}}^r(H, M)$ divides $[K : H]^q$.

Then the same is true of G , i.e., $H_{\mathbb{T}}^r(G, M)$ is of order dividing $[G : 1]^q$.

Proof. For a prime p , let G_p denote the p -Sylow subgroup of G . We have seen that the restriction map $\text{Res} : H_{\mathbb{T}}^r(G, M) \rightarrow H_{\mathbb{T}}^r(G_p, M)$ is injective on $H_{\mathbb{T}}^r(G, M)[p^\infty]$. Since we are interested in the order of $H_{\mathbb{T}}^r(G, M)$, this allows us to restrict to studying $H_{\mathbb{T}}^r(G_p, M)$. Thus, we assume that G is a p -group and proceed by induction on the order of G .

We may assume that G has order greater than 1. Choose a normal subgroup H of G of index p . We can apply the induction hypothesis to the p -group G/H giving that the order of $H_T^r(G/H, M^H)$ divides $[G : H]^q = p^q$ for all $r > 0$. We also obtain from the induction hypothesis that the order of $H_T^r(H, M)$ divides $[H : 1]^q$. The first assumption in the hypotheses gives an exact sequence

$$0 \longrightarrow H_T^r(G/H, M^H) \xrightarrow{\text{Inf}} H_T^r(G, M) \xrightarrow{\text{Res}} H_T^r(H, M).$$

This gives that $H_T^r(G, M)$ has order dividing $\# H_T^r(G/H, M^H) \# H_T^r(H, M) = [G : H]^q [H : 1]^q = [G : 1]^q$ as claimed. This gives the result for all $r > 0$. The $r = 0$ case is handled by the following exercise. \square

Exercise 5.24. Complete the $r = 0$ case of the preceding proof. The following exact sequence may be helpful

$$M^H / \text{Nm}_H(M) \xrightarrow{\text{Nm}_{G/H}} M^G / \text{Nm}_G(M) \xrightarrow{\text{id}} (M^H)^{G/H} / \text{Nm}_{G/H}(M^H).$$

We restate Theorem 5.6 with a little more detail.

Theorem 5.25. Let L/K_v be a finite Galois extension of degree n with Galois group G . We have that $H_T^2(L/K_v)$ is cyclic of degree n . Furthermore, there exists a canonical element $u_{L/K_v} \in H_T^2(L_{\text{ur}}/K_v)$ generating $H_T^2(L/K_v)$ so that $\text{inv}_{K_v}(u_{L/K_v}) = \frac{1}{n}$.

Proof. We apply Lemma 5.23 to the situation with $M = L^\times$, $q = 1$, and $r = 2$. Note that the first hypothesis is given by Hilbert's theorem 90. The second hypothesis is given by Corollary 5.22. Thus, we have that $H_T^2(L/K_v)$ has order dividing n . However, we already know that $H_T^2(L/K_v)$ contains a cyclic subgroup of order n generated by u_{L/K_v} such that $\text{inv}_{K_v}(u_{L/K_v}) = \frac{1}{n}$, namely, we saw that $H_T^2(L/K_v)_{\text{ur}} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Thus we must have $H_T^2(L/K_v)$ is cyclic of order n generated by u_{L/K_v} as claimed. \square

The generator u_{L/K_v} is generally referred to as the *fundamental class*. It will be used to define the local reciprocity map in the next section.

Corollary 5.26. We have

$$H_T^2(\overline{K}_v/K_v) = H_T^2(K_v^{\text{ur}}/K_v).$$

Proof. Observe that since $K_v^{\text{ur}} \subset \overline{K}_v$, we have that $H_T^2(K_v^{\text{ur}}/K_v)$ is a subgroup of $H_T^2(\overline{K}_v/K_v)$. Thus, we just need to show containment in the other direction. The previous theorem shows that given any Galois extension L/K_v , $H_T^2(L/K_v)$ is a cyclic group of order n . This shows that $H_T^2(L/K_v)$ is contained in $H_T^2(K_v^{\text{ur}}/K_v)$. Since $H_T^2(\overline{K}_v/K_v)$ is the union of all such $H_T^2(L/K_v)$, we have the result. \square

The previous corollary will be important when we study Brauer groups, but now we use it to give the following theorem, which will be used in the next section when defining the local reciprocity map.

Theorem 5.27. *There exists a canonical isomorphism*

$$\mathrm{inv}_{K_v} : H_T^2(\overline{K}_v/K_v) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

Moreover, if L/K_v is a finite Galois extension of degree n with Galois group G , we have that the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_T^2(L/K_v) & \longrightarrow & H_T^2(\overline{K}_v/K_v) & \xrightarrow{\mathrm{Res}} & H_T^2(\overline{K}_v/L) \\ & & & & \downarrow \mathrm{inv}_{K_v} & & \downarrow \mathrm{inv}_L \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes. Thus, we recover the invariant map $\mathrm{inv}_{L/K_v} : H_T^2(L/K_v) \rightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

5.3 The local reciprocity map

In this section we define the local reciprocity map ϕ_{K_v} and prove several of its basic properties.

Theorem 5.28. *Let L/K_v be a finite Galois extension with Galois group G . The cup product by u_{L/K_v} defines an isomorphism of G^{ab} onto $K_v^\times/\mathrm{Nm}(L^\times)$. We write the inverse of this map as ϕ_{L/K_v} .*

Given $x \in K_v$, we will write $\phi_{L/K_v}(x)$ for the value $\phi_{L/K_v}(\bar{x})$ where \bar{x} is the class of x in $K_v^\times/\mathrm{Nm}(L^\times)$. This should cause no confusion to the reader. It is customary in other sources to write $(x, L/K_v)$ to denote $\phi_{L/K_v}(\bar{x})$.

This theorem follows immediately from the following more general result upon substituting $r = -2$ into the result.

Theorem 5.29. *Let L/K_v be a finite Galois extension. Then the cup product $\alpha \mapsto \alpha \cup u_{L/K_v}$ defines an isomorphism between $H_T^r(G, \mathbb{Z})$ and $H_T^{r+2}(G, L^\times)$.*

Proof. This is an immediate consequence of the results of the last section combined with Tate's theorem 4.38. \square

We would like some functoriality of this isomorphism in terms of the fields involved, which the following proposition provides. It relies heavily on properties of the cup product which were not proven. We first prove the following lemma.

Lemma 5.30. *Let $K_v \subset E \subset L$ be a tower of finite Galois extensions. Then*

$$\begin{aligned} \mathrm{Res}(u_{L/K_v}) &= u_{L/E} \\ \mathrm{Inf}(u_{E/K_v}) &= [L : E]u_{L/K_v}. \end{aligned}$$

$$\begin{array}{ccccc}
\mathrm{H}_T^2(\overline{K}_v/K_v) & \xrightarrow{\mathrm{Res}} & \mathrm{H}_T^2(\overline{K}_v/E) & \xrightarrow{\mathrm{Res}} & \mathrm{H}_T^2(\overline{K}_v/L) \\
\downarrow \mathrm{inv}_{K_v} & & \downarrow \mathrm{inv}_E & & \downarrow \mathrm{inv}_L \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{[E:K_v]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:E]} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

Proof. Consider the following diagram

Note that the vertical maps are all isomorphisms. Recall that the Kernel-Cokernel lemma says given homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ of abelian groups, one obtains an exact sequence

$$0 \longrightarrow \mathrm{Ker} f \longrightarrow \mathrm{Ker} g \circ f \longrightarrow \mathrm{Ker} g \longrightarrow \mathrm{Coker} f \longrightarrow \mathrm{Coker} g \circ f \longrightarrow \mathrm{Coker} g \longrightarrow 0.$$

We can apply this to the rows of the above diagram to obtain the following commutative diagram

$$\begin{array}{ccccc}
0 \longrightarrow & \mathrm{H}_T^2(E/K_v) & \xrightarrow{\mathrm{Inf}} & \mathrm{H}_T^2(L/K_v) & \xrightarrow{\mathrm{Res}} & \mathrm{H}_T^2(L/E) \\
& \downarrow \mathrm{inv}_{E/K_v} & & \downarrow \mathrm{inv}_{L/K_v} & & \downarrow \mathrm{inv}_{L/E} \\
0 \longrightarrow & \frac{1}{[E:K_v]} \mathbb{Z}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \frac{1}{[L:K_v]} \mathbb{Z}/\mathbb{Z} & \xrightarrow{[L:K_v]} & \frac{1}{[L:E]} \mathbb{Z}/\mathbb{Z}.
\end{array}$$

The fact that each square in the diagram is commutative gives the desired result. \square

Proposition 5.31. *Let $K_v \subset E \subset L$ be finite Galois extensions with $G = \mathrm{Gal}(L/K_v)$ and $H = \mathrm{Gal}(L/E)$. The following diagrams commute*

$$\begin{array}{ccc}
\mathrm{H}_T^r(G, \mathbb{Z}) \xrightarrow{u_{L/K_v}} \mathrm{H}_T^{r+2}(G, L^\times) & & \mathrm{H}_T^r(R, \mathbb{Z}) \xrightarrow{u_{L/K_v}} \mathrm{H}_T^{r+2}(G, L^\times) \\
\downarrow \mathrm{Res} & & \mathrm{Cor} \uparrow \\
\mathrm{H}_T^r(H, \mathbb{Z}) \xrightarrow{u_{L/E}} \mathrm{H}_T^{r+2}(H, L^\times) & & \mathrm{H}_T^r(H, \mathbb{Z}) \xrightarrow{u_{L/E}} \mathrm{H}_T^{r+2}(H, L^\times) \\
& & \mathrm{Cor} \uparrow
\end{array}$$

Proof. From the previous lemma we obtain the following identities, which give the result:

$$\begin{aligned}
\mathrm{Res}(u_{L/K_v}) \cup \mathrm{Res}(\alpha) &= \mathrm{Res}(u_{L/K_v} \cup \alpha) \\
&= u_{L/E} \cup \mathrm{Res}(\alpha)
\end{aligned}$$

and

$$\begin{aligned}\mathrm{Cor}(u_{L/E} \cup \beta) &= \mathrm{Cor}(\mathrm{Res}(u_{L/K_v}) \cup \beta) \\ &= u_{L/K_v} \cup \mathrm{Cor}(\beta).\end{aligned}$$

These are standard results on cup products and can be found in most any book on cohomology. \square

Exercise 5.32. Let $K_v \subset E \subset L$ be a tower of finite abelian extensions. Show that

$$\phi_{L/K_v}(x)|_E = \phi_{E/K_v}(x)$$

for all $x \in K_v$.

The previous exercise allows us to define a homomorphism $\phi_{K_v} : K_v^\times \rightarrow \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$ so that for any finite abelian extension L/K_v one has $\phi_{K_v}(x)|_L = \phi_{L/K_v}(x)$ for all $x \in K_v^\times$. Thus, in order to finish the proof of Theorem 5.1 it remains to investigate $\phi_{K_v}(\varpi_v)|_{K_v^{\mathrm{ur}}}$.

Let L/K_v be a finite unramified extension with Galois group G . Let ϖ_v be a uniformizer of K_v . The fact that L is unramified over K_v allows us to write any element $x \in L$ as $x = u\varpi_v^m$ for $u \in \mathcal{O}_L^\times$ and $m \in \mathbb{Z}$. As we have seen before, this gives an isomorphism

$$L^\times \cong \mathcal{O}_L^\times \times \mathbb{Z}.$$

Note that for any $\sigma \in G$, we have $\sigma(x) = \sigma(u)\varpi_v^m$ since ϖ_v is fixed by G . Thus, we have that the decomposition of L^\times into $\mathcal{O}_L^\times \times \mathbb{Z}$ is a decomposition as G -modules where the action of G on \mathbb{Z} is trivial. Thus, we have

$$\mathrm{H}_T^r(G, L^\times) = \mathrm{H}_T^r(G, \mathcal{O}_L^\times) \oplus \mathrm{H}_T^r(G, \mathbb{Z})$$

by Exercise 4.5. We have already seen that $\mathrm{H}_T^r(G, \mathcal{O}_L^\times) = 0$, so it remains to study $\mathrm{H}_T^r(G, \mathbb{Z})$.

First we determine a cocycle representing u_{L/K_v} . Let $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be the map that sends Frob_{L/K_v}^j to $\frac{j}{n}$ for all $j \in \mathbb{Z}$. The fact that Frob_{L/K_v} generates G gives that f is a generator of $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Recall we have an isomorphism

$$\delta : \mathrm{H}_T^1(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{H}_T^2(G, \mathbb{Z}).$$

Thus, to determine the generator u_{L/K_v} of $\mathrm{H}_T^2(G, L^\times) \cong \mathrm{H}_T^2(G, \mathbb{Z})$ it is enough to determine δf . In order to construct δf , we first choose a 1-cochain $\tilde{f} : G \rightarrow \mathbb{Q}/\mathbb{Z}$. We choose the cochain \tilde{f} to be the map given by $\mathrm{Frob}_{L/K_v}^j \mapsto \frac{j}{n}$ for $0 \leq j \leq n-1$. Using the formulas for the connecting homomorphism δ we obtain

$$\begin{aligned}\delta \tilde{f}(\mathrm{Frob}_{L/K_v}^i, \mathrm{Frob}_{L/K_v}^j) &= \mathrm{Frob}_{L/K_v}^i(\tilde{f}(\mathrm{Frob}_{L/K_v}^j)) - \tilde{f}(\mathrm{Frob}_{L/K_v}^{i+j}) + \tilde{f}(\mathrm{Frob}_{L/K_v}^i) \\ &= \begin{cases} 0 & \text{if } i+j \leq n-1 \\ 1 & \text{if } i+j > n-1. \end{cases}\end{aligned}$$

Recalling that we can identify \mathbb{Z} with $\varpi_v^{\mathbb{Z}} \subset L^\times$, we see that $u_{L/K_v} \in H_T^2(L/K_v)$ is represented by the cocycle ϕ given by

$$\phi(\text{Frob}_{L/K_v}^i, \text{Frob}_{L/K_v}^j) = \begin{cases} 1 & \text{if } i + j \leq n - 1 \\ \varpi_v & \text{if } i + j > n - 1. \end{cases}$$

Observe that since $H_T^0(G, \mathcal{O}_L^\times) = 0$, we have that $\mathcal{O}_{K_v}^\times \subset \text{Nm}(L^\times)$ and so the class of the uniformizer ϖ_v in $K_v^\times / \text{Nm}(L^\times)$ is well-defined.

Proposition 5.33. *Let L/K_v be a finite unramified extension and set $G = \text{Gal}(L/K_v)$. The element Frob_{L/K_v} is mapped to the class of ϖ_v under the map*

$$G \longrightarrow K_v^\times / \text{Nm}(L^\times),$$

i.e., $\phi_{L/K_v}(x) = \text{Frob}_{L/K_v}^{\text{ord}_{\varpi_v}(x)}$ for all $x \in K_v$.

Proof. Recall from the proof of Tate's theorem the splitting module $M(\phi)$ of a G -module M . This was defined as the direct sum $M \oplus Z$ where Z was the free abelian group having the symbols x_σ as a basis where $\sigma \in G, \sigma \neq 1$. The action of G on $M(\phi)$ was given by

$$\sigma(m, x_\tau) = (\sigma m + \phi(\sigma, \tau), x_{\sigma\tau} - x_\sigma).$$

We now consider the case where $M = L^\times$ and ϕ is the ϕ given above representing u_{L/K_v} . We had exact sequences

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow L^\times \longrightarrow L^\times(\phi) \longrightarrow I_G \longrightarrow 0.$$

The fact that $\mathbb{Z}[G]$ and $L^\times(\phi)$ both have trivial cohomology led us to the boundary maps

$$\begin{aligned} H_T^{-2}(G, \mathbb{Z}) &\longrightarrow H_T^{-1}(G, I_G) \\ H_T^{-1}(G, I_G) &\longrightarrow H_T^0(G, L^\times) \end{aligned}$$

both being isomorphisms. Recall that $H_T^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z})$ by definition. We saw before that $H_1(G, \mathbb{Z}) \cong G^{\text{ab}}$ via the fact that $H_1(G, \mathbb{Z}) \cong I_G / I_G^2$ and $I_G / I_G^2 \cong G^{\text{ab}}$. Thus, we have that Frob_{L/K_v} maps to $\text{Frob}_{L/K_v} - 1$ in $H_T^{-1}(G, I_G)$. It remains to determine the image of $\text{Frob}_{L/K_v} - 1$ under the boundary map $H_T^{-1}(G, I_G) \rightarrow H_T^0(G, L^\times)$.

The boundary map $H_T^{-1}(G, I_G) \rightarrow H_T^0(G, L^\times)$ is given by the Snake lemma from the diagram

For ease of notation we set $\sigma = \text{Frob}_{L/K_v}$. We need to follow the element $(\sigma - 1) + I_G^2$ through the diagram (recalling that $(I_G)_G = I_G / I_G^2$.) Recall that

Proof. We know that $\phi_{L/K_v}(u)$ is trivial when restricted to L_{ur} for any $u \in \mathcal{O}_v^\times$ by the previous theorem. Thus, we must have \mathcal{O}_v^\times maps into $\text{Gal}(L/L_{\text{ur}})$.

Conversely, let $\tau \in \text{Gal}(L/L_{\text{ur}})$ and write $f = [L_{\text{ur}} : K_v]$. There exists $x \in K_v^\times$ so that $\phi_{L/K_v}(x) = \tau$. The fact that $\tau \in \text{Gal}(L/L_{\text{ur}})$ means that $\tau|_{L_{\text{ur}}} = 1$. Using the previous theorem we know that $\tau|_{L_{\text{ur}}} = \text{Frob}_{L_{\text{ur}}/K_v}^{\text{ord}_{\varpi_v}(x)}$. Since the restriction is trivial, we must have $f \mid \text{ord}_{\varpi_v}(x)$. Using the fact that $\varpi_L^f = \varpi_v$, we see that there must be a $y \in L^\times$ so that $\text{Nm}(y) = x$. In particular, if we set $z = x \text{Nm}(y)^{-1}$ we have that $z \in \mathcal{O}_v^\times$ and $\phi_{L/K_v}(z) = \phi_{L/K_v}(x) = \tau$. Thus, we have the result. \square

5.4 Lubin-Tate formal group laws

In this section we will use formal group laws and Lubin-Tate theory to prove Theorem 5.2.

Let K_v be a nonarchimedean local field with $\text{char}(k_v) = p$. Set \mathcal{F}_{ϖ_v} to be the set of formal powers series $f \in \mathcal{O}_v[[x]]$ so that

1. $f(X) \equiv \varpi_v X \pmod{X^2}$;
2. $f(X) \equiv X^q \pmod{\varpi_v}$

where $q = \#k_{\varpi_v}$. For example, if we look at the case of $K_v = \mathbb{Q}_p$, then $f(X) = pX + \binom{p}{2}X^2 + \cdots + pX^{p-1} + X^p$ is an example of such a power series. We begin with the following very useful proposition.

Proposition 5.35. *Let $f, g \in \mathcal{F}_{\varpi_v}$, let $n \in \mathbb{Z}$, and let $\phi_1(X_1, \dots, X_n)$ be a linear form in X_1, \dots, X_n with coefficients in \mathcal{O}_v . Then there exists $\phi \in \mathcal{O}_v[[X_1, \dots, X_n]]$ so that*

1. $\phi \equiv \phi_1 \pmod{\text{deg } 2}$;
2. $f(\phi(X_1, \dots, X_n)) = \phi(g(X_1), \dots, g(X_n))$.

Proof. We construct such a ϕ by constructing a sequence $\{\phi_j\}$ with $\phi_j \in \mathcal{O}_v[[X_1, \dots, X_n]]$ of degree j with ϕ_j unique modulo degree $j+1$, $\phi_j \equiv \phi_1 \pmod{\text{deg } 2}$, and $f(\phi(X_1, \dots, X_n)) \equiv \phi(g(X_1), \dots, g(X_n)) \pmod{\text{deg } j+1}$. We then set $\phi = \lim \phi_j$. As our first step we take ϕ_1 , which satisfies the conditions by assumption. Now suppose we have constructed ϕ_j for some positive integer j . Observe that since ϕ_j is unique modulo degree $j+1$, we must have $\phi_i \equiv \phi_j \pmod{\text{deg } j+1}$ for all $i \geq j$. This shows that $\phi_{j+1} - \phi_j$ contains only terms of degree equal to $j+1$.

By assumption we have

$$f(\phi_j(X_1, \dots, X_n)) \equiv \phi_j(g(X_1), \dots, g(X_n)) \pmod{\text{deg } j+1}.$$

Let

$$E_{j+1} = f(\phi_j(X_1, \dots, X_n)) - \phi_j(g(X_1), \dots, g(X_n)) \pmod{\text{deg } j+2}$$

Set

$$\phi_{j+1} = \phi_j - \frac{E_{j+1}}{\varpi_v(1 - \varpi_v^j)}.$$

Our first step is to show that $\phi_{j+1} \in \mathcal{O}_v[[X_1, \dots, X_n]]$. To see this, it is enough to show that $\varpi_v \mid E_{j+1}$. Recall that for any $\psi \in \mathbb{F}_q[[X_1, \dots, X_n]]$ one has $\psi(X_1^q, \dots, X_n^q) = \psi(X_1, \dots, X_n)^q$. We combine this with the fact that since $f, g \in \mathcal{F}_{\varpi_v}$ we have $f(X) \equiv g(X) \equiv X^q \pmod{\varpi_v}$ to obtain

$$\begin{aligned} f(\phi_j(X_1, \dots, X_n)) - \phi_j(g(X_1), \dots, g(X_n)) &\equiv \phi_j(X_1, \dots, X_n)^q - \phi_j(X_1^q, \dots, X_n^q) \pmod{\varpi_v} \\ &\equiv 0 \pmod{\varpi_v}. \end{aligned}$$

Thus, $\varpi_v \mid E_{j+1}$ as claimed.

Since we have that $\phi_j \equiv \phi_1 \pmod{\deg 2}$ and E_{j+1} has pure degree $j+1$, we see that

$$\phi_{j+1} \equiv \phi_j \equiv \phi_1 \pmod{\deg 2}.$$

Observe that we have

$$(5.2) \quad f(\phi_{j+1}) - \phi_{j+1}(g) \equiv f(\phi_{j+1}) - \phi_j(g) + \frac{E_{j+1}(g)}{\varpi_v(1 - \varpi_v^j)} \pmod{\deg j + 2}$$

where we drop the X_i 's from the notation and write $\phi_j(g)$ to mean $\phi_j(g(X_1), \dots, g(X_n))$ and similarly for $E_{j+1}(g)$. We can now compute the Taylor expansions of these terms. For instance, we know that $f(X) = \varpi_v X + (\deg \geq 2)$ and similarly for $g(X)$. Thus we can write

$$\begin{aligned} f(\phi_{j+1}) &= f(\phi_j) + f'(\phi_j)(\phi_{j+1} - \phi_j) + \frac{f''(\phi_j)}{2!}(\phi_{j+1} - \phi_j)^2 + \dots \\ &= f(\phi_j) + \varpi_v \left(\frac{-E_{j+1}}{\varpi_v(1 - \varpi_v^j)} \right) + \dots \\ &\equiv f(\phi_j) - \varpi_v \left(\frac{E_{j+1}}{\varpi_v(1 - \varpi_v^j)} \right) \pmod{\deg j + 2} \end{aligned}$$

where we have used that the terms of higher degree vanish modulo degree $j+2$ since E_{j+1} must only contain terms of degree equal to $j+1$. Similarly, if we consider $E_{j+1}(g(X_1), \dots, g(X_n))$ we see that modulo degree $j+2$, we have

$$\begin{aligned} E_{j+1}(g(X_1), \dots, g(X_n)) &\equiv E_{j+1}(\varpi_v X_1, \dots, \varpi_v X_n) \pmod{\deg j + 2} \\ &\equiv \varpi_v^{j+1} E_{j+1}(X_1, \dots, X_n) \pmod{\deg j + 2}. \end{aligned}$$

Plugging this information into equation (5.2) we obtain

$$\begin{aligned} f(\phi_{j+1}) - \phi_{j+1}(g) &\equiv f(\phi_j) - \varpi_v \left(\frac{E_{j+1}}{\varpi_v(1 - \varpi_v^j)} \right) - \phi_j(g) + \varpi_v^{j+1} \left(\frac{E_{j+1}}{\varpi_v(1 - \varpi_v^j)} \right) \pmod{\deg j + 2} \\ &\equiv E_{j+1} - E_{j+1} \pmod{\deg j + 2} \\ &\equiv 0 \pmod{\deg j + 2}. \end{aligned}$$

It only remains to check the uniqueness of ϕ_{j+1} . Write $\phi_{j+1} = \phi_j + \phi^{j+1}$ and suppose

$$f(\phi_{j+1}) - \phi_{j+1}(g) \equiv 0 \pmod{\deg j + 2}.$$

We show that $\phi^{j+1} = -\frac{E_{j+1}}{\varpi_v(1-\varpi_v^j)}$. As above, we use Taylor expansions along with the fact that ϕ^{j+1} has pure degree $j + 1$. We have

$$f(\phi_{j+1}) \equiv f(\phi_j) + \varpi_v \phi^{j+1} \pmod{\deg j + 2}$$

and

$$\phi_{j+1}(g(X_1), \dots, g(X_n)) \equiv \varpi_v^{j+1} \phi^{j+1}(X_1, \dots, X_n) \pmod{\deg j + 2}.$$

Plugging this into the equation $f(\phi_{j+1}) - \phi_{j+1}(g) \equiv 0 \pmod{\deg j + 2}$ and solving for ϕ^{j+1} gives the result. Thus, by induction we are done. \square

Definition 5.36. Let R be a commutative ring with identity and let $F \in R[[X, Y]]$. We say F is a *commutative formal group law* if:

1. $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
2. $F(0, Y) = Y$ and $F(X, 0) = X$;
3. there exists a unique $G(X)$ so that $F(X, G(X)) = 0$;
4. $F(X, Y) = F(Y, X)$;
5. $F(X, Y) = X + Y \pmod{\deg 2}$.

Exercise 5.37. Show that the conditions $F(0, Y) = Y$ and $F(X, 0) = X$ follow from the other conditions given in the definition.

Let $R = \mathcal{O}_v$ and let $F(X, Y)$ be a commutative formal group law defined over \mathcal{O}_v . Let $x, y \in \mathfrak{m}_v$. Then one has that $F(x, y)$ converges to something in \mathfrak{m}_v . Under this composition \mathfrak{m}_v becomes a group and we write $F(\mathfrak{m}_v)$ to denote this group. For example, if we set $F(X, Y) = X + Y$ then $F(\mathfrak{m}_v)$ is \mathfrak{m}_v with the usual addition. If we set $F(X, Y) = X + Y + XY$, then we obtain the multiplicative group structure on $1 + \mathfrak{m}_v$.

Definition 5.38. Let $F(X, Y)$ and $G(X, Y)$ be formal group laws. A *homomorphism* $F \rightarrow G$ is a power series $h \in TR[[T]]$ such that

$$h(F(X, Y)) = G(h(X), h(Y)).$$

When there exists $h' : G \rightarrow F$ such that $h \circ h' = T = h' \circ h$ we say h is an isomorphism.

Example 5.39. The map $a \mapsto 1 + a$ from \mathfrak{m}_v to $1 + \mathfrak{m}_v$ gives an isomorphism between the additive group $(\mathfrak{m}_v, +)$ and the multiplicative group $(1 + \mathfrak{m}_v, \cdot)$.

Proposition 5.40. *Let $f \in \mathcal{F}_{\varpi_v}$. There exists a commutative formal group F_f with coefficients in \mathcal{O}_v so that*

$$f(F_f(X, Y)) = F_f(f(X), f(Y)),$$

i.e., f is an endomorphism of the formal group.

Proof. Let F_f be the unique solution to $F_f(X, Y) \equiv X + Y \pmod{\deg 2}$ and $f(F_f(X, Y)) = F_f(f(X), f(Y))$ given by Proposition 5.35. One just needs to check that F_f is indeed a commutative formal group law. This amounts to checking each part of the definition, which can be done using the uniqueness in Proposition 5.35. For instance, to show that $F_f(0, Y) = Y$, we first observe that $F_f(0, Y)$ and Y are both solutions to

$$H(X, Y) \equiv Y \pmod{\deg 2}.$$

We also have that $Y(f(X), f(Y)) = f(Y)$ and $F_f(0, f(Y)) = f(F_f(0, Y))$ and so the uniqueness in Proposition 5.35 gives that $F_f(0, Y) = Y$. As another example, one sees that $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$ by observing that each side is a solution to

$$H(X, Y, Z) = X + Y + Z \pmod{\deg 2}$$

and

$$H(f(X), f(Y), f(Z)) = f(H(X, Y, Z)).$$

We leave the rest of the conditions to the following exercise. \square

Exercise 5.41. *Finish checking the rest of the conditions in the previous proof to show that F_f is a commutative formal group law.*

Proposition 5.42. *Let $f \in \mathcal{F}_{\varpi_v}$ and F_f the commutative formal group law given in Proposition 5.40. Then for every $\alpha \in \mathcal{O}_v$ there exists $[\alpha]_f \in \mathcal{O}_v[[X]]$ such that*

1. $[\alpha]_f$ commutes with f ;
2. $[\alpha]_f \equiv \alpha X \pmod{\deg 2}$.

Moreover, $[\alpha]_f$ is an endomorphism of the group law F_f .

Proof. For every $\alpha \in \mathcal{O}_v$ and every $f, g \in \mathcal{F}_{\varpi_v}$, let $[\alpha]_{f,g}(T)$ be the unique solution to

$$[\alpha]_{f,g}(T) \equiv \alpha T \pmod{\deg 2}$$

and

$$f([\alpha]_{f,g}(T)) = [\alpha]_{f,g}(g(T))$$

whose existence is guaranteed by Proposition 5.35. We see that

$$\begin{aligned} F_f([\alpha]_{f,g}(X), [\alpha]_{f,g}(Y)) &\equiv [\alpha]_{f,g}(X) + [\alpha]_{f,g}(Y) \pmod{\deg 2} \\ &\equiv \alpha X + \alpha Y \pmod{\deg 2} \end{aligned}$$

and

$$\begin{aligned} [\alpha]_{f,g}(F_g(X, Y)) &\equiv \alpha F_g(X, Y) \pmod{\deg 2} \\ &\equiv \alpha X + \alpha Y \pmod{\deg 2}. \end{aligned}$$

Thus, each of $F_f([\alpha]_{f,g}(X), [\alpha]_{f,g}(Y))$ and $[\alpha]_{f,g}(F_g(X, Y))$ is a solution of

$$H(X, Y) \equiv \alpha X + \alpha Y \pmod{\deg 2}.$$

We now observe that

$$\begin{aligned} [\alpha]_{f,g}(F_f(f(X), f(Y))) &= ([\alpha]_{f,g} \circ f)(F_f(X, Y)) \\ &= g([\alpha]_{f,g}(F_f(X, Y))) \end{aligned}$$

and

$$\begin{aligned} F_g([\alpha]_{f,g}(f(X)), [\alpha]_{f,g}(f(Y))) &= F_g(g([\alpha]_{f,g}(X)), g([\alpha]_{f,g}(Y))) \\ &= g(F_g([\alpha]_{f,g}(X), [\alpha]_{f,g}(Y))) \end{aligned}$$

and so we can apply Proposition 5.35 to conclude that

$$F_f([\alpha]_{f,g}(X), [\alpha]_{f,g}(Y)) = [\alpha]_{f,g}(F_g(X, Y)).$$

Substituting $f = g$, we achieve the desired result. \square

Proposition 5.43. *The map $\alpha \mapsto [\alpha]_f := [\alpha]_{f,f}$ is an injective homomorphism of \mathcal{O}_v to $\text{End}(F_f)$.*

Exercise 5.44. *Prove Proposition 5.43.*

Proposition 5.45. *Let $f, g \in \mathcal{F}_{\varpi_v}$. Then $F_f \cong F_g$.*

Proof. Let $\alpha \in \mathcal{O}_v^\times$. Then $[\alpha]_{f,g}$ is invertible and provides the desired isomorphism. \square

Note that Proposition 5.45 shows that we can choose any $f \in \mathcal{F}_{\varpi_v}$ when defining the formal group F_f . This allows us to pick convenient f 's depending on the situation of interest. It is also important to note that $[\varpi_v]_f = f$. This follows from the uniqueness of $[\varpi_v]_f$ and the fact that f satisfies both conditions defining $[\varpi_v]_f$.

5.5 Norm subgroups

We now have enough background to prove Theorem 5.2 and thus finish the proofs of the main results of local class field theory. Let K_v be a nonarchimedean local field and \overline{K}_v an algebraic closure. Given any $f \in \mathcal{F}_{\varpi_v}$, we write F_f to denote the corresponding formal group law as given in Proposition 5.40. We write M_f for the group of points in $\mathfrak{m}_{\overline{K}_v}$ equipped with the group law defined by F_f , i.e.,

$M_f = F_f(\mathfrak{m}_{\overline{K}_v})$. For any $\alpha \in \mathcal{O}_v$, we saw in Proposition 5.43 that the map $\alpha \mapsto [\alpha]_f$ gives an \mathcal{O}_v -module structure on M_f . Set E_f^n to be the kernel of the map $[\varpi_v^n]_f$ and $E_f = \bigcup_{n \geq 1} E_f^n$. It is clear that this is precisely the torsion submodule of M_f . Define $K_{v, \varpi_v}^n = K_v(E_f^n)$ and set $K_{v, \varpi_v} = \bigcup_{n \geq 1} K_{v, \varpi_v}^n$. Let $G_{\varpi_v, n} = \text{Gal}(K_{v, \varpi_v}^n / K_v)$. Then we have $\text{Gal}(K_{v, \varpi_v} / K_v) = \varprojlim G_{\varpi_v, n}$.

Proposition 5.46. *The \mathcal{O}_v -module E_f is isomorphic to the divisible module K_v / \mathcal{O}_v .*

Proof. Recall that Proposition 5.45 showed that we can choose $f \in \mathcal{F}_{\varpi_v}$ as we please because the resulting group structures are isomorphic for different choices of f . As such, we choose $f(X) = \varpi_v X + X^q$ where $q = \#k_v$. Let $x \in \mathfrak{m}_{\overline{K}_v}$. We have that $f(X) - x = 0$ has a solution in \overline{K}_v and in fact the solution belongs to $\mathfrak{m}_{\overline{K}_v}$. (One can see that the solution belongs to $\mathfrak{m}_{\overline{K}_v}$ by looking at the Newton polygon for instance. See [Mi98], Chapter 7 for a discussion of Newton polygons.) Using the fact that $[\varpi_v]_f = f$, we see that this gives the map $[\varpi_v]_f$ is a surjective map. This implies that M_f is in fact a divisible module and so a direct sum of copies of K_v / \mathcal{O}_v .

Observe now that since E_f^1 is the set of elements killed by $[\varpi_v]_f$ and $[\varpi_v]_f(T) = f(T)$, E_f^1 is actually the roots of $f(T)$. Again we can use Newton polygons to show the roots of $f(T)$ must lie in $\mathfrak{m}_{\overline{K}_v}$ and so E_f^1 has precisely q elements. This gives that it is isomorphic to $\mathcal{O}_v / (\varpi_v)$ since it is an \mathcal{O}_v -module with q elements. One now uses the fact that $[\varpi_v]_f$ is surjective to deduce that the sequence

$$0 \longrightarrow E_f^1 \longrightarrow E_f^n \xrightarrow{[\varpi_v]_f} E_f^{n-1} \longrightarrow 0$$

is exact. From this it follows that E_f^n is cyclic of order q^n , and so is isomorphic to $\mathcal{O}_v / (\varpi_v^n)$. From this the result follows. \square

Corollary 5.47. *One has $\text{End}_{\mathcal{O}_v}(E_f^n) \cong \mathcal{O}_v / (\varpi_v^n)$ and $\text{Aut}_{\mathcal{O}_v}(E_f^n) \cong (\mathcal{O}_v / (\varpi_v^n))^\times$.*

Proof. This follows immediately from the previous proof using that $E_f^n \cong \mathcal{O}_v / (\varpi_v^n)$ and the fact that the action of \mathcal{O}_v on E_f^n induces an isomorphism $\mathcal{O}_v / (\varpi_v^n) \longrightarrow \text{End}_{\mathcal{O}_v}(E_f^n)$. \square

Exercise 5.48. *Let L/K_v be a finite Galois extension. For any $f \in \mathcal{O}_v[[X]]$ and $x \in \mathfrak{m}_L$, one has*

$$f(\sigma x) = \sigma f(x)$$

for all $\sigma \in \text{Gal}(L/K_v)$.

Theorem 5.49. *1. For each $n \geq 1$, $K_{v, \varpi_v}^n / K_v$ is totally ramified of degree $(q-1)q^{n-1}$.*

2. The action of \mathcal{O}_v on E_f^n defines an isomorphism

$$(\mathcal{O}_v / (\varpi_v^n))^\times \longrightarrow \text{Gal}(K_{v, \varpi_v}^n / K_v).$$

3. For each $n \geq 1$, ϖ_v is a norm from K_{v,ϖ_v} .

Proof. Let x_1 be a root of $f(T)$. Define x_n inductively by choosing x_n to be a root of $f(T) - x_{n-1}$. We obtain a tower of Eisenstein extensions:

$$K_v \subset K_v[x_1] \subset K_v[x_2] \subset \cdots \subset K_v[x_n] \subset K_{v,\varpi_v}^n$$

where $[K_v[x_1] : K_v] = q - 1$ and $[K_v[x_n] : K_v[x_{n-1}]] = q$ for all $n \geq 2$. This shows that $K_v[x_n]$ is totally ramified over K_v of degree $(q - 1)q^{n-1}$.

We know that E_f^n is set of elements killed by $[\varpi_v^n]_f$, i.e., the set of roots of $f \circ \cdots \circ f = f^{(n)}$. This shows that K_{v,ϖ_v}^n is precisely the splitting field of $f^{(n)}$ and so we can view $\text{Gal}(K_{v,\varpi_v}^n/K_v)$ as a subgroup of the set of permutations of E_f^n . However, the previous exercise shows that each element of the Galois group acts on E_f^n as a \mathcal{O}_v -module isomorphism. Thus, the image of $\text{Gal}(K_{v,\varpi_v}^n/K_v)$ in $\text{Sym}(E_f^n)$ is contained in $\text{Aut}_{\mathcal{O}_v}(E_f^n) \cong (\mathcal{O}_v/(\varpi_v^n))^\times$. Thus we have

$$(q - 1)q^{n-1} \leq [K_v[x_n] : K_v] \leq [K_{v,\varpi_v}^n : K_v] = \# \text{Gal}(K_{v,\varpi_v}^n/K_v) \leq (q - 1)q^{n-1}.$$

This gives the first two claims of the theorem.

Define $g(T) = \varpi_v + T^{q-1}$ and set $h_n(T) = g \circ f \circ \cdots \circ f$ where there are n total terms. One can check that $h_n(x_n) = h_{n-1}(x_{n-1}) = \cdots = f(x_1) = 0$. For instance, $h_2(T) = \varpi_v + (\varpi_v T + t^q)^{q-1}$ and so

$$\begin{aligned} h_2(x_2) &= \varpi_v + (\varpi_v x_2 + x_2^q)^{q-1} \\ &= \varpi_v + x_1^{q-1} \\ &= 0. \end{aligned}$$

We have that $h_n(T)$ is monic of degree $(q - 1)q^{n-1}$ and so must be the minimal polynomial of x_n over K_v . Thus,

$$\begin{aligned} \text{Nm}_{K_{v,\varpi_v}^n/K_v} x_n &= (-1)^{(q-1)q^{n-1}} \varpi_v \\ &= \varpi_v \end{aligned}$$

unless $q = 2$ and $n = 1$, in which case $K_{v,\varpi_v}^2 = K_v$ and the result is clear. Thus, we have that ϖ_v is a norm from K_{v,ϖ_v}^n for each $n \geq 1$. \square

Observe that we have constructed a tower of fields

$$K_v \subset K_{v,\varpi_v}^1 = K_v[x_1] \subset K_{v,\varpi_v}^2 = K_v[x_2] \subset \cdots \subset K_{v,\varpi_v}^n = K_v[x_n] \subset \cdots \subset K_{v,\varpi_v} = \bigcup K_{v,\varpi_v}^n$$

with each K_{v,ϖ_v}^n totally ramified over K_v , $[K_{v,\varpi_v}^1 : K_v] = q - 1$, $[K_{v,\varpi_v}^n : K_{v,\varpi_v}^{n-1}] = q$ for all $n \geq 2$, $f(x_n) = x_{n-1}$, and $\mathfrak{m}_{K_{v,\varpi_v}^n} = (x_n)$. We have that the action of \mathcal{O}_v on E_f^n induces an isomorphism

$$(\mathcal{O}_v/(\varpi_v^n))^\times \longrightarrow \text{Gal}(K_{v,\varpi_v}^n/K_v).$$

We can take the inverse limit of this isomorphism to obtain an isomorphism

$$\mathcal{O}_v^\times \xrightarrow{\cong} \text{Gal}(K_{v,\varpi_v}/K_v).$$

The fact that K_{v,ϖ_v} is the union of totally ramified extension of K_v and K_v^{ur} is the union of unramified extensions of K_v gives that $K_{v,\varpi_v} \cap K_v^{\text{ur}} = K_v$. We define a homomorphism

$$\phi_{\varpi_v} : K_v^\times \longrightarrow \text{Gal}(K_{v,\varpi_v} K_v^{\text{ur}}/K_v)$$

by defining $\phi_{\varpi_v}(a)|_{K_{v,\varpi_v}}$ and $\phi_{\varpi_v}|_{K_v^{\text{ur}}}$ for each $a \in K_v^\times$. Eventually we will show that $K_{v,\varpi_v} K_v^{\text{ur}} = K_v^{\text{ab}}$ and $\phi_{\varpi_v} = \phi_{K_v}$. Let $a = u\varpi_v^m \in K_v^\times$. Set $\phi_{\varpi_v}|_{K_v^{\text{ur}}} = \text{Frob}_{K_v}^m$ and $\phi_{\varpi_v}|_{K_{v,\varpi_v}} = [u^{-1}]_f$. We use u^{-1} instead of u so that $K_{v,\varpi_v} K_v^{\text{ur}}$ and ϕ_{ϖ_v} are both independent of the choice of uniformizer ϖ_v . Before we can prove that fact we need some more work with formal groups.

Recall that even though K_v is complete and L/K_v is complete for any finite extension, the field K_v^{ur} is not complete. We write $\widehat{K_v^{\text{ur}}}$ for the completion of K_v^{ur} with respect to the unique extension of the valuation of K_v to K_v^{ur} .

Lemma 5.50. *The homomorphisms*

$$x \mapsto \text{Frob}_{K_v}(x) - x : \mathcal{O}_{\widehat{K_v^{\text{ur}}}} \longrightarrow \mathcal{O}_{\widehat{K_v^{\text{ur}}}}$$

and

$$x \mapsto \text{Frob}_{K_v}(x)/x : \mathcal{O}_{\widehat{K_v^{\text{ur}}}}^\times \longrightarrow \mathcal{O}_{\widehat{K_v^{\text{ur}}}}^\times$$

are surjective with kernels \mathcal{O}_v and \mathcal{O}_v^\times respectively.

Proof. We prove the result for the first homomorphism as the argument for the second is analogous. We begin by using induction to show that the sequence

$$0 \longrightarrow \mathcal{O}_v/\mathfrak{m}_v^n \longrightarrow \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^n \xrightarrow{\text{Frob}_{K_v} - 1} \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^n \longrightarrow 0$$

is exact. The $n = 1$ case claims that the sequence

$$0 \longrightarrow k_v \longrightarrow \bar{k}_v \xrightarrow{x \mapsto x^q - x} \bar{k}_v \longrightarrow 0$$

is exact. However, this is clear as \bar{k}_v is the algebraic closure of k_v . Now assume that we have exactness for $n - 1$. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}} & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^n & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^{n-1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}} & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^n & \longrightarrow & \mathcal{O}_{K_v^{\text{ur}}}/\mathfrak{m}_{K_v^{\text{ur}}}^{n-1} \longrightarrow 0 \end{array}$$

where all the of vertical arrows arise from the map $\text{Frob}_{K_v} - 1$. We apply the Snake Lemma to study this diagram. Using our induction hypothesis for

$n - 1$ and the case $n = 1$, we have that the map $\text{Frob}_{K_v} - 1 : \mathcal{O}_{K_v^{\text{ur}}} / \mathfrak{m}_{K_v^{\text{ur}}}^n \rightarrow \mathcal{O}_{K_v^{\text{ur}}} / \mathfrak{m}_{K_v^{\text{ur}}}^n$ is surjective. Moreover, we have that the kernel of this map has order q^n . Since $\mathcal{O}_v / \mathfrak{m}_v^n$ is contained in the kernel and has q^n elements, we must have that this is precisely the kernel and so we get the exactness.

To finish the proof we observe the following. The valuation ring $\mathcal{O}_{K_v^{\text{ur}}}$ is a discrete valuation ring with maximal ideal $\mathfrak{m}_{K_v^{\text{ur}}}$. In particular, this gives that

$$\varprojlim \mathcal{O}_{K_v^{\text{ur}}} / \mathfrak{m}_{K_v^{\text{ur}}}^n \cong \widehat{\mathcal{O}_{K_v^{\text{ur}}}}.$$

Now we just take the inverse limits of the exact sequence to get the result. \square

Given a power series f in one variable, we write f^{-1} for the inverse with respect to composition, i.e., the power series such that $f \circ f^{-1} = T = f^{-1} \circ f$.

Proposition 5.51. *Let ϖ_v and π be two different uniformizers of K_v and F_f and F_g the formal group laws defined by $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_{\varpi_v}$. If we write $\varpi_v = u\pi$, then there exists $\epsilon \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}^\times$ such that $\text{Frob}_{K_v}(\epsilon) = \epsilon u$ and a power series $h(T) \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}[[T]]$ so that*

1. $h(T) \equiv \epsilon T \pmod{\deg 2}$;
2. $\text{Frob}_{K_v} h = h \circ [u]_f$;
3. $h(F_f(X, Y)) = F_g(h(X), h(Y))$;
4. $h \circ [a]_f = [a]_g \circ h$ for every $a \in \mathcal{O}_v$.

In other words, h is an isomorphism between F_f and F_g over $\widehat{\mathcal{O}_{K_v^{\text{ur}}}}$ that commutes with the action of \mathcal{O}_v .

Proof. We begin by showing there is an $h \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}[[T]]$ that satisfies the first two conditions above. We construct h inductively. Let $\epsilon \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}^\times$ so that $\text{Frob}_{K_v}(\epsilon) = \epsilon u$. Such an element exists by Lemma 5.50. Set $h_1(T) = \epsilon T$. We now construct $h_r(T)$ a polynomial of degree r so that

$$\begin{aligned} h_r(T) &= h_{r-1}(T) + xT^r \\ \text{Frob}_{K_v}(h_r) &\equiv h_r \circ [u]_f \pmod{\deg r + 1} \end{aligned}$$

for some $x \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}$. As $h_1(T) = \epsilon T$, both of the conditions are clear for $h_1(T)$. Now suppose that we have constructed $h_r(T)$ satisfying the conditions. Let $a \in \widehat{\mathcal{O}_{K_v^{\text{ur}}}}$ be such that $\text{Frob}_{K_v}(a) - a = c(\epsilon u)^{-r-1}$ where c is the coefficient of T^{r+1} in $h_r \circ [u]_f - \text{Frob}_{K_v}(h_r)$. Such an element can be found by Lemma 5.50. We claim that $h_{r+1}(T) = h_r(T) + bT^{r+1}$ satisfies the conditions where $b = a\epsilon^{r+1}$. The first condition is automatic, so it only remains to check the

second condition. However, for this we check

$$\begin{aligned}
\text{Frob}_{K_v}(h_{r+1}(T)) &= \text{Frob}_{K_v}(h_r(T)) + \text{Frob}_{K_v}(a\epsilon^{r+1}T^{r+1}) \\
&= \text{Frob}_{K_v}(h_r(T)) + \text{Frob}_{K_v}(a)\text{Frob}_{K_v}(\epsilon T)^{r+1} \\
&\equiv \text{Frob}_{K_v}(h_r(T)) + \left(a + \frac{c}{(\epsilon u)^{r+1}}\right) (\text{Frob}_{K_v}(\epsilon))^{r+1}T^{r+1} \pmod{\deg r + 2} \\
&\equiv \text{Frob}_{K_v}(h_r(T)) + a\text{Frob}_{K_v}(\epsilon)^{r+1}T^{r+1} + cT^{r+1} \pmod{\deg r + 2} \\
&\equiv h_r \circ [u]_f(T) - cT^{r+1} + a\text{Frob}_{K_v}(\epsilon)^{r+1}T^{r+1} + cT^{r+1} \pmod{\deg r + 2} \\
&\equiv h_r \circ [u]_f(T) + a\text{Frob}_{K_v}(\epsilon)^{r+1}T^{r+1} \pmod{\deg r + 2} \\
&\equiv h_r \circ [u]_f(T) + a(\epsilon u)^{r+1}T^{r+1} \pmod{\deg r + 2} \\
&\equiv h_r \circ [u]_f(T) + a\epsilon^{r+1}T^{r+1} \circ [u]_f(T) \pmod{\deg r + 2} \\
&\equiv h_r \circ [u]_f(T) + bT^{r+1} \circ [u]_f \pmod{\deg r + 2} \\
&\equiv h_{r+1} \circ [u]_f.
\end{aligned}$$

Thus, taking the limit of these h_r we have the h we desire.

We now show that we can take h so that $g = \text{Frob}_{K_v} h \circ f \circ h^{-1}$. Set $j = \text{Frob}_{K_v} h \circ f \circ h^{-1}$. Observe that we have

$$\begin{aligned}
j &= h \circ [u]_f \circ f \circ h^{-1} \\
&= h \circ f \circ [u]_f \circ h^{-1}.
\end{aligned}$$

The fact that $h \circ [u]_f = \text{Frob}_{K_v} h$ gives $h \circ [u]_f \circ (\text{Frob}_{K_v} h)^{-1} = T$. Thus, we have

$$[u]_f \circ (\text{Frob}_{K_v} h)^{-1} = h^{-1}.$$

We combine this with the fact that f and $[u]_f$ both have coefficients in \mathcal{O}_v to conclude

$$\begin{aligned}
\text{Frob}_{K_v} j &= \text{Frob}_{K_v} h \circ f \circ [u]_f \circ \text{Frob}_{K_v} h^{-1} \\
&= \text{Frob}_{K_v} h \circ f \circ h^{-1} \\
&= j.
\end{aligned}$$

Thus, we must have $j \in \mathcal{O}_v[[T]]$ since it is fixed by Frob_{K_v} . We have that

$$\begin{aligned}
j(T) &\equiv \text{Frob}_{K_v} \epsilon \pi \epsilon^{-1} T \pmod{T^2} \\
&\equiv \epsilon u \pi \epsilon^{-1} T \pmod{T^2} \\
&\equiv \epsilon \varpi_v \epsilon^{-1} T \pmod{T^2} \\
&\equiv \varpi_v T \pmod{T^2}.
\end{aligned}$$

We also calculate

$$\begin{aligned}
j(T) &\equiv \text{Frob}_{K_v} h \circ (h^{-1})^q \pmod{\mathfrak{m}_v} \\
&\equiv \text{Frob}_{K_v} h(\text{Frob} h^{-1}(T^q)) \pmod{\mathfrak{m}_v} \\
&\equiv T^q \pmod{\mathfrak{m}_v}.
\end{aligned}$$

Thus, we have $j \in \mathcal{F}_{\varpi_v}$. Now set $j' = [1]_{g,j} \circ h$. Now j' still satisfies the first two conditions and

$$\begin{aligned} \text{Frob}_{K_v} j' \circ f \circ (j')^{-1} &= [1]_{g,j} \circ j \circ [1]_{g,j}^{-1} \\ &= g. \end{aligned}$$

The last two claims now are just applications of Proposition 5.35, which we leave as an exercise. \square

Lemma 5.52. *Let L/K_v be an algebraic extension and let $x \in \widehat{L}$. If x is separable and algebraic over L , then $x \in L$.*

Proof. Let $L' = \widehat{L} \cap \overline{K}_v$. Let $\sigma \in \text{Gal}(\overline{K}_v/L)$. We know that σ is continuous and it is the identity on L . For any $x \in L'$, we have that x is the limit of elements in x and so σ is necessarily trivial on x as well. Thus we have $\text{Gal}(\overline{K}_v/L) = \text{Gal}(\overline{K}_v/L')$. Galois theory now gives that $L' = L$ as desired. \square

Theorem 5.53. *The field $K_{v,\varpi_v} K_v^{\text{ur}}$ is independent of the choice of ϖ_v , as is the map ϕ_{ϖ_v} .*

Proof. Let ϖ_v and $\varpi'_v = u\varpi_v$ be two different uniformizers of K_v . Let $f \in \mathcal{F}_{\varpi_v}$ and $g \in \mathcal{F}_{\varpi'_v}$ and define h as in Proposition 5.51. Then we have

$$\begin{aligned} \text{Frob}_{K_v} \circ h \circ [\varpi_v]_f &= (h \circ [u]_f) \circ [\varpi_v]_f \\ &= h \circ [\varpi'_v]_f \\ &= [\varpi'_v]_g \circ h, \end{aligned}$$

i.e., we have $\text{Frob}_{K_v} h(f(T)) = g(h(T))$. Thus, if $f(\alpha) = 0$, then $g(h(\alpha)) = 0$ as well. If $g(\beta) = 0$, then $f(h^{-1}(\beta)) = 0$. Thus, h defines a bijection between E_f^1 and E_g^1 . Thus we have

$$\begin{aligned} \widehat{K}_v^{\text{ur}}[E_g^1] &= \widehat{K}_v^{\text{ur}}[h(E_f^1)] \\ &\subseteq \widehat{K}_v^{\text{ur}}[E_f^1] \\ &= \widehat{K}_v^{\text{ur}}[h^{-1}(E_g^1)] \\ &\subseteq \widehat{K}_v^{\text{ur}}[E_g^1]. \end{aligned}$$

Thus, we have $\widehat{K}_v^{\text{ur}}[E_g^1] = \widehat{K}_v^{\text{ur}}[E_f^1]$. We combine this fact with Lemma 5.52 to conclude that $K_v^{\text{ur}}[E_g^1] = K_v^{\text{ur}}[E_f^1]$. A similar argument gives $K_v^{\text{ur}}[E_g^n] = K_v^{\text{ur}}[E_f^n]$ for all $n \geq 1$ and so $K_{v,\varpi_v} K_v^{\text{ur}} = K_{v,\varpi'_v} K_v^{\text{ur}}$ as claimed.

We now need to show that ϕ_{ϖ_v} does not depend on the choice of ϖ_v . Observe that on K_v^{ur} , $\phi_{\varpi_v}(\varpi_v)$ and $\phi_{\varpi'_v}(\varpi_v)$ both give Frob_{K_v} . Thus, they agree on K_v^{ur} . Again, let h be as in Proposition 5.51. By definition we have that $\phi_{\varpi_v}(\varpi_v)$ is the identity map on K_{v,ϖ_v} . We wish to show that $\phi_{\varpi'_v}(\varpi_v)$ is also the identity map on K_{v,ϖ_v} . To show this, first observe that K_{v,ϖ_v}^n is generated over K_v by the elements $h(x)$ for $x \in E_f^n$ since h gives a bijection between E_f^n and E_g^n .

Thus, to show that $\phi_{\varpi'_v}(\varpi_v)$ is the identity on K_{v,ϖ_v} , it is enough to show that for all $n \geq 1$ and all $x \in E_f^n$ we have

$$\phi_{\varpi'_v}(\varpi_v)(h(x)) = h(x).$$

As $\varpi_v = u^{-1}\varpi'_v$, we have $\phi_{\varpi'_v}(\varpi_v) = \phi_{\varpi'_v}(u^{-1})\phi_{\varpi'_v}(\varpi'_v) = \sigma_1\sigma_2$ where

$$\sigma_1 = \begin{cases} \text{Frob}_{K_v} & \text{on } K_v^{\text{ur}} \\ \text{id} & \text{on } E_f^n \end{cases}$$

and

$$\sigma_2 = \begin{cases} \text{id} & \text{on } K_v^{\text{ur}} \\ [u]_f & \text{on } E_f^n. \end{cases}$$

We now use the fact that h has coefficients in $\widehat{K_v^{\text{ur}}}$ along with Proposition 5.51 to conclude that

$$\begin{aligned} \phi_{\varpi'_v}(\varpi_v)(h(x)) &= \sigma_1\sigma_2(h(x)) \\ &= \sigma_1(h(\sigma_2 x)) \\ &= \sigma_1(h([u]_f(x))) \\ &= h(x). \end{aligned}$$

Thus, $\phi_{\varpi'_v}(\varpi_v) = \text{id}$ on K_{v,ϖ_v} as well. Now since ϖ_v is an arbitrary uniformizer of K_v and the uniformizers generate K_v^\times (For $x \in K_v^\times$, write $x = u\varpi_v^m$. Then $x = (u\varpi_v)\varpi_v^{m-1}$ and $u\varpi_v$ is another uniformizer!) we have the result. \square

Exercise 5.54. Prove that for all m, n one has

$$\phi_{\varpi_v}(x)|_{K_{v,\varpi_v}^n K_m} = \text{id}$$

for all $x \in (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$.

Lemma 5.55. For all $x \in K_v^\times$, $\phi_{K_v}(x)|_{K_{v,\varpi_v}^n K^{\text{ur}}} = \phi_{\varpi_v}(x)$.

Proof. Recall that we showed for any n , ϖ_v is a norm from K_{v,ϖ_v}^n and so we know that $\phi_{K_v}(\varpi_v)$ acts trivially on K_{v,ϖ_v}^n . Namely, since $\phi_{K_v}|_{K_{v,\varpi_v}^n} = \phi_{K_{v,\varpi_v}^n/K_v}$ and $\phi_{K_{v,\varpi_v}^n/K_v}$ is trivial on $\text{Nm } K_{v,\varpi_v}^n$, we get that $\phi_{K_v}(\varpi_v)$ acts trivially on K_{v,ϖ_v}^n . We also know that ϕ_{ϖ_v} acts trivially on K_{v,ϖ_v}^n by the previous exercise with $m = 1$. We know that ϕ_{K_v} and ϕ_{ϖ_v} both act as Frob_{K_v} on K_v^{ur} , and so the two maps agree on $K_{v,\varpi_v}^n K_v^{\text{ur}}$ for all n , and so on the union $\bigcup K_{v,\varpi_v}^n K_v^{\text{ur}}$. However, we know that K_{v,ϖ_v}^\times is generated by the different uniformizers. Thus, we have the result. \square

Lemma 5.56. For $m, n \geq 0$ set $K_v^{n,m} = K_{v,\varpi_v}^n K_m$. We have $\text{Nm}((K_v^{n,m})^\times) = (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$.

Proof. We know that $\phi_{\varpi_v}(x)|_{K_v^{n,m}} = \text{id}$ for all $x \in (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$ and so by the previous theorem we know that $\phi_{K_v}(x)|_{K_v^{n,m}} = \text{id}$ for all $x \in (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$. Thus we have $(1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle \subseteq \text{Nm}((K_v^{n,m})^\times)$. On the other hand, we have

$$\begin{aligned} [K_v^\times : (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle] &= [\mathcal{O}_v^\times : 1 + \mathfrak{m}_v^n][\langle \varpi_v \rangle : \langle \varpi_v^m \rangle] \\ &= (q-1)q^n m \\ &= [K_{v,\varpi_v}^n : K_v][K_m : K_v] \\ &= [K_{v,\varpi_v}^{m,n} : K_v]. \end{aligned}$$

We know that ϕ_{K_v} induces an isomorphism

$$K_v^\times / \text{Nm}((K_v^{n,m})^\times) \longrightarrow \text{Gal}(K_v^{n,m}/K_v)$$

and so we must have $\text{Nm}((K_v^{n,m})^\times) = (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$. \square

Lemma 5.57. *Let L/K_v be a finite extension and assume $\text{Nm}(L^\times)$ is of finite index in K_v^\times . Then $\text{Nm}(L^\times)$ is open in K_v^\times .*

Proof. We have seen before that \mathcal{O}_L^\times is compact and so $\text{Nm}(\mathcal{O}_L^\times)$ is necessarily closed in K_v^\times . The only elements that have a unit norm are units, so we have

$$\mathcal{O}_v^\times / \text{Nm}(\mathcal{O}_L^\times) \hookrightarrow K_v^\times / \text{Nm}(L^\times).$$

Thus, $\text{Nm}(\mathcal{O}_L^\times)$ is closed of finite index in \mathcal{O}_v^\times and so is open in \mathcal{O}_v^\times (recall our valuation is discrete.) This also gives $\text{Nm}(\mathcal{O}_L^\times)$ is also open in K_v^\times . This shows that $\text{Nm}(L^\times)$ contains an open subgroup of K_v^\times and so is itself open in K_v^\times . \square

Theorem 5.58. *We have that $\phi_{K_v} = \phi_{\varpi_v}$ and $K_v^{\text{ab}} = K_{v,\varpi_v} K_v^{\text{ur}}$.*

Proof. Let L/K_v be a finite abelian extension. We know that $K_v^\times / \text{Nm}(L^\times) \cong \text{Gal}(L/K_v)$ and so we must have $\text{Nm}(L^\times)$ is of finite index. Thus, the previous lemma implies that $\text{Nm}(L^\times)$ is open in K_v^\times . Any open subgroup of finite index in K_v^\times must contain $(1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$ for some $m, n \geq 0$. We know that the map

$$\phi_{K_v} : K_v^\times \longrightarrow \text{Gal}(LK_v^{n,m}/K_v)$$

is an onto map. We also have that for $x \in K_v^\times$, $\phi_{K_v}(x)$ fixes the elements of L if and only if $x \in \text{Nm}(L^\times)$ and $\phi_{K_v}(x)$ fixes the elements of $K_v^{m,n}$ if and only if $x \in (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$. However, we have that $(1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle \subset \text{Nm}(L^\times)$ and so we must have $L \subseteq K_v^{n,m}$. Now if we take the union over all finite abelian extensions we see that $K_v^{\text{ab}} = K_{v,\varpi_v} K_v^{\text{ur}}$ and so $\phi_{K_v} = \phi_{\varpi_v}$. \square

Finally, we complete the proof of Theorem 5.2, which we restate here for convenience.

Theorem 5.59. *Let N be a subgroup of K_v^\times . The subgroup N is of the form $\text{Nm}_{L/K_v}(L^\times)$ for some finite abelian extension L/K_v if and only if N is of finite index and open.*

Proof. We already know that for any finite abelian extension L/K_v , $\text{Nm}(L^\times)$ is necessarily of finite index. This combined with Lemma 5.57 gives one direction of the theorem. Now suppose that N is of finite index and open in K_v^\times . Then as we observed above, there exists $n, m \geq 0$ so that $(1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle \subset N$. We also observed that $\text{Nm}((K_v^{n,m})^\times) = (1 + \mathfrak{m}_v^n)\langle \varpi_v^m \rangle$. Let L be the subfield of $K_v^{m,n}$ fixed by $\phi_{K_v^{m,n}/K_v}(N)$. Then we have that N is the kernel of the map $\phi_{K_v} : K_v^\times \rightarrow \text{Gal}(L/K_v)$ and so equals $\text{Nm}(L^\times)$ by Theorem 5.1. \square

This concludes the proofs of the main results of local class field theory. We conclude this section with the very explicit example of studying finite abelian extensions of $K_v = \mathbb{Q}_p$ and the local reciprocity map in this case. Recall that we have seen that for $p \nmid n$, the extension $\mathbb{Q}_p(\zeta_n)$ is an unramified extension of \mathbb{Q}_p . In fact, we have that $\mathbb{Q}_p^{\text{ur}} = \bigcup_{p \nmid n} \mathbb{Q}_p(\zeta_n)$. We also saw before that $\text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}}$.

It remains to determine the field $K_{v, \varpi_v} = (\mathbb{Q}_p)_p$. Let $f(T) = (T+1)^p - 1$. It is not difficult to see that $f \in \mathcal{F}_p$.

Exercise 5.60. Show that $F_f(X, Y) = X + Y + XY$. For $a \in \mathbb{Z}_p$ show that

$$\binom{a}{m} = \frac{a(a-1)\cdots(a-m+1)}{m(m-1)\cdots 1}$$

lies in \mathbb{Z}_p . Show that for $a \in \mathbb{Z}_p$ we have $[a]_f = (1+T)^a - 1$.

We have

$$\begin{aligned} E_f^n &= \{x \in \overline{\mathbb{Q}_p} : (x+1)^{p^n} = 1\} \\ &\cong \mu_{p^n} \end{aligned}$$

where E_f^n has the group structure given by F_f and μ_{p^n} is the group of p^n th roots of unity with normal multiplication. The action of \mathbb{Z}_p on E_f^n transfers to the action of \mathbb{Z}_p on μ_{p^n} given by

$$a \cdot \zeta = \zeta^a,$$

which makes sense since ζ is a p^n th root of unity. Thus, $E_f^n \cong \mathbb{Z}/p^n\mathbb{Z}$ as \mathbb{Z}_p -modules. This shows that our fields $K_{v, \varpi_v}^n \cong \mathbb{Q}_p(\mu_{p^n})$. Thus, we have that $(\mathbb{Q}_p)_p = \mathbb{Q}_p(\zeta_{p^\infty})$ where we write ζ_{p^∞} to indicate we have attached all p -power roots of unity. The Galois group is given by

$$\begin{aligned} \text{Gal}((\mathbb{Q}_p)_p/\mathbb{Q}_p) &= \varprojlim \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \\ &\cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \\ &\cong \mathbb{Z}_p^\times. \end{aligned}$$

Note that this shows that $\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p^{\text{cycl}}$, i.e., we have the local Kronecker-Weber theorem that all finite abelian extensions of \mathbb{Q}_p are contained in some cyclotomic extension $\mathbb{Q}_p(\zeta_n)$.

We now describe the local reciprocity map for \mathbb{Q}_p . Let $L = \mathbb{Q}_p(\zeta_n)$. First suppose that $p \nmid n$. Then we have that L/\mathbb{Q}_p is an unramified extension with degree equal to the degree of the residue field extension. The residue field is given by \mathbb{F}_{p^m} where m is the largest power of p so that $n \mid (p^m - 1)$. The local reciprocity map in this case sends $x = up^b \in \mathbb{Q}_p^\times$ to Frob_p^b . We have that the kernel of the map is $\text{Nm}(L^\times) = \mathbb{Z}_p^\times \langle p^m \rangle$.

Now suppose that n is a power of p , say $n = p^r$. In this case we have that L is totally ramified over \mathbb{Q}_p of degree $(p-1)p^{r-1}$, in fact, $L = (\mathbb{Q}_p)^r$. For $x \in \mathbb{Q}_p^\times$, write $x = up^b$ as above. Then we have $\phi_{\mathbb{Q}_p}(a)$ sends ζ_n to $\zeta_n^{u^{-1}}$. The kernel of the local reciprocity map is $\text{Nm}(L^\times) = \{up^s : u \equiv 1 \pmod{p^r}, s \in \mathbb{Z}\}$.

Finally, write $n = ap^r$. We can write $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_a)\mathbb{Q}_p(\zeta_{p^r})$. The local reciprocity map is then given by the action on each piece separately as given above.

5.6 Final Remarks

In the previous sections we constructed the local reciprocity map $\phi_{K_v} : K_v^\times \rightarrow \text{Gal}(K_v^{\text{ab}}/K_v)$ and showed that it gives for any finite abelian extension L/K_v an isomorphism $K_v^\times / \text{Nm}(L^\times) \cong \text{Gal}(L/K_v)$. This of course fails to tell us what exactly K_v^\times is isomorphic to and it also fails to give us a satisfactory description of $\text{Gal}(K_v^{\text{ab}}/K_v)$. We use this section to remedy this situation.

We begin with the isomorphism $K_v^\times / \text{Nm}(L^\times) \cong \text{Gal}(L/K_v)$ for L/K_v an abelian extension. We know that K_v^{ab} is formed by taking the union over finite abelian extensions of K_v and $\text{Gal}(K_v^{\text{ab}}/K_v) = \varprojlim_L \text{Gal}(L/K_v)$ where the limit is over finite abelian extensions ordered with respect to inclusion. Applying this inverse limit to our isomorphism above we obtain

$$\widehat{K}_v^\times = \varprojlim_L K_v^\times / \text{Nm}(L^\times) \cong \varprojlim_L \text{Gal}(L/K_v) \cong \text{Gal}(K_v^{\text{ab}}/K_v)$$

where \widehat{K}_v^\times is the profinite completion of K_v^\times with respect to the subgroups $\text{Nm}(L^\times)$ where we have used the results of local class field theory to conclude that the norm subgroups are a sufficient set of subgroups to take this limit.

It now remains to give a satisfactory description of \widehat{K}_v^\times and then to describe the image of K_v^\times inside $\text{Gal}(K_v^{\text{ab}}/K_v)$. One can apply Kummer theory to conclude that the subgroups $(K_v^\times)^n$ form a cofinal subset of the subgroups of finite index of K_v^\times and so

$$\widehat{K}_v^\times \cong \varprojlim_{n \geq 1} (K_v^\times / (K_v^\times)^n).$$

We now use that $K_v^\times \cong \varpi_v^{\mathbb{Z}} \times \mathcal{O}_v^\times$ and that \mathcal{O}_v is a profinite group to obtain

$$\widehat{K}_v^\times \cong \widehat{\varpi}_v^{\mathbb{Z}} \times \mathcal{O}_v^\times,$$

which gives our explicit description of the Galois group $\text{Gal}(K_v^{\text{ab}}/K_v)$.

Exercise 5.61. Note that $\phi_{K_v} : K_v^\times \rightarrow \text{Gal}(K_v^{\text{ab}}/K_v)$ is an injective homomorphism. (Do not confuse this with the fact that when one restricts to $\text{Gal}(L/K_v)$ there is a kernel!) Thus, K_v^\times is isomorphic to its image in $\text{Gal}(K_v^{\text{ab}}/K_v)$. Given $g \in \text{Gal}(K_v^{\text{ab}}/K_v)$, write \bar{g} to denote the image of g in $\text{Gal}(\bar{k}_v/k_v) \cong \text{Gal}(K_v^{\text{ur}}/K_v)$. Show that the image of K_v^\times is precisely the subgroup

$$W_{K_v}^{\text{ab}} = \{g \in \text{Gal}(K_v^{\text{ab}}/K_v) : \bar{g} = \text{Frob}_v^n \text{ for some } n \in \mathbb{Z}\}.$$

This group is often referred to as the local Weil group.

Bibliography

- [AM69] M. F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*, Perseus Books, ISBN: 0-201-40751-5.
- [CF67] J.W.S Cassels and A. Frohlich, *Algebraic Number Theory*, Thompson Book Company, ISBN: 0-121-63251-2.
- [FT94] A. Frohlich and M.J. Taylor, *Algebraic Number Theory*, Cambridge studies in advanced mathematics Vol. 27, ISBN: 0-521-43834-9.
- [J96] G. Janusz, *Algebraic Number Fields*, AMS Graduate Studies in Mathematics Vol. 7, ISBN: 0-8218-0429-4.
- [L86] S. Lang, *Algebraic Number Theory*, Springer Graduate Texts in Mathematics 110, ISBN: 0-387-96375-8.
- [Mat94] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics Vol. 8, ISBN: 0-521-36764-6.
- [Mi98] J. Milne, *Algebraic Number Theory*, <http://www.jmilne.org/math>, 1-138 (1998).
- [Mi97] J. Milne, *Class Field Theory*, <http://www.jmilne.org/math>, 1-222 (1997).
- [N99] J. Neukirch, *Algebraic Number Theory*, Springer: A Series of Comprehensive Studies in Mathematics Vol. 322, ISBN: 3-540-65399-6.
- [S79] J-P. Serre, *Local Fields*, Springer Graduate Texts in Mathematics 67, ISBN: 0-387-90424-7.