MSc Mathematics

Track: Algebra and Geometry

Master thesis

Lubin-Tate theory

by

Guillermo Fernández Castro

October 1, 2018

Supervisor: dr. Arno Kret

Second examiner: dr. Sander Dahmen

Department of Mathematics

Faculty of Sciences

VU UNIVERSITY AMSTERDAM

Abstract

We present the main statements about Lubin-Tate theory and how they lead to the classical results of local class field theory. This is done avoiding all cohomological arguments, showing the local Kronecker-Weber theorem using the Hasse-Arf theorem and proving all necessary properties about the reciprocity map using Lubin-Tate formal groups and relative Lubin-Tate extensions. This exposition is primarily based on those of Iwasawa [Iwa86], Hazewinkel [Haz75], and Milne [Mil13].

Title: Lubin-Tate theory
Author: Guillermo Fernández Castro, g.fernandezcastro@student.vu.nl, 2594996
Supervisor: dr. Arno Kret
Second examiner: dr. Sander Dahmen
Date: October 1, 2018

Department of Mathematics
VU University Amsterdam
de Boelelaan 1081, 1081 HV Amsterdam
`http://www.math.vu.nl/`

Summary

Number theory is the branch of mathematics studying properties of numbers and the relations between them. Some of these relations are given in the form of polynomial equations, for example,

$$X^n + Y^n = Z^n, \qquad X^2 - dY^2 = 1, \qquad X^2 + d = Y^3,$$

where all the terms have integer coefficients; a number theorist would be interested in studying integer solutions to equations like these.

This, however, has proven to be extremely difficult: There is no single method to find these solutions, and while a few equations can be solved easily, many others have been studied for years —or even centuries, as was the case with Fermat's Last Theorem. Many techniques have been developed over the years in order to better tackle these problems. Class field theory is one of those techniques. It uses Galois theory, which studies a sort of algebraic symmetries of fields —namely, their automorphisms—, and formulates with it deep statements about the properties of some field extensions of the rational numbers. Proving these statements would generally require knowledge about many abstract topics, but a variant of them, known as local class field theory, can be proved through other means.

One such method is Lubin-Tate theory. Developed in the 1960s, it leads to the results of local class field theory, but it can also be applied to other settings beyond it, relevant to modern research —there are, after all, proofs for the local Langlands conjecture which have been influenced by the ideas of Lubin and Tate. It becomes then of interest to understand this theory better, so the purpose of this document is to give an introduction to Lubin-Tate theory, developing the main ideas behind it and explaining how it leads to the results of local class field theory.

Introduction

The study of the extensions of the rational numbers, and more generally of number fields, is essential in order to better understand Diophantine equations. In this context, class field theory begins by characterizing and showing certain properties of Abelian extensions of these fields, as well as of their local counterparts, the fields of p-adic numbers and more general local fields. One example of this is the Kronecker-Weber theorem, asserting that every Abelian extension of $\mathbf{Q}$ is contained in a cyclotomic extension; its local version gives an analogous statement regarding Abelian extensions of the p-adic numbers $\mathbf{Q}_p$. For more general fields, one can still give some properties of their Abelian extensions, but generally no explicit descriptions of them will be available using class field theory.

Originally, the statements from local class field theory were derived from those of global class field theory, by completing the fields at the relevant primes and deriving the Artin reciprocity map for local fields from the one for global fields. However, it was desirable to find a formulation of local class field theory independent of the global case, so that global class field theory could be derived from local class field theory. One approach to do this is using cohomological methods, which make it possible to prove local class field theory, and then using the idèlic formulation of Chevalley to get global class field theory from the local version. While being a powerful method, it has an important drawback, namely that its abstraction does not lead to explicit constructions. This is where Lubin-Tate theory becomes useful.

Lubin and Tate introduced their theory in 1965. In their article [LT65], they present a way to describe the maximal Abelian extension of a non-Archimedean local field K, as well as the reciprocity law. For this, they use the fact that, given an Abelian closure of K, there is one maximal unramified extension K^{nr} of K inside of it; they then construct an Abelian, maximal totally ramified extension K_π of K, and see that the compositum of the two give rise to the Abelian closure. The extension K_π is not canonical, but depends on the choice of a uniformizing parameter π of K. Nevertheless, one can give, independently on the choice of π, an explicit description of the reciprocity law via the study of the Galois group of K_π/K.

While the approach of Lubin and Tate gave a description of the Abelian closure of

K, this was done assuming the results of local class field theory. In later articles, Lubin [Lub81], Rosen [Ros81] and Gold [Gol81] proved the so-called local Kronecker-Weber theorem directly, without using local class field theory. The approach of Rosen uses Kummer theory for local fields of characteristic 0, while the ones of Lubin and Gold use ramification groups and the Hasse-Arf theorem. It is the latter approach the one found in the book of Iwasawa [Iwa86] and the article of Yoshida [Yos08], and it is the one we shall use here.

This text is organized as follows.

Chapter 1 gives preliminary results about formal groups, and introduces Lubin-Tate formal groups associated to certain power series with coefficients in $\mathcal{O}_K$, the ring of integers of K. We see that these formal groups lead to a formal $\mathcal{O}_K$-module. The nature of this chapter is at times more general than necessary, insofar as it gives more general results than are immediately necessary for Chapter 2, but it sets the foundations for later chapters, where the extra generality becomes useful.

In Chapter 2 we introduce the Lubin-Tate extensions of a local field K. These are generated by the roots of a polynomial like the one of Chapter 1, and we use the results on Lubin-Tate formal groups to show that these extensions are Galois and totally ramified. We also give results about the norm groups of these extensions. The overall nature of the computations is rather elementary, allowing us to describe these relevant properties in a very explicit way. This is mostly the approach followed in the aptly-named article of Hazewinkel [Haz75], who ultimately shows many important results in local class field theory from this elementary point of view. The reason for this is to give a more accessible introduction to the setting of Lubin-Tate theory, using only results from algebraic number theory and Galois theory, without needing the full extent of the results from Chapter 1.

In Chapter 3 we construct the totally ramified extension K_π/K, based on the Lubin-Tate extensions of Chapter 2, and we use it to formulate the reciprocity law in a preliminary way. For this we present the Lubin-Tate extensions as generated by torsion elements for the formal $\mathcal{O}_K$-module: This allows us to show, using results from formal groups, that the reciprocity law is well-defined and independent of the choice of uniformizer π of K.

The reciprocity law takes its usual form after Chapter 4, where we prove the local Kronecker-Weber theorem using the Hasse-Arf theorem on ramification groups. This requires us to introduce the theory of ramification groups, including their upper numbering. With this, we can show that the Abelian closure of K can be described in terms of the maximal unramified subextension and the totally ramified extension K_π.

Finally, in Chapter 5 we return to the reciprocity law, fully described now using the local Kronecker-Weber theorem, and give a characterization of it in terms of norm groups

of Abelian extensions of K. In this chapter we also introduce a generalization of the Lubin-Tate extension, given by de Shalit [Sha85].

Contents

1 Formal groups

The goal of this chapter is to give an explicit description of the Lubin-Tate tower of extensions of a non-Archimedean local field K. These extensions are defined via the notion of formal groups, which we introduce. We then give elementary proofs for some of the most relevant results about these Lubin-Tate extensions, including a description of their Galois groups and the image of the norm map inside $K^\times$. This chapter is based primarily on the treatments of [Lan90, Chap. 8, §1] and [Iwa86, Chap. 3, §5 and Chap. 4, §1–3].

1.1 First definitions and examples

From now on, given a ring R, we will denote by $R[[X]]$ the ring of power series in the variable X with coefficients in R. We assume some knowledge on this ring; a reference for this is [Iwa86, Chap. 3, §4].

Definition 1.1.1. Let R be a ring (assumed non-trivial, commutative, with identity). A **formal group over** R is a formal power series $F(X,Y) \in R[[X,Y]]$ with the following properties:

(F1) $F(X,Y) \equiv X + Y \bmod (X,Y)^2$,

(F2) $F(F(X,Y),Z) = F(X,F(Y,Z))$,

(F3) $F(X,Y) = F(Y,X)$.

To justify the name of formal group, we would like for this power series to come with some notion of neutral and inverse elements, as the properties (F2) and (F3) are analogous to associativity and commutativity. We would like, for instance, to show that $F(X,0) = X$ and $F(0,Y) = Y$, that is, to show that the zero series acts as a neutral element. We take care of this in the following proposition.

Proposition 1.1.2. *Let F be a formal group over R. Then*

(i) $F(X,0) = X$ *and* $F(0,Y) = Y$,

(ii) there exists a unique power series $i_F(X) \in XR[[X]]$ *such that* $F(X, i_F(X)) = F(i_F(X), X) = 0$.

Proof. Let $f(X) = F(X, 0)$, then the associativity condition (F2) implies $f(f(X)) = f(X)$, that is, $f \circ f = f$. Now, f has an inverse under composition: We have $f(X) \equiv X \bmod X^2$, so in particular it has no constant term and the coefficient of X is invertible in R, and thus we can define the coefficients of f^{-1} by induction so that $f^{-1}(f(X)) = f(f^{-1}(X)) = X$. Expanding f, we see that

$$f^{-1}(f(f(X))) = f(X) = F(X, 0)$$

while at the same time,

$$f^{-1}(f(f(X)) = f^{-1}((f \circ f)(X)) = f^{-1}(f(X)) = X$$

so $F(X, 0) = X$, and therefore the zero series acts as the neutral element of F. Commutativity as in (F3) finishes the proof of (i). From this we deduce that all the terms of $F(X, Y)$ of degree greater or equal than 2 are divisible by XY, so we can write

$$F(X, Y) = X + Y + \sum_{i,j \geqslant 1} a_{ij} X^i Y^j$$

where $a_{ij} = a_{ji}$ by the property (F3). By induction, it can be shown that there exist $b_2, b_3, \ldots$ such that the power series $i_F(X) = -X + \sum_{k \geqslant 2} b_k X^k$ satisfies (ii). If a series $g \in XR[[X]]$ also satisfies (ii), then associativity as in (F2) implies

$$\begin{aligned} g(X) &= F(g(X), 0) = F(g(X), F(X, i_F(X))) = F(F(g(X), X), i_F(X)) = F(0, i_F(X)) \\ &= i_F(X), \end{aligned}$$

thus showing uniqueness. □

Definition 1.1.3. Let F and G be formal groups over R. A power series $f(X) \in XR[[X]]$ is called a **homomorphism from** F **to** G if it satisfies $f(F(X, Y)) = G(f(X), f(Y))$. The set of homomorphisms from F to G is denoted $\mathrm{Hom}_R(F, G)$. An **endomorphism of** F is a homomorphism from F to itself; the set of endomorphisms of F is denoted $\mathrm{End}_R(F)$ and it is a monoid under composition, where the identity endomorphism is $\mathrm{id} = X$.

We can actually give more structure to the monoid $\mathrm{End}_R(F)$. Given two endomorphisms $f, g \in \mathrm{End}_R(F)$, we may define their sum, denoted $f +_F g$, as $(f +_F g)(X) = F(f(X), g(X))$. This makes $\mathrm{End}_R(F)$ into a (possibly non-commutative) ring under addition and composition.

We now consider some examples of formal groups.

Example 1.1.4. (i) The **formal additive group** is the power series $F(X,Y) = X + Y$.

(ii) The **formal multiplicative group** is the power series $F(X,Y) = X + Y + XY$.

(iii) Let F be a formal group over a complete valuation ring R, and let $\mathfrak{m}$ be its unique maximal ideal. For any positive integer k, the quotient $R/\mathfrak{m}^k$ is an Artinian ring with unique prime ideal $\mathfrak{m}/\mathfrak{m}^k$. Then, by definition of the radical of an ideal, we find that $\mathfrak{m}/\mathfrak{m}^k = \mathrm{nil}(R)$ the nilradical of R, so every element of $\mathfrak{m}/\mathfrak{m}^k$ is nilpotent. In this case, the law $(x,y) \mapsto x +_F y := F(x,y)$ defines a group structure in $\mathfrak{m}/\mathfrak{m}^k$, and any endomorphism $f \in \mathrm{End}_R(F)$ becomes also a group endomorphism of $(\mathfrak{m}/\mathfrak{m}^k, +_F)$. Now, for any $m \in \mathfrak{m}$, we have that m^k tends to zero, in the sense of the valuation, as k increases; by continuity, the new group law $+_F$ of $\mathfrak{m}/\mathfrak{m}^k$ extends to a group law $+_F$ in $\mathfrak{m}$, where again $x +_F y := F(x,y)$ for any $x, y \in \mathfrak{m}$. Similarly, endomorphisms of F become endomorphisms of $(\mathfrak{m}, +_F)$.

1.2 Lubin-Tate formal groups

Since the goal of this master's thesis is to use formal groups in the setting of local fields, it is convenient to assume from now on that R is the ring of integers of a local field. We will always assume our local fields to be non-Archimedean. For more on local fields, see [Iwa86, Chap. 2], [Frö67, p.1–41] or [Neu99, Chap. II].

Let p be a prime, and let K be a non-Archimedean local field with $R = \mathcal{O}_K$ its ring of integers and $\mathfrak{p}$ its maximal ideal, such that the quotient field $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ has cardinality $q = p^r$ for some r. Let π be a uniformizer of K, that is, $(\pi) = \mathfrak{p}$. We choose a power series $f \in \mathcal{O}_K[[X]]$ such that

$$f(X) \equiv \pi X \bmod X^2$$
$$f(X) \equiv X^q \bmod \pi.$$

Example 1.2.1. (i) Take the polynomial $f(X) = X^q + \pi X$, then clearly f is a power series satisfying the conditions above.

(ii) Take $K = \mathbf{Q}_p$ and the uniformizer $\pi = p$; then the polynomial

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

also satisfies the conditions above.

We will eventually define an extension of K based on the power series f; in order to deduce some of its properties, we will need the formal groups we have introduced. However, it will be convenient to prove some results in a more general setting: Instead of defining f over K, we consider the maximal unramified extension K^{nr} of K inside the separable closure K^{sep}, and take its completion with respect to the extension of the valuation on K to K^{nr}. We denote this completion by $\widehat{K^{\mathrm{nr}}}$. The extension K^{nr}/K is Galois and its Galois group is generated by the Frobenius element $\phi \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$, which satisfies $\phi(a) \equiv a^q \bmod \mathfrak{p}$. Given a power series $F \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X_1, \ldots, X_n]]$, the Frobenius ϕ acts on it by taking the image of the coefficients under ϕ; the resulting power series will be denoted F^ϕ.

Lemma 1.2.2. *Let π and π' be uniformizers of $\widehat{K^{\mathrm{nr}}}$. Let f, g be power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f \equiv g \equiv X^q \bmod \pi \qquad f \equiv \pi X \bmod X^2 \qquad g \equiv \pi' X \bmod X^2.$$

Let L be a linear form in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[X_1, \ldots, X_n]$,

$$L(X_1, \ldots, X_n) = a_1 X_1 + \cdots + a_n X_n,$$

such that $\pi L = \pi' L^\phi$. Then there exists a unique power series $F \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X_1, \ldots, X_n]]$ such that

$$f(F(X_1, \ldots, X_n)) = F^\phi(g(X_1), \ldots, g(X_n)). \tag{1.2.1}$$

and

$$F \equiv L \bmod (X_1, \ldots, X_n)^2.$$

Moreover, in case f, g, and L have all coefficients in $\mathcal{O}_K$, then $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$.

Proof. (See [Lan90, p.193, Lemma] or [Iwa86, p.47, Proposition 3.12].) We can prove this by showing that, for every $m \geqslant 1$, there exists a unique polynomial F_m of degree at most m such that the equalities hold modulo $(X_1, \ldots, X_n)^{m+1}$. The result then follows by induction. For $m = 1$ we may take $F_1 = L$; as a result, we immediately get that $f(F_1(X_1, \ldots, X_n)) = F_1^\phi(g(X_1), \ldots, g(X_n))$ from the conditions on L. Assuming that there is such a unique F_m, to show that F_{m+1} exists we would require that $F_{m+1} = F_m + H_{m+1}$ where H_{m+1} is a homogeneous polynomial of degree $m+1$ over $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$; the uniqueness of H_{m+1} would imply the uniqueness of F_{m+1}. Composing such F_{m+1} with f and g gives

$$\begin{aligned} &f(F_{m+1}(X_1, \ldots, X_n)) \\ &\equiv f(F_m(X_1, \ldots, X_n)) + \pi H_{m+1}(X_1, \ldots, X_n) \bmod (X_1, \ldots, X_n)^{m+2} \end{aligned}$$

and

$$\begin{aligned}
&F^{\phi}_{m+1}(g(X_1),\dots,g(X_n))\\
&\equiv F^{\phi}_{m}(g(X_1),\dots,g(X_n)) + H^{\phi}_{m+1}(\pi' X_1,\dots,\pi' X_n)\\
&\equiv F^{\phi}_{m}(g(X_1),\dots,g(X_n)) + \pi'^{m+1} H^{\phi}_{m+1}(X_1,\dots,X_n) \bmod (X_1,\dots,X_n)^{m+2}.
\end{aligned}$$

Removing all variables for clarity, the congruence we aim to prove

$$f \circ F_{m+1} \equiv F^{\phi}_{m+1} \circ g \bmod (X_1,\dots,X_n)^{m+2},$$

becomes

$$(f \circ F_m - F^{\phi}_m \circ g) + \pi H_{m+1} - \pi'^{m+1} H^{\phi}_{m+1} \equiv 0 \bmod (X_1,\dots,X_n)^{m+2}. \tag{1.2.2}$$

To show that there exists a unique H_{m+1}, we consider equations for its coefficients. Note that

$$f \circ F_m - F^{\phi}_m \circ g \equiv 0 \bmod \mathfrak{p}:$$

To see this, write $F_{m+1} = \sum_{\mathbf{i}} b_{\mathbf{i}} X^{\mathbf{i}}$, where we denote by $X^{\mathbf{i}}$ the monomial $X_1^{i_1} \cdots X_n^{i_n}$; then

$$f(F_m(X_1,\dots,X_n)) - F^{\phi}_m(g(X_1),\dots,g(X_n)) \equiv \sum_{\mathbf{i}} (b^q_{\mathbf{i}} - b^{\phi}_{\mathbf{i}}) X^{\mathbf{i}} \equiv 0 \bmod \mathfrak{p}$$

since $f \equiv g \equiv X^q \bmod \mathfrak{p}$ and $b^{\phi}_{\mathbf{i}} = \phi(b_{\mathbf{i}}) \equiv b^q_{\mathbf{i}} \bmod \mathfrak{p}$. Hence, the coefficient of $X^{\mathbf{i}}$ must admit an expression of the form $-\pi\alpha$ for some $\alpha \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$. Let $c_{\mathbf{i}}$ be the coefficient of $X^{\mathbf{i}}$ (assumed of degree $m+1$) in H_{m+1}. Then, the congruence (1.2.2) for the summands on $X^{\mathbf{i}}$ gives

$$-\pi\alpha + \pi c_{\mathbf{i}} - \pi'^{m+1} c^{\phi}_{\mathbf{i}} = 0$$

which becomes

$$c_{\mathbf{i}} = \alpha + c^{\phi}_{\mathbf{i}} \beta \tag{1.2.3}$$

where $\beta = \pi'^{m+1}/\pi$ has norm strictly smaller than 1. Expanding this expression yields

$$c_{\mathbf{i}} = \alpha + \phi(\alpha)\beta + \phi^2(c_{\mathbf{i}})\beta\phi(\beta) = \alpha + \phi(\alpha)\beta + \phi^2(\alpha)\beta\phi(\beta) + \cdots,$$

which is convergent in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$. This shows existence, as both α and β are known. To show uniqueness, let $d_{\mathbf{i}}$ be another solution, then both the norms $|c_{\mathbf{i}} - d_{\mathbf{i}}|$ and $|\phi(c_{\mathbf{i}}) - \phi(d_{\mathbf{i}})|$ must be equal. However, substituting in (1.2.3) yields that $|c_{\mathbf{i}} - d_{\mathbf{i}}| = |\beta|\,|\phi(c_{\mathbf{i}}) - \phi(d_{\mathbf{i}})|$; since the norm of β is strictly smaller than 1, both equalities can only be true if the norms are zero, which means $c_{\mathbf{i}} = d_{\mathbf{i}}$. Hence H_{m+1} exists and is unique, and so is F_{m+1}. Existence and uniqueness of F then follow by induction.

Finally, let us suppose that all of f, g and L have coefficients in $\mathcal{O}_K$. We can show that F has coefficients in $\mathcal{O}_K$ by showing inductively that all the F_m also have coefficients in $\mathcal{O}_K$. For $m = 1$, $F_1 = L$, so it holds. Assuming that $F_m \in \mathcal{O}_K[[X_1, \ldots, X_n]]$, then the coefficient $-\pi\alpha$ of the term in $X^{\mathbf{i}}$ of $f \circ F_m - F_m \circ g$ must also lie in $\mathcal{O}_K$. Hence $\alpha \in \mathcal{O}_K$, and by (1.2.3) and the fact that $\mathcal{O}_K$ is complete we have $c_{\mathbf{i}} \in \mathcal{O}_K$, which implies that F_{m+1} has coefficients in $\mathcal{O}_K$. □

The cases we will consider most are those where the power series f and g are taken in $\mathcal{O}_K[[X]]$ and $\pi = \pi'$. While it is convenient to formulate some of the next results for power series with coefficients in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$, we will focus for the time being on what can be said when only one prime element π is at play. We will return to considering the interplay between different primes in Section 3.

Theorem 1.2.3. *Let π be a uniformizer of $\widehat{K^{\mathrm{nr}}}$, and let f be a power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f \equiv X^q \bmod \pi \qquad\qquad f \equiv \pi X \bmod X^2.$$

Then there exists a unique formal group F_f over $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$ such that f is a homomorphism from F_f to F_f^ϕ. If $f \in \mathcal{O}_K[[X]]$, then $F_f \in \mathcal{O}_K[[X, Y]]$ and f is an endomorphism of F_f.

Definition 1.2.4. In this context, the formal group F_f is called the **Lubin-Tate formal group associated to** f.

Proof of Theorem 1.2.3. We can apply Lemma 1.2.2 for $f = g$ and $L(X, Y) = X + Y$. The existence of F_f with $f \circ F_f = F_f^\phi \circ f$ follows immediately with the case where $f \in \mathcal{O}_K[[X]]$ implying that $F_f \in \mathcal{O}_K[[X, Y]]$ and hence $F_f^\phi = F_f$. It remains to be checked that such F_f has the properties of a formal group. Property (F1) follows from having used the form $L(X, Y) = X + Y$. Associativity (F2) is a consequence of the uniqueness property of Lemma 1.2.2: Let G be the unique power series with $f \circ G = G^\phi \circ f$ and $G \equiv X + Y + Z \bmod (X, Y, Z)^2$, and let $G_1(X, Y, Z) := F_f(F_f(X, Y), Z)$, $G_2(X, Y, Z) := F_f(X, F_f(Y, Z))$; then

$$f \circ G_1(X, Y, Z) = F_f^\phi(f(F_f(X, Y)), f(Z)) = F_f^\phi(F_f^\phi(f(X), f(Y)), f(Z)) = G_1^\phi \circ f$$
$$f \circ G_2(X, Y, Z) = F_f^\phi(f(X), f(F_f(Y, Z))) = F_f^\phi(f(X), F_f^\phi(f(Y), f(Z))) = G_2^\phi \circ f$$

and hence $G_1 = G = G_2$. Commutativity (F3) is similar, since the power series $H(X, Y) = F_f(Y, X)$ has the same properties as F_f and the latter is unique. Hence F_f is a formal group, and as a consequence so is F_f^ϕ, so f is indeed a homomorphism of formal groups. □

Example 1.2.5. Let $K = \mathbf{Q}_p$, and let $f(X) = (1 + X)^p - 1$. Then the Lubin-Tate formal

group of f is the multiplicative group

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

We have $F_f(X,Y) \equiv X + Y \bmod (X,Y)^2$ and

$$\begin{aligned} f(F_f(X,Y)) &= (1 + (1+X)(1+Y) - 1)^p - 1 = (1+X)^p(1+Y)^p - 1 \\ &= (1 + (1+X)^p - 1)(1 + (1+Y)^p - 1) - 1 = F_f(f(X), f(Y)). \end{aligned}$$

Uniqueness of F_f shows then the equality.

Theorem 1.2.6. *Let π be a prime element of $\widehat{K^{\mathrm{nr}}}$. Let f, g be power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f(X) \equiv g(X) \equiv X^q \bmod \pi \qquad\qquad f(X) \equiv g(X) \equiv \pi X \bmod X^2.$$

For any $a \in \mathcal{O}_K$, there exists a unique power series $[a]_{f,g} \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that

$$\begin{aligned} f([a]_{f,g}(X)) &= [a]^{\phi}_{f,g}(g(X)) \\ [a]_{f,g}(X) &\equiv aX \bmod X^2. \end{aligned}$$

If $f, g \in \mathcal{O}_K[[X]]$, then so is $[a]_{f,g}$.

Proof. This follows from applying Lemma 1.2.2 using the linear form $L(X) = aX$. □

Note that, since for all $a \in \mathcal{O}_K$ we have $[a]_{f,g} \equiv aX \bmod X^2$, in particular we have $[a]_{f,g} \in X\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$, so compositions like $[a]_{f,g} \circ [b]_{g,h}$ make sense as power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$.

Corollary 1.2.7. *Let π be a prime element of $\widehat{K^{\mathrm{nr}}}$. Let f, g, h be power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f(X) \equiv g(X) \equiv h(X) \equiv X^q \bmod \pi \qquad f(X) \equiv g(X) \equiv h(X) \equiv \pi X \bmod X^2.$$

For any $a, b \in \mathcal{O}_K$, we have

(i) $[a+b]_{f,g}(X) = [a]_{f,g}(X) +_{F_f} [b]_{f,g}(X) := F_f([a]_{f,g}(X), [b]_{f,g}(X))$,

(ii) $[ab]_{f,h}(X) = [a]_{f,g} \circ [b]_{g,h}$, *in particular* $[1]_{f,g}([1]_{g,f}(X)) = X$.

(iii) if $f \in \mathcal{O}_K[[X]]$, then $[\pi]_{f,f}(X) = f(X)$.

Proof. These properties follow by uniqueness of the power series $[a]_{f,g}$ and the definition of formal group. □

Since the case where $f = g$ deserves special attention and will come up frequently, we will abbreviate and denote $[a]_f = [a]_{f,f}$.

Corollary 1.2.8. *Let π be a prime element of $\widehat{K^{\mathrm{nr}}}$. Let f be a power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f(X) \equiv X^q \bmod \pi \qquad\qquad f(X) \equiv \pi X \bmod X^2.$$

The association $a \mapsto [a]_f$ is an injective ring homomorphism from $\mathcal{O}_K$ into $\mathrm{End}_{\mathcal{O}_K}(F_f)$.

Example 1.2.9. Take $K = \mathbf{Q}_p$, and $f = (1+X)^p - 1$, so that $F_f(X,Y) = (1+X)(1+Y) - 1$. For $a \in \mathcal{O}_{\mathbf{Q}_p} = \mathbf{Z}_p$, define

$$(1+X)^a = \sum_{m \geqslant 0} \binom{a}{m} T^m \text{ where } \binom{a}{m} = \frac{a(a-1)\cdots(a-m+2)(a-m+1)}{m!}.$$

The element $\binom{a}{m}$ is well-defined: It gives the usual definition when $a \in \mathbf{Z}$, and if $a = \lim a_n$ with $a_n \in \mathbf{Z}$, then $\binom{a_n}{m} \to \binom{a}{m}$. Under this notation, we have that $[a]_f = (1+X)^a - 1$. Indeed, $(1+X)^a - 1 \equiv aX \bmod X^2$, and

$$\begin{aligned} f((1+X)^a - 1) &= (1 + (1+X)^a - 1)^p - 1 = (1+X)^{ap} - 1 \\ &= (1 + (1+X)^p - 1)^a - 1 = (1 + (f(X))^a - 1. \end{aligned}$$

Moreover, the case where $a = p$ gives directly f.

2 Lubin-Tate extensions

The goal of this chapter is to describe the Lubin-Tate tower of extensions of a local field K. These extensions are defined via the notion of Lubin-Tate formal groups, which we introduced in the previous chapter. We give elementary proofs for some of the most relevant results about these Lubin-Tate extensions, including a description of their Galois groups and the image of the norm map inside $K^\times$. Most of these explicit computations can be found in [Haz75, §6].

2.1 The Lubin-Tate tower of extensions

Let K be a non-Archimedean local field whose residue field is a finite extension of $\mathbf{F}_p$; let $\mathcal{O}_K$ denote its ring of integers with $\mathfrak{p}_K$ the maximal ideal of $\mathcal{O}_K$, and let $U_K = \mathcal{O}_K^\times$ denote its group of units. Let q denote the cardinality of $\mathcal{O}_K/\mathfrak{p}$. We denote the maximal unramified extension of K inside a fixed separable closure by K^{nr}, and its completion with respect to the norm by $\widehat{K^{\mathrm{nr}}}$; the Frobenius automorphism of both K^{nr} and $\widehat{K^{\mathrm{nr}}}$ is denoted by ϕ.

Definition 2.1.1. Let π be a prime element of $\widehat{K^{\mathrm{nr}}}$, and let $f \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ be a power series such that $f(X) \equiv \pi X \bmod X^2$ and $f(X) \equiv X^q \bmod \pi$. We define

$$\begin{aligned} f^{(0)} &= X, \\ f^{(1)} &= f, \\ f^{(m+1)} &= f^{\phi^m} \circ f^{(m)}, \text{ for } m \geqslant 1 \end{aligned}$$

where f^{ϕ^m} is the power series whose coefficients are the images under ϕ^m of those of f.

In case the power series f in Definition 2.1.1 has coefficients in $\mathcal{O}_K$, then $f^{\phi^m} = f$ for all $m \geqslant 1$ and $f^{(m)} = f \circ f \circ \cdots \circ f$ denotes the m-th iterate of f.

We define the following extensions of K.

Definition 2.1.2. Let π be a prime of K, and let $f \in \mathcal{O}_K[[X]]$ be such that $f \equiv X^q \bmod \pi$ and $f \equiv \pi X \bmod X^2$. For any $m \geqslant 1$, take a root λ_m of $f^{(m)}$ such that $f^{(m-1)}(\lambda_m) \neq 0$.

We can take the λ_m in such a way that $f(\lambda_m) = \lambda_{m-1}$. Then we define the **$m$-th Lubin-Tate extension** $K_{\pi,m}/K$ by $K_{\pi,m} = K(\lambda_m)$. Note that the condition $f(\lambda_m) = \lambda_{m-1}$ implies that $K_{\pi,m-1} \subseteq K_{\pi,m}$, as they are complete.

Proposition 2.1.3. *The extension $K_{\pi,m}$ is independent of the choice of f.*

Proof. (See [Haz75, p.170, Remark 6.11].) Consider a polynomial $g \in \mathcal{O}_K[X]$ such that $g(X) \equiv \pi X \bmod X^2$ and $g(X) \equiv X^q \bmod \pi$, By Theorem 1.2.6, there exists a unique power series $[1]_{f,g}$ such that $[1]_{f,g}(X) \equiv X \bmod X^2$ and $f([1]_{f,g})(X) = [1]_{f,g}(g(X))$. In particular, $f^{(r)} \circ [1]_{f,g} = [1]_{f,g} \circ g^{(r)}$ for all r. Hence, if μ_m is a root of $g^{(m)}$ that is not a root of $g^{(m-1)}$, we deduce that $[1]_{f,g}(\mu_m)$ is a root of $f^{(m)}$ that is not a root of $f^{(m-1)}$. However, since $[1]_{f,g}(\mu_m) \in K(\mu_m)$, we deduce that $K_{\pi,m} \subseteq K(\mu_m)$; as the degrees of both extensions of K are the same, we conclude that $K_{\pi,m} = K(\mu_m)$. □

Theorem 2.1.3 shows, in particular, that we may define $K_{\pi,m}$ from a polynomial $f \in \mathcal{O}_K[X]$ with the necessary characteristics. As a result, the extensions $K_{\pi,m}/K$ are all finite and, hence, algebraic. For the remainder of this section, we will assume that f is such a polynomial, unless stated otherwise.

Example 2.1.4. (i) Take $K = \mathbf{Q}_p$, and consider the polynomial $f(X) = (1+X)^p - 1$. Then $f^{(m)}(X) = (1+X)^{p^m} - 1$, so its roots are of the form $\zeta_{p^m} - 1$ where ζ_{p^m} is a primitive p^m-th root of unity. Hence,

$$(\mathbf{Q}_p)_{p,m} = \mathbf{Q}_p(\zeta_{p^m}).$$

(ii) Take $K = \mathbf{Q}_p$, and consider the polynomials $f(X) = (1+X)^p - 1$ and $g(X) = X^p + pX$. The roots of g are the $(p-1)$-th roots of $-p$. Thus, by Proposition 2.1.3,

$$(\mathbf{Q}_p)_{p,1} = \mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p(\sqrt[p-1]{-p}).$$

Theorem 2.1.5. *For any m, the extension $K_{\pi,m}/K$ is totally ramified.*

Proof. Note that, since X divides f, we have that $f^{(m-1)}$ divides $f^{(m)}$; the polynomial $f^{(m)}/f^{(m-1)}$ will have leading coefficient 1 and all other coefficients in $\mathfrak{p}$, the constant term being π. This means that $f^{(m)}/f^{(m-1)}$ is an Eisenstein polynomial relative to $\mathfrak{p}$. Hence, the extension $K_{\pi,m} = K_{\pi,m-1}(\lambda_m)$ is totally ramified over $K_{\pi,m-1}$; and by induction, it is totally ramified over K. □

The next step would be to show that $K_{\pi,m}/K$ is a Galois extension.

Lemma 2.1.6. *For any $m \geqslant 1$, the extension $K_{\pi,m}/K$ is separable.*

Proof. Consider the polynomial $f(X) = X^q + \pi X$, then by definition

$$f^{(m)}(X) \equiv X^{q^m} \bmod \pi, \qquad\qquad f^{(m)}(X) \equiv \pi^m X \bmod X^2$$

This means that

$$f^{(m)}/f^{(m-1)}(X) = (f^{(m-1)}(X))^{q-1} + \pi \equiv \pi^{m-1}X^{q-1} + \pi \bmod X^q.$$

As a result, $f^{(m)}/f^{(m-1)}$ is not a polynomial in X^p, and hence it is separable if it is irreducible. We have irreducibility by Eisenstein's criterion, since $f^{(m)}/f^{(m-1)}$ is an Eisenstein polynomial in $\mathcal{O}_K$ relative to the ideal $\mathfrak{p}$, so the polynomial is separable, and so is the extension $K_{\pi,m}/K_{\pi,m-1}$, and hence $K_{\pi,m}/K$ by induction. □

In order to show that $K_{\pi,m}/K$ is Galois, it suffices now to show that all roots of $f^{(m)}$ lie in $K_{\pi,m}$. Here our knowledge of formal groups will be useful. Let $u \in \mathcal{O}_K^\times$ be a unit, then $[u]_f(\lambda_m)$ will be again an element of $K_{\pi,m}$; this follows since it is a power series on an element λ_m of the complete field $K_{\pi,m}$. Then, using repeatedly that $f \circ [u]_f = [u]_f \circ f$, we arrive at $f^{(m)}([u]_f(\lambda_m)) = [u]_f(f^{(m)}(\lambda_m)) = 0$, so $[u]_f(\lambda_m)$ is a root of $f^{(m)}$. We will be able to show that $K_{\pi,m}/K$ is Galois if changing the element u yields all remaining roots of $f^{(m)}$. In order to do this, we will need the following lemma.

Lemma 2.1.7. *Let $f(X)$ be a power series with coefficients in $\mathcal{O}_K$, and let L be a finite extension of K. Assume that there exists $\lambda \in L$ such that $f(\lambda) = 0$ and $|\lambda| < 1$. Then there exists a factorization $f(X) = (X - \lambda)g(X)$ where g is a power series over $\mathcal{O}_L$.*

Proof. (See [Haz75, p.168, Lemma 6.8].) Let f_n be the reduction of f modulo X^n. By division with remainder, we can write $f_n(X) = (X - \lambda)g_n + b_n$ for some $g_n \in \mathcal{O}_L[X]$ of degree smaller than n and $b_n \in \mathcal{O}_L$. Then $b_n = (f - f_n)(\lambda)$, so $|b_n| \leqslant |\lambda|^n$. Reducing f modulo X^{n+1} gives a polynomial g_{n+1} and an element b_{n+1} of norm lower than $|\lambda|^{n+1}$; thus, both b_n and b_{n+1} reduce to 0 modulo λ^n and, modulo the ideal (X^n, λ^n), we find that

$$(X - \lambda)(g_{n+1} - g_n)(X) \equiv 0 \bmod (X^n, \lambda^n).$$

Now, if we write

$$g_{n+1} - g_n = \sum_{i=0}^{n} a_i X^i,$$

the above congruence implies that

$$\begin{aligned} -\lambda a_0 \equiv 0 \bmod \lambda^n &\Rightarrow |a_0| \leqslant |\lambda|^{n-1} \\ a_0 - \lambda a_1 \equiv 0 \bmod \lambda^n &\Rightarrow |a_1| \leqslant \left|\lambda^{-1} a_0\right| \leqslant |\lambda|^{n-2} \\ &\cdots \\ a_{n-2} - \lambda a_{n-1} \equiv 0 \bmod \lambda^n &\Rightarrow |a_{n-1}| \leqslant |\lambda|^0 = 1. \end{aligned}$$

From this, we deduce that the sequence of g_n's converges to a power series g over $\mathcal{O}_L$ such that $g \equiv g_n \bmod (X^n, \lambda^n)$. Hence, $f(X) \equiv (X - \lambda) g(X) \bmod (X^n, \lambda^n)$ for all n, and thus we obtain equality. □

Theorem 2.1.8. *The extension $K_{\pi,m}/K$ is Galois, and its Galois group is isomorphic to $U_K/U_K^{(m)}$, where $U_K^{(m)}$ is the subgroup of U_K consisting of elements of the form $1+x$ with $x \in \mathfrak{p}^m$.*

Proof. (See [Haz75, p.169, Proposition 6.9].) Let $u \in U_K$; we begin by showing that, if u is such that $[u]_f$ fixes λ_m, then $u \in U_K^{(m)}$. Note that $f^{(r)}(\lambda_m)$, for $r \leqslant m$, is also fixed by $[u]_f$, as $f^{(r)} \circ [u]_f = [u]_f \circ f^{(r)}$. Moreover, any other root of $f^{(m)}$ is fixed as well: Such a root μ is given by $s(\lambda_r)$ for some $r \leqslant m$ and for a certain K-isomorphism $s : K(\lambda_r) \to K(\mu)$, and continuity of s together with the fact that $[u]_f(s(\lambda_r)) \equiv s([u]_f(\lambda_r)) \bmod \lambda_r^n$ for all n shows that $[u]_f(s(\lambda_r)) = s(\lambda_r)$. We can now apply Lemma 2.1.7 repeatedly to the power series $[u]_f(X) - X$ and all the roots of $f^{(m)}$: there exists then a power series g such that $[u]_f(X) - X = f^{(m)}(X) g(X)$. Let $a \in \mathcal{O}_{K_{\pi,m}}$ be the constant coefficient of g; then the coefficient of X on the right-hand side is $a\pi^m$, whereas the one for the left-hand side is $u - 1$. Therefore, since $|a| \geqslant 1$ and $u - 1 \in K$, we find that $u \in 1 + \mathfrak{p}^m = U_K^{(m)}$.

Extending the argument above, we see that, if $u_1, u_2 \in U_K$ are such that $[u_1]_f(\lambda_m) = [u_2]_f(\lambda_m)$, then $u_1 \equiv u_2$ in $U_K/U_K^{(m)}$: this follows since $[u_2^{-1} u_1]_f = [u_2]_f^{-1} \circ [u_1]_f$ fixes λ_m. So every element of $U_K/U_K^{(m)}$ determines a root of $f^{(m)}$; since $f^{(m)}$ has $q^{m-1}(q-1)$ roots, which is the number of elements of $U_K/U_K^{(m)}$, this group determines all the roots of $f^{(m)}$ and, thus, $K_{\pi,m}/K$ is Galois. Its Galois group becomes isomorphic to $U_K/U_K^{(m)}$ under the map sending $s \in \mathrm{Gal}(K_{\pi,m}/K)$ to the class of units u such that $s(\lambda_m) = [u]_f(\lambda_m)$. □

2.2 Associated norm subgroups

Having shown that the extensions $K_{\pi,m}/K$ are Galois and totally ramified, we set out to obtain more information from them. In particular, we will be interested in knowing what the image under the norm map of the filtration of unit groups $\left\{U_{K_{\pi,m}}^{(m)}\right\}$ looks like. We will actually show that $N_{K_{\pi,m}/K}(U_{K_{\pi,m}}^{(m)}) = U_K^{(m)}$, which we do in several steps.

Lemma 2.2.1. *Let k be a field, and let $g_0 = X^n + a_1X^{n-1} + \cdots + a_n$ be a polynomial over k such that n is coprime with the characteristic of k if this is non-zero. Then there exists an integer $r > 0$ and a polynomial $g \in k[X]$ of degree at most $r-1$ such that the polynomial $h = X^r g_0 + g$ is separable.*

Proof. (See [Haz75, p.164, Lemma 6.3].) We distinguish two cases. If k is infinite, then there must exist an element $c \in k$ such that the polynomial $Xg_0 + c$ does not share a common factor with $\frac{\mathrm{d}g_0}{\mathrm{d}X}$, since the derivative has only finitely many factors; we can then take $r = 1$ and $h = Xg_0 + c$.

Let us now assume that k is finite, of cardinality q. Since n is coprime with the characteristic of k, we have that $nX^{n-1} \neq 0$ in $k[X]$ and thus the derivative of g_0 is not the zero polynomial. Let $\alpha_1, \ldots, \alpha_{n-1}$ be the roots of $\frac{\mathrm{d}g_0}{\mathrm{d}X}$ inside an algebraic closure of k, and let k' be a finite extension of k containing the α_i's. Then k' has cardinality q^s for some s. Consider the polynomial $h = (X^{q^{s+1}} - X^q)g_0 + 1$. Its derivative is $\frac{\mathrm{d}h}{\mathrm{d}X} = (X^{q^{s+1}} - X^q)\frac{\mathrm{d}g_0}{\mathrm{d}X}$. We see that any α where the derivative of h vanishes cannot be a zero of h. For, if $\frac{\mathrm{d}g_0}{\mathrm{d}X}(\alpha) = 0$, then $\alpha = \alpha_i \in k'$ for some i and the relation $\alpha^{q^s} = \alpha$ must be satisfied; as a result, $\alpha^{q^{s+1}} = \alpha^q$ and thus $h(\alpha) = 1$. If, however, α is not a root of the derivative of g_0, then it must hold $\alpha^{q^{s+1}} = \alpha^q$ and again $h(\alpha) = 1$. Therefore h is separable. Finally, we remark that this procedure is valid for any k' containing the elements $\alpha_1, \ldots, \alpha_{n-1}$; choosing k' large enough so that $q^{s+1} - 1 \geqslant q + n$ allows us to set $r = q^{s+1}$ and $g = -X^q g_0 + 1$, which satisfy the desired conditions. □

Theorem 2.2.2. *Let K be a non-Archimedean local field, and let $K_{\pi,m}$ be its m-th Lubin-Tate extension. Then*

$$N_{K_{\pi,m}/K}(U^{(m)}_{K_{\pi,m}}) \subseteq U^{(m)}_K.$$

Proof. (See [Haz75, p.164, Theorem 6.5].) We begin by noting that, if u is a unit in $K_{\pi,m}$, then it can be expressed as a product $u'u''$ where $u' \in U^{(1)}_{K_{\pi,m}}$ and u'' is a $(q-1)$-th root of unity. This implies that, since all these roots of unity are contained in K,

$$N_{K_{\pi,m}/K}(u) = N_{K_{\pi,m}/K}(u')(u'')^{(q-1)q^{m-1}} = N_{K_{\pi,m}/K}(u'),$$

so it suffices to show that $N_{K_{\pi,m}/K}(U^{(1)}_{K_{\pi,m}})$ is contained in $U^{(m)}_K$. We may assume that $m \geqslant 2$, since the case $m = 1$ is clear.

Let now $u \in U^{(1)}_{K_{\pi,m}}$; we will denote $\lambda := \lambda_m$ for ease of notation. We know that λ is a uniformizer of $K_{\pi,m}$, since the condition $f(\lambda_m) = \lambda_{m-1}$ implies ultimately that π can be expressed in terms of λ, and with it every element of $\mathcal{O}_{K_{\pi,m}}$. As such, we can write u in terms of λ: After reducing u modulo $\mathfrak{p}^m$, we find that

$$u = 1 + a_1\lambda + a_2\lambda^2 + \cdots + a_n\lambda^n + x$$

where $|x| \leqslant |\pi|^m$ and $a_i \in \mathcal{O}_K$ for all $i = 1, \ldots, n$, and n is such that $n+1 = m(q-1)q^{m-1}$. The a_i's define the polynomial $d(X) = X^n + a_1 X^{n-1} + \cdots + a_n$; we denote by d' its reduction modulo $\mathfrak{p}$. Since $n+1$ is a multiple of q, the degree of d' is coprime to the characteristic of k, so by Lemma 2.2.1, there exists a number $r > 0$ and a polynomial $g' \in k[X]$ of degree at most $r-1$ such that the polynomial $h'(X) = X^r d'(X) + g'(X) \in k[X]$ is separable. Now let $g \in \mathcal{O}_K[X]$ be a lift of g', and let h be the polynomial $h(X) = X^r d(X) + g(X)$. We have that h reduces to h' modulo $\mathfrak{p}$; since h' is separable over k, by the correspondence between finite extensions of k and finite, unramified extensions of K, we deduce that all the roots of h lie in K^{nr}. We may choose the constant term of h to be equal to 1, as both r and g' can be chosen so that X does not divide h'; as a result, the product of the roots of h must be equal to ± 1, which in turn implies that all roots have unit norm and are therefore units of K^{nr}.

Let $z_1, \ldots, z_t \in U_{K^{\mathrm{nr}}}$ be these roots of h, where $t = n + r$; thus $h(X) = \prod_{i=1}^t (X - z_i)$. Evaluating h at $X = \lambda^{-1}$ gives

$$h(\lambda^{-1}) = \prod_{i=1}^t (\lambda^{-1} - z_i) = \lambda^{-t} \prod_{i=1}^t (1 - \lambda z_i)$$

so $\prod_{i=1}^t (1 - \lambda z_i) = \lambda^t (\lambda^{-r} d(\lambda^{-1}) + g(\lambda^{-1}))$. Since

$$\lambda^t \lambda^{-r} d(\lambda^{-1}) = \lambda^n (\lambda^{-n} + a_1 \lambda^{-n+1} + \cdots + a_n) = 1 + a_1 \lambda + \cdots + a_n \lambda^n,$$

we find that $\prod_{i=1}^t (1 - \lambda z_i) = 1 + a_1 \lambda + \cdots + a_n \lambda^n + x'$ where $x' = \lambda^t g(\lambda^{-1})$. The element x' has the property that $|x'| = |\lambda|^t \, |g(\lambda^{-1})| \leqslant |\lambda|^t \, |\lambda|^{-r+1} = |\lambda|^{n+1} = |\pi|^m$. As a result, we may write

$$u = (1 + a_1 \lambda + \cdots + a_n \lambda^n + x') + (x - x') = (1 + y) \prod_{i=1}^t (1 - \lambda z_i)$$

where $|y| = |x - x'| \leqslant |\pi|^m$. Thus, $N_{K_{\pi,m}/K}(1 + y) \in U_K^{(m)}$.

To see that $N_{K_{\pi,m}/K}(u) \in U_K^{(m)}$, it now suffices to show that $N_{K_{\pi,m}/K}(\prod_{i=1}^t (1 - \lambda z_i)) \in U_K^{(m)}$. In order to do this, we claim it is enough to show that $N_{K_{\pi,m} \cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(\prod_{i=1}^t (1 - \lambda z_i)) \in U_{K^{\mathrm{nr}}}^{(m)}$. To see why, note that $U_K^{(m)} = U_{K^{\mathrm{nr}}}^{(m)} \cap U_K$, since K^{nr}/K is an unramified extension, and we already know that $N_{K_{\pi,m}/K}(\prod_{i=1}^t (1 - \lambda z_i)) \in U_K$. Moreover, the norm maps $N_{K_{\pi,m}/K}$ and $N_{K_{\pi,m} \cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}$ are equal when restricted to $K_{\pi,m}$: Any element in $K_{\pi,m}$ has the same minimum polynomial over K and over K^{nr}, since $K_{\pi,m}/K$ is totally ramified but K^{nr}/K is unramified. These two facts together justify our claim.

Now, to compute $N_{K_{\pi,m} \cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(1 - \lambda z_i)$, we use that the minimum polynomial of λ over

K^{nr} is also $f^{(m)}(X)/f^{(m-1)}(X)$; using that

$$N_{K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(a+b\lambda) = (-b)^{[K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}]}\frac{f^{(m)}(-a/b)}{f^{(m-1)}(-a/b)},$$

we see that

$$N_{K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(1-\lambda z_i) = N_{K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(z_i)N_{K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}(z_i^{-1}-\lambda) = z_i^{(q-1)q^{m-1}}\frac{f^{(m)}(z_i^{-1})}{f^{(m-1)}(z_i^{-1})}$$

and therefore, using that $(q-1)q^{m-1}$ is even since $m \geqslant 2$,

$$\begin{aligned} N_{K_{\pi,m}\cdot K^{\mathrm{nr}}/K^{\mathrm{nr}}}\left(\prod_{i=1}^{t}(1-\lambda z_i)\right) &= \left(\prod_{i=1}^{t} z_i\right)^{(q-1)q^{m-1}} \prod_{i=1}^{t}\frac{f^{(m)}(z_i^{-1})}{f^{(m-1)}(z_i^{-1})} \\ &= (\pm 1)^{(q-1)q^{m-1}}\frac{\prod_{i=1}^{t} f^{(m)}(z_i^{-1})}{\prod_{i=1}^{t} f^{(m-1)}(z_i^{-1})} \\ &= 1 + \frac{\prod_{i=1}^{t} f^{(m)}(z_i^{-1}) - \prod_{i=1}^{t} f^{(m-1)}(z_i^{-1})}{\prod_{i=1}^{t} f^{(m-1)}(z_i^{-1})}. \end{aligned}$$

Thus, it suffices to see that

$$\left|\frac{\prod f^{(m)}(z_i^{-1}) - \prod f^{(m-1)}(z_i^{-1})}{\prod f^{(m-1)}(z_i^{-1})}\right| \leqslant |\pi|^m.$$

We know that $z_i \in U_{K^{\mathrm{nr}}}$ for all i, so z_i^{-1} is also a unit and, since $f \equiv X^q \bmod \pi$, we find that $f(z_i^{-1})$ is also a unit in K^{nr}; from this we are able to deduce that $f^{(m-1)}(z_i^{-1}) \in U_{K^{\mathrm{nr}}}$. So we are done if we show that $\left|\prod f^{(m)}(z_i^{-1}) - \prod f^{(m-1)}(z_i^{-1})\right| \leqslant |\pi|^m$.

We note the following: Modulo $\mathfrak{p}$, the map $z \to f(z)$ acts like the Frobenius automorphism in $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ modulo $\mathfrak{p}$. Since the Frobenius automorphism must permute the roots of h, and therefore also its inverses, we see that $f(z_i^{-1}) \equiv z_j^{-1}$ modulo $\mathfrak{p}$ for some $j \in 1,\ldots,t$. To extend this to a relation between $f^{(m)}(z_i^{-1})$ and $f^{(m-1)}(z_j^{-1})$, we note that, for arbitrary $a, b \in \mathcal{O}_{K^{\mathrm{nr}}}$, if $a \equiv b \bmod \pi^s$ for some $s \geqslant 1$, then $a^q \equiv b^q \bmod \pi^{s+1}$, since

$$|a^q - b^q| = |a-b|\left|a^{q-1} + a^{q-2}b + \cdots + b^{q-1}\right| \leqslant |\pi|^s\,|\pi| = |\pi|^{s+1}$$

as $a^{-1} \equiv a^{-2}b \equiv \cdots \equiv b^{q-1}$ and thus $a^{q-1} + a^{q-2}b + \cdots + b^{q-1} \equiv qa^{-1} \equiv 0$ modulo π^s. As a result, we have that $f(a) \equiv f(b) \bmod \pi^{s+1}$; returning to the z_i's and applying f multiple times, we find that $f^{(m)}(z_i^{-1}) \equiv f^{(m-1)}(z_j^{-1}) \bmod \mathfrak{p}^m$. Finally, because the assignment $i \mapsto j$ is a permutation, thus bijective, we find that

$$\prod_{i=1}^{t} f^{(m)}(z_i^{-1}) \equiv \prod_{i=1}^{t} f^{(m-1)}(z_i^{-1}) \bmod \pi^m,$$

which finishes the proof. □

Corollary 2.2.3. *Let K be a non-Archimedean local field, and let $K_{\pi,m}$ be its m-th Lubin-Tate extension. Then*

$$N_{K_{\pi,m}/K}(U_{K_{\pi,m}}) = U_K^{(m)}.$$

Proof. (See [Haz75, p.169, Corollary 6.10].) We have that $U_K/N_{K_{\pi,m}/K}(U_{K_{\pi,m}}) \cong \mathrm{Gal}(K_{\pi,m}/K)$; on the other hand, by Theorem 2.1.8 we know that $\mathrm{Gal}(K_{\pi,m}/K) \cong U_K/U_K^{(m)}$. Adding now that Theorem 2.2.2 shows that $N_{K_{\pi,m}/K}(U_{K_{\pi,m}}) \subseteq U_K^{(m)}$ we conclude that the two groups must be equal. □

Corollary 2.2.4. *The image of $K_{\pi,m}^{\times}$ under the norm map $N_{K_{\pi,m}/K}$ equals $\langle\pi\rangle \times U_K^{(m)}$.*

Proof. We know from Corollary 2.2.3 that $N_{K_{\pi,m}/K}(U_{K_{\pi,m}}) = U_K^{(m)}$, so it suffices to show that there is a prime element of $K_{\pi,m}$ that is mapped to π under the norm map. For this, take a root λ_m of $f^{(m)}$ that is not a root of $f^{(m-1)}$. Then λ_m is a root of the irreducible polynomial $f^{(m)}/f^{(m-1)}$, which has constant term equal to π. Hence, $N_{K_{\pi,m}/K}(\lambda_m) = (-1)^{q-1}\pi$. Considering that the minimum polynomial of $-\lambda_m$ is $f^{(m)}/f^{(m-1)}$ but where the coefficients of odd degree have switched signs, we deduce that $N_{K_{\pi,m}/K}(-\lambda_m) = \pi$. □

3 The reciprocity law

The aim of this chapter is to compute explicitly the reciprocity map from local class field theory. To do this, we will find a map from the multiplicative group of a non-Archimedean local field K to the Galois field of a composite extension —namely, of the compositum of maximal unramified and totally ramified extensions of K—, and we will give its complete description. This, by itself, will not be enough to establish that we have found the reciprocity map, as we will still need the local Kronecker-Weber theorem for K, to be discussed later. Nevertheless, the treatment of the topic in this chapter includes all the remaining ingredients. This chapter is based on the treatments of Lang [Lan90, Chap.8, §2–4] and Iwasawa [Iwa86, Chap.4, §2–3].

3.1 The Lubin-Tate extension associated to π

Let π be a uniformizer of K, let $f(X) = X^q + \pi X$ and let F_f be its associated Lubin-Tate formal group. For $m \geqslant 1$, let $K_{\pi,m}/K$ be the Lubin-Tate extension of degree $(q-1)q^{m-1}$ associated to π. Recall that $K_{\pi,m}$ is an Abelian, totally ramified extension, generated over K by the roots of $f^{(m)}$. Since $f^{(m)}$ divides $f^{(m')}$ for all $m \leqslant m'$, we have $K_{\pi,m} \subseteq K_{\pi,m'}$ for all $m \leqslant m'$.

We fix a separable closure K^{sep} of K. Recall that, in the setting of formal Lubin-Tate modules, the maximal ideal $\mathfrak{m}_{K^{\text{sep}}}$ of K^{sep} is equipped with the formal $\mathcal{O}_K$-module structure given by

$$x +_f y := F(x,y), \qquad a \cdot_f x := [a]_f(x)$$

for $x, y \in \mathfrak{m}_{K^{\text{sep}}}$ and $a \in \mathcal{O}_K$.) In this context, the roots of $f^{(m)} = [\pi^m]_f$ can be seen as the π^m-torsion elements inside $\mathfrak{m}_{K^{\text{sep}}}$. We denote this set of torsion points by $\mathfrak{m}_{K^{\text{sep}}}[\pi^m]$. Since, for every $\lambda_{m+1} \in \mathfrak{m}_{K^{\text{sep}}}[\pi^{m+1}]$, we have that $f(\lambda_{m+1})$ is a zero of $f^{(m)}$, the polynomial f induces maps $\mathfrak{m}_{K^{\text{sep}}}[\pi^{m+1}] \to \mathfrak{m}_{K^{\text{sep}}}[\pi^m]$ sending $\lambda \in \mathfrak{m}_{K^{\text{sep}}}[\pi^{m+1}]$ to $f(\lambda)$. Taking the inverse limit, we define the **Tate module** as

$$T_\pi(\mathfrak{m}_{K^{\text{sep}}}) = \varprojlim_m \mathfrak{m}_{K^{\text{sep}}}[\pi^m].$$

The extension

$$K_\pi := \bigcup_{m \geqslant 1} K_{\pi,m},$$

is an Abelian, totally ramified extension of K which we call the **Lubin-Tate extension of K associated to π**. Since the extension $K_{\pi,m}/K$ has Galois group $\mathrm{Gal}(K_{\pi,m}/K) \cong U_K/U_K^{(m)}$ (see Theorem 2.1.8), we deduce that

$$\mathrm{Gal}(K_\pi/K) = \varprojlim_m U_K/U_K^{(m)} \cong U_K = \mathcal{O}_K^\times.$$

We will later see that this totally ramified extension K_π/K is *maximal*, in the sense that there are no non-trivial, totally ramified extensions of K_π. For the remaining of this chapter, we will study the interplay of this extension K_π with the maximal unramified extension K^{nr} of K. We recall the way K^{nr} was constructed. For every finite, separable field extension L/K, it can be shown that there exists a unique unramified extension $K \subseteq T \subseteq L$ such that the residue field of T equals the residue field of L. This establishes a bijection between the set of finite, unramified extensions of K and the set of finite extensions of $k = \mathbf{F}_q$, so the unique extension of degree n of $\mathbf{F}_q$ corresponds to an unramified extension K_n/K of degree n. Now, the group of units of $\mathbf{F}_{q^n}$ is generated by a primitive (q^n-1)-th root of unity, with minimal polynomial $\bar{g}$ a factor of the cyclotomic polynomial $(\Phi_{q^n-1} \bmod p)$. Since $q^n - 1$ is not divisible by p, we see that $(\Phi_{q^n-1} \bmod p)$ is separable and, hence, the polynomial $\bar{g}$ lifts, by Hensel's lemma, to a factor g of Φ_{q^n-1}. The extension K_n/K is thus generated by a root of f, that is, a primitive (q^n-1)-th root of unity. As a result, we have that

$$K^{\mathrm{nr}} = \bigcup_{p \nmid m} K(\zeta_m)$$

where ζ_m is a primitive m-th root of unity. The Galois group $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ is isomorphic to $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$, which in turn is the inverse limit of the groups $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong (\mathbf{Z}/n\mathbf{Z})$. This limit equals the (additive) **group of profinite integers $\widehat{\mathbf{Z}}$**, a topological group which contains $\mathbf{Z}$ as a dense subgroup and is topologically generated by the Frobenius automorphism of $\overline{\mathbf{F}_q}$.

Example 3.1.1. Let $K = \mathbf{Q}_p$. Then its maximal unramified extension is $(\mathbf{Q}_p)^{\mathrm{nr}} = \bigcup_{p \nmid m} \mathbf{Q}_p(\zeta_m)$. On the other hand, since its m-th Lubin-Tate extension associated to the prime p is $(\mathbf{Q}_p)_{p,m} = \mathbf{Q}_p(\zeta_{p^m})$ (see Example 2.1.4(i)), we have that $(\mathbf{Q}_p)_p = \bigcup_{m \geqslant 1} \mathbf{Q}_p(\zeta_{p^m})$. As a consequence of this,

$$(\mathbf{Q}_p)^{\mathrm{nr}} \cdot (\mathbf{Q}_p)_p = \mathbf{Q}_p(\zeta_\infty) = \bigcup_{n \geqslant 1} \mathbf{Q}_p(\zeta_n).$$

To see why, write $n = p^r m$ with $p \nmid m$; then ζ_n will lie in any field containing ζ_{p^r} and ζ_m. In particular $\zeta_n \in \mathbf{Q}_p(\zeta_{p^r}) \cdot \mathbf{Q}_p(\zeta_m) = (\mathbf{Q}_p)_{p,r} \cdot (\mathbf{Q}_p)_m^{\mathrm{nr}}$, where $(\mathbf{Q}_p)_m^{\mathrm{nr}}$ denotes the unramified extension of $\mathbf{Q}_p$ of degree m. As a result, $\mathbf{Q}_p(\zeta_n) = (\mathbf{Q}_p)_{p,r} \cdot (\mathbf{Q}_p)_m^{\mathrm{nr}}$.

Showing that the compositum $(\mathbf{Q}_p)^{\mathrm{nr}} \cdot (\mathbf{Q}_p)_p$ is related to the Abelian closure of $\mathbf{Q}_p$ is the goal of Chapter 4.

3.2 Changing the prime

As discussed in the previous section, since $K_{\pi,m}$ does not depend on f, neither will K_π. However, as the notation suggests, K_π will in principle depend on the choice of uniformizer. We would still like for these extensions to be somehow related, and we will be able to see this by examining their associated formal groups. This will later on be of value, as it will also allow us to show that the reciprocity map we find is well-defined.

Throughout this section, K^{nr} denotes the maximal unramified extension of K, $\widehat{K^{\mathrm{nr}}}$ its completion, and ϕ denotes the Frobenius automorphism of K^{nr} and $\widehat{K^{\mathrm{nr}}}$. Given a power series $\theta(X) = \sum a_n X^n \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$, we denote by θ^ϕ the power series $\theta^\phi(X) = \sum \phi(a_n) X^n$.

Lemma 3.2.1. *The homomorphism*

$$\begin{aligned} \phi \cdot \mathrm{inv} : \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}} &\to \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}} \\ a &\mapsto \phi(a) a^{-1} \end{aligned}$$

is surjective, and its kernel is $\mathcal{O}_K^\times$.

Proof. (See [Haz75, p.159, Lemma 5.2(i)].) We prove this result by passing to the filtration

$$\mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}} = U_{\widehat{K^{\mathrm{nr}}}} \supseteq U^{(1)}_{\widehat{K^{\mathrm{nr}}}} \supseteq \cdots \supseteq U^{(m)}_{\widehat{K^{\mathrm{nr}}}} \supseteq \cdots$$

where $U^{(m)}_{\widehat{K^{\mathrm{nr}}}} = 1 + \mathfrak{m}^m_{\widehat{K^{\mathrm{nr}}}}$. Then the quotients $U_{\widehat{K^{\mathrm{nr}}}}/U^{(1)}_{\widehat{K^{\mathrm{nr}}}}$ and $U^{(m)}_{\widehat{K^{\mathrm{nr}}}}/U^{(m+1)}_{\widehat{K^{\mathrm{nr}}}}$ are isomorphic to $\overline{k}^\times$ and $\overline{k}$, where $\overline{k}$ is the algebraic closure of the residue field k of K. The maps induced by $\phi \cdot \mathrm{inv}$ over the quotients become now

$$\begin{aligned} \overline{k}^\times &\to \overline{k}^\times & \qquad \overline{k} &\to \overline{k} \\ x &\mapsto x^{q-1} & \qquad x &\mapsto x^q - x \end{aligned}$$

since $\phi(x) \equiv x^q \bmod \mathfrak{m}_{\widehat{K^{\mathrm{nr}}}}$. The field $\overline{k}$ is algebraically closed, so for every $a \in \overline{k}$ the equations $x^{q-1} = a$ and $x^q - x = a$ have a solution, and so the maps are surjective.

Take now $u \in U_{\widehat{K^{\mathrm{nr}}}}$. Since the maps on the quotients are surjective, there exists $v \in U_{\widehat{K^{\mathrm{nr}}}}$

such that $\phi(v)v^{-1} \equiv u \bmod U^{(1)}_{\widehat{K^{\mathrm{nr}}}}$. So $u = \phi(v)v^{-1}u_1$ for some $u_1 \in U^{(1)}_{\widehat{K^{\mathrm{nr}}}}$. Similarly, there exist $v_1 \in U^{(1)}_{\widehat{K^{\mathrm{nr}}}}$ and $u_2 \in U^{(2)}_{\widehat{K^{\mathrm{nr}}}}$ such that $u_1 = \phi(v_1)v_1^{-1}u_2$. This gives sequences of elements v_m and u_m such that $u_m, v_m \in U^{(m)}_{\widehat{K^{\mathrm{nr}}}}$ and $u_m = \phi(v_m)v_m^{-1}u_{m+1}$ for all $m \geqslant 1$. Take the partial products $\hat{v}_m = \prod_{i=1}^{m} v_i$, then writing $v_{m+1} = 1 + \pi^{m+1}a$ we find

$$|\hat{v}_m - \hat{v}_{m+1}| = |\hat{v}_m| \left|1 - (1 + \pi^{m+1}a)\right| \leqslant |\pi|^{m+1},$$

so the sequences of products converge and thus $u = (\phi \cdot \mathrm{inv})(v \prod_{m=1}^{\infty} v_m)$, so $\phi \cdot \mathrm{inv}$ is surjective. □

We set out now to explore consequences of Lemma 1.2.2 regarding the use of different uniformizers of K. As we did back then, we consider the general setting where the uniformizers are taken in $\widehat{K^{\mathrm{nr}}}$.

Proposition 3.2.2. *Let π and π' be two uniformizers of $\widehat{K^{\mathrm{nr}}}$, and let f and g be polynomials of degree q such that*

$$f(X) \equiv g(X) \equiv X^q \bmod \pi \qquad f(X) \equiv \pi X \bmod (X^2) \qquad g(X) \equiv \pi' X \bmod (X^2).$$

Let F_f and F_g denote the Lubin-Tate formal groups associated to f and g respectively. Then there exists a formal series $\theta \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ and an element $\epsilon \in \mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}}$ such that

(i) $\theta \equiv \epsilon X \bmod (X^2)$;

(ii) $g \circ \theta = \theta^{\phi} \circ f$;

(iii) *θ defines an isomorphism of formal groups $F_f \to F_g$, that is, $\theta(F_f(X, Y)) = F_g(\theta(X), \theta(Y))$;*

(iv) *for all $a \in \mathcal{O}_K$, $\theta \circ [a]_f = [a]_g \circ \theta$;*

(v) *suppose that $\pi \in K$ and $\pi' \in K_n^{\mathrm{nr}}$, the unramified extension of K of degree n, and $f \in \mathcal{O}_K[[X]]$ and $g \in \mathcal{O}_{K_n^{\mathrm{nr}}}[[X]]$; then*

$$\theta^{\phi^n} = \theta \circ [u]_f,$$

where $u \in U_K$ is such that $N_{K_n^{\mathrm{nr}}/K}(\pi') = u\pi^n$.

Proof. (See [Lan90, p.201, Theorem 3.1] and [Iwa86, p.56, Proposition 4.5 and p.77, Lemma 5.14].) By Lemma 3.2.1 the map $\phi \cdot \mathrm{inv} : \mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}} \to \mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}}$ is surjective, hence there exists a unit $\epsilon \in \mathcal{O}^{\times}_{\widehat{K^{\mathrm{nr}}}}$ such that $\phi(\epsilon)\epsilon^{-1} = \pi'/\pi$. Hence $\phi(\epsilon)\pi = \epsilon\pi'$, so the linear form $L(X) = \epsilon X$ fulfills the conditions of 1.2.2 (after changing the roles of π and π'). As a result, there exists a unique power series $\theta \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ satisfying (i) and (ii). To see (iii), we compare the actions of $\theta \circ F_f$ and $F_g \circ \theta$: They are both congruent to $\epsilon X + \epsilon Y$ modulo

$(X,Y)^2$ by (i), and applying (ii) and Theorem 1.2.3 gives

$$g \circ (\theta \circ F_f) = \theta^\phi \circ f \circ F_f = \theta^\phi \circ F_f^\phi \circ f = (\theta \circ F_f)^\phi \circ f$$
$$g \circ (F_g \circ \theta) = F_g^\phi \circ g \circ \theta = F_g^\phi \circ \theta^\phi \circ f = (F_g \circ \theta)^\phi \circ f.$$

Both $\theta \circ F_f$ and $F_g \circ \theta$ fulfill the conditions of Lemma 1.2.2, so by uniqueness they must be the same, thus proving (iii). It can be shown analogously that (iv) holds: Both $\theta \circ [a]_f$ and $[a]_g \circ \theta$ are congruent to $a\epsilon X + a\epsilon Y$ modulo $(X,Y)^2$, and Theorem 1.2.6 implies

$$g \circ (\theta \circ [a]_f) = (\theta \circ [a]_f)^\phi \circ f$$
$$g \circ ([a]_g \circ \theta) = ([a]_f \circ \theta)^\phi \circ f,$$

so uniqueness shows (iv).

For (v), suppose that $\pi \in K$ and $\pi' \in K_n^{\mathrm{nr}}$ and that f and g have coefficients in these fields respectively. For any $m \geqslant 1$, let $f^{(m)}$ and $g^{(m)}$ be as in Definition 2.1.1, i.e.

$$g^{(1)} = g, \qquad\qquad g^{(m+1)} = g^{\phi^m} \circ g^{(m)} \text{ for } m > 1$$

and $f^{(m)} = f \circ f \circ \cdots \circ f$. We show by induction that

$$g^{(m)} \circ \theta = \theta^{\phi^m} \circ f^{(m)} \text{ for all } m \geqslant 1 : \tag{3.2.1}$$

The case $m = 1$ is done by (ii), and assuming the induction hypothesis for some m,

$$\begin{aligned} g^{(m+1)} \circ \theta &= g^{\phi^m} \circ g \circ \theta = g^{\phi^m} \circ \theta^{\phi^m} \circ f^{(m)} = (g \circ \theta)^{\phi^m} \circ f^{(m)} \\ &= (\theta^\phi \circ f)^{\phi^m} \circ f^{(m)} = \theta^{\phi^{m+1}} \circ f \circ f^{(m)} \\ &= \theta^{\phi^{m+1}} \circ f^{(m+1)}. \end{aligned}$$

Now, by definition,

$$g^{(n)} \equiv \phi^{m-1}(\pi') \cdots \phi(\pi')\pi' X = N_{K_n^{\mathrm{nr}}/K}(\pi') X \bmod X^2.$$

On the other hand, g has coefficients on K_n^{nr}, so $g^{\phi^n} = g$. As a result,

$$\begin{aligned} g \circ g^{(n)} &= g^{\phi^n} \circ g^{(n)} = g^{(n+1)} \\ &= g^{\phi^n} \circ g^{\phi^{n-1}} \circ \cdots g^\phi \circ g = (g^{\phi^{n-1}} \circ \cdots \circ g)^\phi \circ g \\ &= (g^{(n)})^\phi \circ g. \end{aligned}$$

By uniqueness in Theorem 1.2.6, it must hold true that

$$g^{(n)} = [N_{K_n^{\mathrm{nr}}/K}(\pi')]_g = [u]_g \circ [\pi]_g^n.$$

Hence, since $f = [\pi]_f$,

$$g^{(n)} \circ \theta = [u\pi^n]_g \circ \theta = \theta \circ [u]_f \circ [\pi]_f^n = \theta \circ [u]_f \circ f^{(n)},$$

and this is in turn equal to $\theta^{\phi^n} \circ f^{(n)}$ by Equation (3.2.1), so

$$(\theta^{\phi^n} - \theta \circ [u]_f) \circ f^{(n)} = 0. \tag{3.2.2}$$

It remains to show that this implies (v). We claim the following: If a power series $h \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ is such that $h \circ f \equiv 0 \bmod \pi^m$ for $m \geqslant 1$, then $h \equiv 0 \bmod \pi^m$. We prove the claim by induction. Modulo π, we have that $f \equiv X^q$, so $h(X^q) \equiv 0$ implies $h \equiv 0 \bmod \pi$; this covers the case $m = 1$. Assuming the claim holds for some m, suppose $h \circ f \equiv 0 \bmod \pi^{m+1}$. In particular, $h \circ f \equiv 0 \bmod \pi^m$, so by the induction hypothesis we have $h = \pi^m h_1$ with $h_1 \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$. Then $\pi^m h_1 \circ f \equiv 0 \bmod \pi^{m+1}$, or equivalently, $h_1 \circ f \equiv 0 \bmod \pi$. By the case $m = 1$, we have $h_1 \equiv 0 \bmod \pi$, and thus $h \equiv 0 \bmod \pi^{m+1}$. This proves the claim. As a consequence, if $h \circ f = 0$, then $h = 0$; going back to Equation (3.2.2), we see that this implies that $\theta^{\phi^n} = \theta \circ [u]_f$, completing the proof. □

3.3 The reciprocity map, modulo local Kronecker-Weber

We return to the notation at the beginning of the chapter, where K_π denotes the Lubin-Tate extension associated to the uniformizer π of K, generated by the π^m-torsion points $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$. In order to better understand the structure of the Tate module $T_\pi(\mathfrak{m}_{K^{\mathrm{sep}}})$, we focus first on the π^m-torsion sets.

Let $x \in \mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$, and consider the map

$$\begin{aligned} \mathcal{O}_K &\to \mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m] \\ a &\mapsto [a]_f(x). \end{aligned}$$

The above map is a well-defined $\mathcal{O}_K$-module homomorphism, since $[\pi^m]_f \circ [a]_f = [a]_f \circ [\pi^m]_f$ by (ii). It has kernel $(\pi)^m$; both $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$ and $\mathcal{O}_K/(\pi)^m$ have q^m elements, so the injective map $\mathcal{O}_K/(\pi)^m \to \mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$ is an isomorphism. Hence, $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$ is a

free $\mathcal{O}_K/(\pi)^m$-module of rank 1, so $\mathrm{End}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]) \cong \mathcal{O}_K/(\pi)^m$ and $\mathrm{Aut}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]) \cong (\mathcal{O}_K/(\pi)^m)^\times$.

Moreover, we have that $\mathrm{Gal}(K_{\pi,m}/K)$ acts on $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$, since for $\sigma \in \mathrm{Gal}(K_{\pi,m}/K)$ we have $\sigma \circ [\pi]_f = [\pi]_f \circ \sigma$ as $[\pi]_f = f$ has coefficients in $\mathcal{O}_K$. Thus, we obtain a representation

$$\mathrm{Gal}(K_{\pi,m}/K) \to \mathrm{Aut}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]) \cong (\mathcal{O}_K/(\pi)^m)^\times \cong U_K/U_K^{(m)}.$$

The map $\mathrm{Gal}(K_{\pi,m}/K) \to \mathrm{Aut}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m])$ is injective: The extension $K_{\pi,m}/K$ is generated over K by some torsion element $\lambda \in \mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$, so two different elements of the Galois group of $K_{\pi,m}/K$ must map λ to different elements of $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$, and hence give rise to different elements of the automorphism group of the torsion points. Counting cardinalities, we see the injectivity of $\mathrm{Gal}(K_{\pi,m}/K) \to U_K/U_K^{(m)}$ implies bijectivity, so this representation is actually an isomorphism. Note that we have just re-derived Theorem 2.1.8 in a new way, replacing explicit computations by a more clever argument using our knowledge of the π^m-torsion.

If we now pass to the limit, we find that $T_\pi(\mathfrak{m}_{K^{\mathrm{sep}}}) \cong \mathcal{O}_K$ is a free $\mathcal{O}_K$-module of rank 1, whereas the isomorphisms $\mathrm{Gal}(K_{\pi,m}/K) \to (\mathcal{O}_K/(\pi)^m)^\times$ induce at the limit an isomorphism $\mathrm{Gal}(K_\pi/K) \cong \mathcal{O}_K^\times$. To see how this isomorphism behaves, it is useful to look back on the explicit computations of Theorem 2.1.8. For $\sigma \in \mathrm{Gal}(K_\pi/K)$, its restriction to $K_{\pi,m}$ corresponds, according to 2.1.8, to the unit $u \in U_K/U_K^{(m)}$ such that $\sigma = [u]_f$ over $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$. By the inverse limit construction, the isomorphism $\mathrm{Gal}(K_\pi/K) \to \mathcal{O}_K^\times \cong U_K$ maps σ to the unit u such that $\sigma = [u]_f$. As it turns out, it will be more convenient for us to choose another isomorphism, namely by inverting the image of the original one: it will send σ to the unit u such that $\sigma = [u]_f^{-1}$.

Now, let K^{nr} be the maximal unramified extension of K, and consider the compositum $K^{\mathrm{nr}} \cdot K_\pi$. We will later see that this compositum equals K^{Ab}, the Abelian closure of K, which justifies studying the Galois group $\mathrm{Gal}(K^{\mathrm{nr}} \cdot K_\pi/K)$. For this, we will use our knowledge of the Galois groups of K^{nr} and K_π separately. The way to do this is via what we will later call the **reciprocity map**.

Proposition 3.3.1. *The field $K^{\mathrm{nr}} \cdot K_\pi$ is independent of the choice of π.*

Proof. (See [Lan90, p.203, Theorem 4.1] and [Iwa86, p.65, Lemma 5.1(ii)].) Let π' be another uniformizer of K, and let f and g be such that $f \equiv g \equiv X^q \bmod \pi$, $f \equiv \pi X \bmod X^2$ and $g \equiv \pi' X \bmod X^2$. Let F_f and F_g be the Lubin-Tate formal groups associated to f and g respectively, then Theorem 3.2.2 shows that there exists a power series $\theta \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ defining an isomorphism $\theta : F_f \to F_g$. Since $\theta \circ [a]_f = [a]_g \circ \theta$ by (iv), we actually have that θ is an isomorphism of $\mathcal{O}_K$-modules $(\mathfrak{m}_{K^{\mathrm{sep}}}, +_{F_f}, \cdot_{F_f}) \to$

$(\mathfrak{m}_{K^{\mathrm{sep}}}, +_{F_g}, \cdot_{F_g})$. In particular, θ induces an isomorphism of Tate modules $\theta : T_\pi(\mathfrak{m}_{K^{\mathrm{sep}}}) \to T_{\pi'}(\mathfrak{m}_{K^{\mathrm{sep}}})$.

We claim that $\widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m} = \widehat{K^{\mathrm{nr}}} \cdot K_{\pi',m}$ for all $m \geqslant 1$. As $\widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m} = \widehat{K^{\mathrm{nr}}}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m])$, these are both finite extensions of $\widehat{K^{\mathrm{nr}}}$, hence complete. Since θ has coefficients in $\widehat{K^{\mathrm{nr}}}$, then $\theta(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]) \subseteq \widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m}$. Being θ an isomorphism of the two torsion modules, this implies that $\widehat{K^{\mathrm{nr}}}(\mathfrak{m}_{K^{\mathrm{sep}}}[\pi'^m]) \subseteq \widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m}$, hence $\widehat{K^{\mathrm{nr}}} \cdot K_{\pi',m} \subseteq \widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m}$. Going in the other direction with θ^{-1} we obtain the other containment. This proves the claim.

Now, consider the extension $K^{\mathrm{nr}} \cdot K_{\pi,m}/K^{\mathrm{nr}}$. It is finite and Galois, and its completion $\widehat{K^{\mathrm{nr}} \cdot K_{\pi,m}}$ must be its closure inside the completion of K^{sep} with respect to the topology induced by the norm. The field $\widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m}$ is complete, hence closed in the completion of K^{sep}, and it contains $K^{\mathrm{nr}} \cdot K_{\pi,m}$, therefore it also contains $\widehat{K^{\mathrm{nr}} \cdot K_{\pi,m}}$. Since both $\widehat{K^{\mathrm{nr}}}$ and $K_{\pi,m}$ must be contained in $\widehat{K^{\mathrm{nr}} \cdot K_{\pi,m}}$, the other containment follows. Thus $\widehat{K^{\mathrm{nr}}} \cdot K_{\pi,m}$ is the completion of $K^{\mathrm{nr}} \cdot K_{\pi,m}$, and by the above argument it is also that of $K^{\mathrm{nr}} \cdot K_{\pi',m}$.

Consider the compositum $L := K^{\mathrm{nr}} \cdot K_{\pi,m} \cdot K_{\pi',m}$. It is a finite Galois extension over $K^{\mathrm{nr}} \cdot K_{\pi,m}$ and $K^{\mathrm{nr}} \cdot K_{\pi',m}$. Seen as an extension over the former, we find that

$$(\widehat{K^{\mathrm{nr}} \cdot K_{\pi,m}}) \cap L = K^{\mathrm{nr}} \cdot K_{\pi,m}$$

since $L/K^{\mathrm{nr}} \cdot K_{\pi,m}$ is Galois. We also find

$$(\widehat{K^{\mathrm{nr}} \cdot K_{\pi',m}}) \cap L = K^{\mathrm{nr}} \cdot K_{\pi',m}$$

in an analogous manner. The left-hand sides of both expressions are the same as argued before, so $K^{\mathrm{nr}} \cdot K_{\pi,m} = K^{\mathrm{nr}} \cdot K_{\pi',m}$. This equality is true for all $m \geqslant 1$; as a result, $K^{\mathrm{nr}} \cdot K_\pi = K^{\mathrm{nr}} \cdot K_{\pi'}$, proving the result. □

Theorem 3.3.2. *Let π be a prime of K. Given $a \in K^\times$, we write $a = u\pi^n$ for some $u \in \mathcal{O}_K^\times$ and some integer n. We define the map $\rho_{K,\pi} : K^\times \to \mathrm{Gal}(K^{\mathrm{nr}} \cdot K_\pi/K)$ as*

$$\rho_{K,\pi}(a)|_{K_\pi} = \sigma_u \text{ where } \sigma_u = [u^{-1}]_f \in \mathrm{Gal}(K_\pi/K)$$
$$\rho_{K,\pi}(a)|_{K^{\mathrm{nr}}} = \phi^n$$

where ϕ denotes the Frobenius element in $\mathrm{Gal}(K^{\mathrm{nr}}/K)$. Then the map $\rho_{K,\pi}$ is independent of the choice of π.

Proof. (See [Lan90, p.203, Theorem 4.1].) Let π' be another prime element of K. Since every unit in $\mathcal{O}_K^\times = U_K$ can be expressed as a quotient of two prime elements of K, we deduce that $K^\times$ is generated by the prime elements of K and, as a result, it suffices to see that $\rho_{K,\pi}$ and $\rho_{K,\pi'}$ agree on every prime. In particular, it suffices to see that

$\rho_{K,\pi}(\pi') = \rho_{K,\pi'}(\pi')$. Both automorphisms are the Frobenius over K^{nr}, and $\rho_{K,\pi'}(\pi')$ is the identity over $K_{\pi'}$, so we are done once we check that $\rho_{K,\pi}(\pi')$ is also the identity on $K_{\pi'}$.

Now, let f and g be polynomials such that $f \equiv g \equiv X^q \bmod \pi$, $f \equiv \pi X \bmod X^2$ and $g \equiv \pi' X \bmod X^2$. We know that $K_{\pi'}$ is generated over K by the π'^m-torsion points in $\mathfrak{m}_{K^{\mathrm{sep}}}$ for all m. By Theorem 3.2.2, there exists an isomorphism θ of the Lubin-Tate formal groups associated to f and g, which induces an isomorphism $\theta : (\mathfrak{m}_{K^{\mathrm{sep}}}, +_f, \cdot_f) \to (\mathfrak{m}_{K^{\mathrm{sep}}}, +_g, \cdot_g)$ mapping the π^m-torsion elements to the π'^m-torsion elements. Hence, $K_{\pi'}$ is generated over K by the elements $\theta(x)$ where x is any generator of $K_{\pi,m}$ for any m. We want to see that $\rho_{K,\pi}(\pi')(\theta(x)) = \theta(x)$ for such an x. Write $\pi' = u\pi$, then

$$\rho_{K,\pi}(\pi')(\theta(x)) = \rho_{K,\pi}(u) \circ \rho_{K,\pi}(\pi)(\theta(x)).$$

We can use that $\rho_{K,\pi}(\pi)$ is the Frobenius over K^{nr} but leaves x fixed:

$$\rho_{K,\pi}(\pi')(\theta(x)) = \rho_{K,\pi}(u)(\theta^{\phi}(x)).$$

Using now that $\rho_{K,\pi}(u)$ is the identity over K^{nr}, so that commutes with θ and θ^{ϕ} by continuity, while being equal to σ_u over K_π, we get

$$\begin{aligned}\rho_{K,\pi}(\pi')(\theta(x)) &= \theta^{\phi}(\sigma_u(x)) = \theta \circ [u]_f \circ [u^{-1}]_f(x) \\ &= \theta(x).\end{aligned}$$

This shows that $\rho_{K,\pi}(\pi') = \rho_{K,\pi'}(\pi')$ for any two primes π and π' of K. This concludes the proof. □

From now on, we will denote the map $\rho_{K,\pi}$ by ρ_K.

4 The Local Kronecker-Weber Theorem

In this chapter we will show how Lubin-Tate extensions help us prove the Kronecker-Weber theorem for non-Archimedean local fields. In particular, we will show how the Abelian closure of a non-Archimedean local field K can be expressed as a compositum of a totally ramified and an unramified extension of K, for which we will require some details on ramification groups and the Hasse-Arf theorem. The structure of this chapter is based on [Mil13, Chap.1, §4] and [Iwa86, Chap.7, §2,4].

4.1 Motivation: the decomposition theorem

In its essence, the local Kronecker-Weber theorem asserts that a particular extension of K, namely its Abelian closure, can be expressed as a compositum of two subextensions, one of them being the maximal unramified extension K^{nr} of K. To find what the other one must look like —or, rather, that it looks like what we want it to look like, which is a Lubin-Tate extension—, we first turn our attention to the following theorem.

Theorem 4.1.1. *Let E/K be a Galois extension containing K^{nr}, and let $\psi \in \mathrm{Gal}(E/K)$ be a lift of the Frobenius automorphism $\phi \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$. Denote by F the fixed field of ψ inside E. Then the following hold:*

(i) $K^{\mathrm{nr}} \cap F = K$

(ii) $E = K^{\mathrm{nr}} \cdot F$

(iii) $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$.

Proof. (See [Iwa86, p.40, Lemma 3.4].) The intersection $K^{\mathrm{nr}} \cap F$ consists of the points of K^{nr} that are fixed under ψ. Since $\psi|_{K^{\mathrm{nr}}} = \phi$, and the fixed points of K^{nr} under ϕ are those in K, statement (i) is clear. Statement (iii) follows from the fact that, by infinite Galois theory, the Galois group $\mathrm{Gal}(E/F)$ must be equal to the closure of $\langle\psi\rangle$ inside $\mathrm{Gal}(E/K)$; since $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \widehat{\mathbf{Z}}$ with generator ϕ, the two Galois groups are isomorphic.

To see (ii), we want to check that the extension E/F is a subextension of $K^{\mathrm{nr}} \cdot F/F$; that is, that every finite extension L/F inside E is contained in $K^{\mathrm{nr}} \cdot F$. Suppose L/F is finite of degree n, and take the field K_n^{nr}, the unramified extension of K of degree n. Then the compositum $K_n^{\mathrm{nr}} \cdot L$ is a finite extension of F. As a result of (iii), the Galois group $\mathrm{Gal}(K_n^{\mathrm{nr}} \cdot L/F)$ must be a finite, cyclic group, in which both $\mathrm{Gal}(K_n^{\mathrm{nr}} \cdot L/K_n^{\mathrm{nr}} \cdot F)$ and $\mathrm{Gal}(K_n^{\mathrm{nr}} \cdot L/L)$ have index n. Hence, the two groups are the same, so $L = K_n^{\mathrm{nr}} \cdot F$ and thus $L \subseteq K^{\mathrm{nr}} \cdot F$, proving (ii). □

Note that the extension F in Theorem 4.1.1 is maximal totally ramified inside E: The condition $F \cap K^{\mathrm{nr}}$ implies that it is totally ramified, whereas L not being maximally totally ramified inside E would imply that $K^{\mathrm{nr}} \cdot F$ is a strict subextension of E. This should serve as motivation for our approach to prove the local Kronecker-Weber theorem.

Corollary 4.1.2. *Let F be an Abelian extension of K that is the fixed field of the lift $\psi \in \mathrm{Gal}(K^{\mathrm{Ab}}/K)$ of the Frobenius $\phi \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$. Then F is an Abelian maximal totally ramified extension of K such that $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot F$.*

The remaining of this chapter is dedicated to proving that the Lubin-Tate extension K_π for a uniformizer π of K can be used as the extension F; that is, that K_π is the fixed field of some lift of Frobenius to $\mathrm{Gal}(K^{\mathrm{Ab}}/K)$. However, in order to do this, it will be necessary to introduce the machinery of ramification groups; in particular, the notion of upper numbering for this groups will be very helpful for this task.

4.2 Ramification groups

We begin by defining the ramification groups in the lower numbering, as seen in [Ser68, Chap.IV] or [Neu99, Chap.II, §10]. In what follows, K will be a non-Archimedean local field with residue field $k = \mathcal{O}_K/(\pi)$ of characteristic p.

Definition 4.2.1. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and ring of integers $\mathcal{O}_L$ with maximal ideal generated by the prime π_L. For $i = -1, 0, 1, \ldots$, we define the i-th **ramification group of** L/K as the subgroup

$$G_i := \left\{\sigma \in G : |\sigma a - a| \leqslant |\pi_L|^{i+1} \text{ for all } a \in \mathcal{O}_L\right\} \subseteq G.$$

The group G_0 is also known as the **inertia group of** L/K.

We note that this defines a sequence of subgroups

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq \ldots.$$

The inertia group G_0 corresponds to the inertia field of L/K, the largest unramified extension of K contained in L. For $i \geqslant 1$, we can express the i-th ramification group as

$$G_i = \left\{\sigma \in G : |\sigma\pi_L - \pi_L| \leqslant |\pi_L|^{i+1}\right\}.$$

Moreover, we have that the G_i are normal subgroups of G, being the kernel of the map sending $\sigma \in \mathrm{Gal}(L/K)$ to $\sigma|_{\mathcal{O}_L} \bmod \pi_L$. Since L/K is finite, necessarily $G_i = 1$ for large enough i. The quotient G/G_0 is isomorphic to $\mathrm{Gal}(k_L/k)$, where $k_L = \mathcal{O}_L/(\pi_L)$ is the residue field of L. We also have that G_0/G_1 injects into $k_L^\times$, and that G_i/G_{i+1} injects into k_L for $i \geqslant 1$. Indeed, the map sending $\sigma \in G_i/G_{i+1}$ to $\sigma(\pi_L)\pi_L^{-1} \in U_L^{(i)}/U_L^{(i+1)}$ is a well-defined group homomorphism —where U_L denotes the group of units of $\mathcal{O}_L$ and $U_L^{(i)}$ the subgroup $1 + \mathfrak{p}_L^i$—, since $\sigma(u)u^{-1} \in U_L^{(i+1)}$ for all $u \in U_L$; composition with maps $U_L/U_L^{(1)} \to k_L^\times$ and $U_L^{(i)}/U_L^{(i+1)} \to k_L$ gives the desired maps. This implies that

$$(G_0 : G_1) \,\big|\, q - 1, \quad (G_i : G_{i+1}) \,\big|\, q \text{ for } i \geqslant 1. \tag{4.2.1}$$

Another immediate property we deduce from the definition is that, if H is a subgroup of G, then considering its ramification groups gives

$$H_i = G_i \cap H \text{ for all } i.$$

We can see what the ramification groups look like for our Lubin-Tate extensions. Let $K_{\pi,m}$ be the totally ramified extension of K generated by a root of $f^{(m)}$, where $f(X) = X^q + \pi X$. We know from Lemma 2.1.8 that $\mathrm{Gal}(K_{\pi,m}/K) \cong U_K/U_K^{(m)}$; this isomorphism allows us to understand the ramification groups more easily.

Proposition 4.2.2. *For $i \geqslant 0$, let G_i denote the i-th ramification group of $K_{\pi,m}/K$. Then, under the isomorphism $G = \mathrm{Gal}(K_{\pi,m}/K) \cong U_K/U_K^{(m)}$, the group $U_K^{(i)}/U_K^{(m)}$ maps onto G_{q^i-1}.*

Proof. (See [Mil13, p.44, Proposition 4.1].) For $i = 0$ we recover the map $U_K/U_K^{(m)} \cong G$, since $G_0 = G$ as the extension $K_{\pi,m}/K$ is totally ramified. Let $i \geqslant 1$. We want to check that

$$|[u]_f(\lambda_m) - \lambda_m| \leqslant |\lambda_m|^{q^i}$$

where $u \in U_K^{(i)}$ is such that $u \notin U_K^{(i+1)}$. We write $u = 1 + \pi^i v$ with $v \in U_K$. Then

$$[u]_f(\lambda_m) = [1 + \pi^i v]_f(\lambda_m) = [1]_f(\lambda_m) + [v]_f f^{(i)}(\lambda_m) = \lambda_m + v'\lambda_{m-i}$$

for some unit $v' \in \mathcal{O}_{K_{\pi,m}}^\times$. Taking norms, this gives

$$|[u]_f(\lambda_m) - \lambda_m| = |\lambda_{m-i}|$$

and since the extension $K_{\pi,m}/K_{\pi,m-i}$ is totally ramified of degree q^i, we have $|\lambda_{m-i}| = |\lambda_m|^{q^i}$. Hence, $|[u]_f(\lambda_m) - \lambda_m| = |\lambda_m|^{q^i} > |\lambda_m|^{q^i+1}$. This means in particular that no element of G_{q^i-1} can be the image of an element not in $U_K^{(i)}/U_K^{(m)}$, so under the isomorphism it must hold that $U_K^{(i)}/U_K^{(m)} \cong G_{q^i-1}$, and the proof is finished. □

Corollary 4.2.3. *Let $G = \mathrm{Gal}(K_{\pi,m}/K)$. Then the ramification groups of $K_{\pi,m}/K$ are as follows:*

$$\begin{aligned} G = G_{-1} = G_0 &\cong U_K/U_K^{(m)} \\ G_1 = G_2 = \cdots = G_{q-1} &\cong U_K^{(1)}/U_K^{(m)} \\ G_q = G_{q+1} = \cdots = G_{q^2-1} &\cong U_K^{(2)}/U_K^{(m)} \\ &\vdots \\ G_{q^{m-2}} = G_{q^{m-2}+1} = \cdots = G_{q^{m-1}-1} &\cong U_K^{(m-1)}/U_K^{(m)} \\ \text{for } i \geqslant q^{m-1}, G_i = \{\mathrm{id}\} &\cong U_K^{(m)}/U_K^{(m)}. \end{aligned}$$

The upper numbering

One would desire a simpler relation to hold between the ramification groups of $\mathrm{Gal}(K_{\pi,m}/K)$ and the subgroups of $U_K/U_K^{(m)}$. It turns out that this is one of the results we find once we change to the ramification groups in the upper numbering. For this, we need to extend the definition of the ramification groups so that their index can range over the real numbers greater than -1.

Definition 4.2.4. For $x \geqslant -1$, we let $G_x := G_{\lceil x \rceil}$ where $\lceil x \rceil$ denotes the smallest integer greater or equal to x.

We will be in particular interested in the groups with index $x > 0$: in this case,

$$G_x = \left\{ \sigma \in G_0 : |\sigma a - a| \leqslant |\pi_L|^{\lceil x \rceil + 1} \text{ for all } a \in \mathcal{O}_L \right\}.$$

Using this extended definition, we may define the upper numbering of the ramification groups in the following way.

Definition 4.2.5. Let L/K be finite Galois, and let $G = \mathrm{Gal}(L/K)$. Let $\varphi_{L/K} : \mathbf{R}_{\geqslant 0} \to \mathbf{R}$ be the unique, piecewise linear, continuous function satisfying

$$\varphi_{L/K}(0) = 0, \qquad \varphi'_{L/K}(x) = \frac{1}{(G_0 : G_x)} \text{ for } x \notin \mathbf{Z}.$$

Then we define, for $y \geqslant 0$, the group $G^y := G_x$ where $\varphi_{L/K}(x) = y$.

When the extension L/K is clear from the context, we will remove the subscript and denote $\varphi_{L/K}$ by φ.

Example 4.2.6. Take $L = K_{\pi,m}$, $G = \mathrm{Gal}(K_{\pi,m}/K)$. Corollary 4.2.3 shows that, given $i \geqslant 1$, then $G_x \cong U_K^{(i)}/U_K^{(m)}$ for $x \in (q^{i-1} - 1, q^i - 1]$. Since $(U_K : U_K^{(1)}) = q - 1$ and $(U_K^{(i)} : U_K^{(i+1)}) = q$, we find that

$$(G_0 : G_x) = (q-1)q^{i-1} \text{ for } x \in (q^{i-1} - 1, q^i - 1].$$

So the function φ has slope $\frac{1}{(q-1)q^{i-1}}$ in the interval $(q^{i-1} - 1, q^i - 1)$ for $i = 1, 2, \ldots, m$. We claim that

$$\varphi([q^{i-1} - 1, q^i - 1]) = [i - 1, i]$$

for $i = 1, 2, \ldots, m$. Since φ is strictly increasing for $x > 0$, it suffices to check the condition on the boundary of the interval. This can be done by induction. For $i = 1$ we have that $\varphi(0) = 0$ and φ has a slope of $\frac{1}{q-1}$, so $\varphi(q-1) = 1$. Suppose that $\varphi(q^{i-1} - 1) = i - 1$. Then the equation of the line defining φ on the interval $[q^{i-1} - 1, q^i - 1]$ is

$$\varphi(x) - (i-1) = \frac{1}{(q-1)q^{i-1}}(x - (q^{i-1} - 1)),$$

so when $\varphi(x) = i$ we find

$$x = (q-1)q^{i-1}i - (q-1)q^{i-1}(i-1) + (q^{i-1} - 1) = (q-1)q^{i-1} + q^{i-1} - 1 = q^i - 1.$$

So $\varphi(q^i - 1) = i$ for $i = 0, 1, \ldots, m$.

As before, we may also try to find a suitable expression of the ramification groups of the Lubin-Tate extensions.

Proposition 4.2.7. *Let $G = \mathrm{Gal}(K_{\pi,m}/K)$. Then, under the isomorphism $G \cong U_K/U_K^{(m)}$, we have $G^i \cong U_K^{(i)}/U_K^{(m)}$.*

Proof. This is a consequence of Proposition 4.2.2 and Example 4.2.6: The former shows that $U_K^{(i)}/U_K^{(m)} \cong G_{q^i-1}$, while the latter asserts that $\varphi(q^i - 1) = i$, which implies that $G^i = G_{q^i-1}$. □

Upper numbering and quotients

Another advantage of this upper numbering is that it allows simple relations to hold between the ramification of a group and that of its quotients. Since this will be important in order to define ramification groups for infinite extensions, we take our time to prove it.

Theorem 4.2.8. *Let $L, M/K$ be finite Galois extensions such that $K \subseteq L \subseteq M$, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. Then*

$$(G/H)^y = \mathrm{Im}(G^y \to G/H) = G^y H/H.$$

We prove this theorem in several steps.

Definition 4.2.9. Let L/K be a finite, Galois extension, and let $G = \mathrm{Gal}(L/K)$. For $\sigma \in G$, we define $i_G(\sigma) \in \mathbf{Z}_{\geqslant 0} \cup \{\infty\}$ to be such that

$$|\sigma(\pi_L) - \pi_L| = |\pi_L|^{i_G(\sigma)}.$$

Note that this definition allows us to reformulate the definition of ramification group in the lower numbering. If $\sigma = \mathrm{id}$, then by definition $i_G(\sigma) = \infty$. Otherwise, we have $i_G(\sigma) \in \mathbf{Z}$; in this case,

$$\sigma \in G_r \Leftrightarrow i_G(\sigma) \geqslant r + 1. \tag{4.2.2}$$

Lemma 4.2.10. *Let L/K be a finite Galois extension, and let $G = \mathrm{Gal}(L/K)$. Let $\varphi : \mathbf{R}_{\geqslant 0} \to \mathbf{R}$ be its associated function as in Definition 4.2.5. Then*

$$\varphi(x) = -1 + \frac{1}{\mathrm{card}\,(G_0)} \sum_{\sigma \in G} \min\big(i(\sigma), x + 1\big) \tag{4.2.3}$$

where $\mathrm{card}\,(G_0)$ *denotes the cardinal of* G_0.

Proof. Denote by $\lambda(x)$ the right-hand side of expression (4.2.3). By the characterization (4.2.2) of the ramification groups in terms of the i_G function, we have that $\sigma \in G_0$ if and only if $i_G(\sigma) \geqslant 1$, so in this case $\min\big(i(\sigma), 1\big) = 1$. On the other hand, if $\sigma \notin G_0$ then $i_G(\sigma) = 0$ and the corresponding summand in $\lambda(0)$ vanishes. Hence,

$$\lambda(0) = -1 + \frac{1}{\mathrm{card}\,(G_0)} \sum_{\sigma \in G_0} 1 = -1 + \frac{\mathrm{card}\,(G_0)}{\mathrm{card}\,(G_0)} = 0 = \varphi(0).$$

Let $\sigma \in G_r$ with $\sigma \notin G_{r+1}$. Then $i_G(\sigma) = r+1$. As a result, the function $\min\big(i_G(\sigma), x+1\big)$ is constant for $x \geqslant r$, and it equals $x + 1$ for $x \leqslant r$. Seeing it now as a function of σ for a fixed x, we see that it is non-constant only when $\sigma \in G_x$. Therefore, in the derivative of λ at a point $x \notin \mathbf{Z}$ the only summands with a non-zero contribution will be those with $\sigma \in G_x$, so

$$\lambda'(x) = \frac{1}{\mathrm{card}\,(G_0)} \sum_{\sigma \in G_x} 1 = \frac{\mathrm{card}\,(G_x)}{\mathrm{card}\,(G_0)} = \frac{1}{(G_0 : G_x)}.$$

Since λ satisfies the same properties of φ, we conclude that $\varphi = \lambda$. □

Lemma 4.2.11. *Let $K \subseteq L \subseteq M$ be finite Galois extensions, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. Denote by $e(M/L)$ the ramification index of M/L. Then, for $\sigma \in G/H$,*

$$i_{G/H}(\sigma) = \frac{1}{e(M/L)} \sum_{\substack{\tau \in G \\ \tau|_L = \sigma}} i_G(\tau).$$

Proof. (See [Iwa86, p.104, Theorem 7.7(i)].) Let $\mathcal{O}_L$ and $\mathcal{O}_M$ be the rings of integers of L and M respectively, and let π_L and π_M be respective prime generators of $\mathcal{O}_L$ and $\mathcal{O}_M$ over $\mathcal{O}_K$; i.e. $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ and $\mathcal{O}_M = \mathcal{O}_K[\pi_M]$. We want to show that

$$|\pi_M|^{i_{G/H}(\sigma)} = |\pi_M|^{\frac{1}{e(M/L)} \sum i_G(\tau)}. \tag{4.2.4}$$

The left-hand side of Equation (4.2.4) can be written differently using the definition of $i_{G/H}$ and the fact that $|\pi_L| = |\pi_M|^{e(M/N)}$:

$$|\pi_M|^{i_{G/H}(\sigma)} = |\pi_L|^{\frac{1}{e(M/L)} i_{G/H}(\sigma)} = |\sigma(\pi_L) - \pi_L|^{\frac{1}{e(M/L)}}. \tag{4.2.5}$$

As for the right-hand side of Equation (4.2.4), we do the following. Fix $\chi \in G$ such that $\chi|_L = \sigma$. Then composition with χ gives a bijection between H and the set of elements of G that equal σ when restricted to L. As a result, we can write

$$\begin{aligned} |\pi_M|^{\frac{1}{e(M/L)} \sum i_G(\tau)} = \prod_{\substack{\tau \in G \\ \tau|_L = \sigma}} |\pi_M|^{\frac{1}{e(M/L)} i_G(\tau)} &= \prod_{\tau \in H} |\pi_M|^{\frac{1}{e(M/L)} i_G(\chi\tau)} \\ &= \left| \prod_{\tau \in H} \big(\chi\tau(\pi_M) - \pi_M\big) \right|^{\frac{1}{e(M/L)}}. \end{aligned} \tag{4.2.6}$$

Putting Equations (4.2.5) and (4.2.6) together, it suffices to show that

$$|\sigma(\pi_L) - \pi_L| = \left| \prod_{\tau \in H} \big(\chi\tau(\pi_M) - \pi_M\big) \right|. \tag{4.2.7}$$

We introduce the following notation: For a polynomial $g \in \mathcal{O}_M[X]$ and an automorphism $\alpha \in G$, we denote by g^α the polynomial whose coefficients are the image under α of those of g. Back to our problem, let $g \in \mathcal{O}_L[X]$ be the minimal polynomial of π_M over L. Then g has integral coefficients since $\pi_M \in \mathcal{O}_M$. Since $M = L(\pi_M)$, the roots of g are exactly the H-conjugates of π_M, and $g(X) = \prod_{\tau \in H}(X - \tau(\pi_M))$. Consider the polynomial g^χ:

$$g^\chi(X) = \prod_{\tau \in H}(X - \chi\tau(\pi_M)) \in \mathcal{O}_M[X].$$

At $X = \pi_M$, the polynomial g vanishes, so $g^\chi(\pi_M) - g(\pi_M) = g^\chi(\pi_M)$ and thus

$$g^\chi(\pi_M) - g(\pi_M) = \prod_{\tau \in H} (\pi_M - \chi\tau(\pi_M)).$$

Now, all the coefficients of the polynomial $g^\chi - g$ are divisible by $\chi(\pi_L) - \pi_L$. To see this, write $g(X) = \sum_i a_i X^i$, then $\chi(a_i) - a_i$ is the coefficient of X^i in $g^\chi - g$. Fixing an index i, and writing $a_i = \sum_j b_j \pi_L^j$ where $b_j \in \mathcal{O}_K$ for all j —since $a_i \in \mathcal{O}_L = \mathcal{O}_K[\pi_L]$—, we see that

$$\chi(a_i) - a_i = \sum_j \Big(\chi(b_j)\chi(\pi_L)^j - b_j \pi_L^j \Big) = \sum_j b_j \Big(\chi(\pi_L)^j - \pi_L^j \Big)$$

and $\chi(\pi_L)^j - \pi_L^j = 0$ for $j = 0$ and equal to $(\chi(\pi_L) - \pi_L)\Big(\sum_{\ell=1}^{j} \chi(\pi_L)^{j-\ell} \pi_L^{\ell-1} \Big)$ otherwise. Hence,

$$\left| \prod_{\tau \in H} (\pi_M - \chi\tau(\pi_M)) \right| = |g^\chi(\pi_M) - g(\pi_M)| \leqslant |\chi(\pi_L) - \pi_L| = |\sigma(\pi_L) - \pi_L|\,,$$

showing one inequality of Equation (4.2.7). To see the other inequality, we write $\pi_L \in \mathcal{O}_M = \mathcal{O}_K[\pi_M]$ as $\pi_L = \sum_j h_j \pi_M^j$ with $h_j \in \mathcal{O}_K$ for all j. Then the polynomial $h(X) = \sum_j h_j X^j \in \mathcal{O}_K[X]$ satisfies $h(\pi_M) = \pi_L$, or equivalently, the polynomial $h(X) - \pi_L$ vanishes at $X = \pi_M$. Therefore it must be a multiple of the minimal polynomial g of π_M: we write $h(X) - \pi_L = g(X)g_1(X)$ for a suitable $g_1 \in \mathcal{O}_L[X]$. Acting on these polynomials by χ, and using that h is invariant under this action since $h \in \mathcal{O}_K[X]$, we find that $h(X) - \chi(\pi_L) = g^\chi(X) g_1^\chi(X)$. Evaluating at $X = \pi_M$ and taking norms yields

$$|\pi_L - \chi(\pi_L)| = |g_1^\chi(\pi_M)| \left| \prod_{\tau \in H} (\pi_M - \chi\tau(\pi_M)) \right|.$$

Using now that $g_1(\pi_M)$ and thus $g_1^\chi(\pi_M)$ lie in $\mathcal{O}_M$ and that $\chi|_L = \sigma$, we obtain

$$|\pi_L - \sigma(\pi_L)| \leqslant \left| \prod_{\tau \in H} (\pi_M - \chi\tau(\pi_M)) \right|.$$

This finishes the proof. □

Lemma 4.2.12. *Let $K \subseteq L \subseteq M$ be finite Galois extensions, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. For $\sigma \in G/H$, let*

$$j(\sigma) := \max_{\substack{\tau \in G \\ \tau|_L = \sigma}} \{ i_G(\tau) \}\,.$$

Then the following equality holds:

$$i_{G/H}(\sigma) - 1 = \varphi_{M/L}(j(\sigma) - 1).$$

Proof. (See [Iwa86, p.105, Theorem 7.7(ii)].) The equality is clear if $\sigma = \mathrm{id}$, so we will assume that $\sigma \neq \mathrm{id}$. Using the alternate expressions of $\varphi_{M/L}$ and $i_{G/H}$ shown in Lemma 4.2.10 and lemma 4.2.11, it suffices to show that

$$\frac{1}{e(M/L)} \sum_{\substack{\tau \in G \\ \tau|_L = \sigma}} i_G(\tau) = \frac{1}{\mathrm{card}\,(H_0)} \sum_{\tau \in H} \min\big(i_H(\tau), j(\sigma)\big).$$

Since H_0 is the inertia group of M/L, its cardinality equals the ramification index of M/L, so we only need to show that the two sums are equal. We fix $\chi \in G$ such that $\chi|_L = \sigma$ and $i_G(\chi) = j(\sigma)$. Suppose $\tau \in H$ is such that $i_H(\tau) \geqslant j(\sigma)$. This means, via the characterization (4.2.2) of the ramification groups in terms of the i function, that $\tau \in H_{j(\sigma)-1} = G_{j(\sigma)-1} \cap H$. We also know that $\chi \in G_{j(\sigma)-1}$, so $\chi\tau \in G_{j(\sigma)-1}$ and $i_G(\chi\tau) \geqslant j(\sigma)$. Since $\chi\tau$ is an automorphism of M which gives σ when restricted to L, we also have $i_G(\chi\tau) \leqslant j(\sigma)$ by definition of $j(\sigma)$, and thus $i_G(\chi\tau) = j(\sigma) = \min\big(i_H(\tau), j(\sigma)\big)$. Suppose now that $\tau \in H$ is such that $i_H(\tau) < j(\sigma)$. Then $\tau \notin H_{j(\sigma)-1}$, so $\chi\tau \notin G_{j(\sigma)-1}$ and $i_G(\chi\tau) < j(\sigma)$. Using now the definition of the i function, we see that $i_G(\chi\tau) = \min\big(i_G(\chi), i_G(\tau)\big)$ since $i_G(\chi) \neq i_G(\tau)$, and therefore $i_G(\chi\tau) = \min\big(j(\sigma), i_H(\tau)\big)$. Finally, since composition with χ gives a bijection between H and the elements of G which give σ when restricted to L, we have that

$$\sum_{\tau \in H} \min\big(i_H(\tau), j(\sigma)\big) = \sum_{\tau \in H} i_G(\chi\tau) = \sum_{\substack{\tau \in G \\ \tau|_L = \sigma}} i_G(\tau)$$

and the proof is complete. □

Lemma 4.2.13 (Herbrand's Theorem)**.** *Let $K \subseteq L \subseteq M$ be finite Galois extensions, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. For $r \geqslant -1$, we have*

$$G_r H/H = (G/H)_{\varphi_{M/L}(r)}.$$

Proof. Let $\sigma \in (G/H)_{\varphi_{M/L}(r)}$. By the expression (4.2.2) relating the i_G function and the ramification groups, we have that this is equivalent to $i_{G/H}(\sigma) \geqslant \varphi_{M/L}(r) + 1$. Lemma 4.2.12 now states that this is equivalent to

$$\varphi_{M/L}(r) \leqslant \varphi_{M/L}(j(\sigma) - 1).$$

The function $\varphi_{M/L}$ is strictly increasing, so this is equivalent to

$$r \leqslant j(\sigma) - 1,$$

which in turn is equivalent —by finiteness of G— to the existence of $\tau \in G$ such that $\tau|_L = \sigma$ and $i_G(\tau) \geqslant r + 1$. This means that $\tau \in G_r$, and $\sigma \in G_r H/H$, so $(G/H)_{\varphi_{M/L}(r)} \subseteq G_r H/H$. The other containment results after following the chain of equivalences in the other direction. □

Lemma 4.2.14. *Let $K \subseteq L \subseteq M$ be finite Galois extensions. As in Definition 4.2.5, we associate to the extensions M/K, L/K, and M/L the functions $\varphi_{M/K}$, $\varphi_{L/K}$, $\varphi_{M/L}$ respectively. Then*

$$\varphi_{M/K} = \varphi_{L/K} \circ \varphi_{M/L}.$$

Proof. We need to see that the function $\varphi_{L/K} \circ \varphi_{M/L}$ satisfies the conditions of Definition 4.2.5. Clearly it vanishes at $x = 0$. Its derivative at a point x (assuming $x \notin \mathbf{Z}$ and $\varphi_{M/L} \notin \mathbf{Z}$) equals

$$\begin{aligned}\varphi'_{L/K}(\varphi_{M/L}(x)) \cdot \varphi'_{M/L}(x) &= \frac{1}{\left((G/H)_0 : (G/H)_{\varphi_{M/L}(x)}\right)} \cdot \frac{1}{\left(H_0 : H_x\right)} \\ &= \frac{\operatorname{card}\left((G/H)_{\varphi_{M/L}(x)}\right)}{\operatorname{card}\left((G/H)_0\right)} \cdot \frac{\operatorname{card}\left(H_x\right)}{\operatorname{card}\left(H_0\right)}.\end{aligned}$$

Using Herbrand's theorem (Lemma 4.2.13) and the isomorphy theorems we see that

$$(G/H)_{\varphi_{M/L}(x)} = G_x H/H \cong G_x/(G_x \cap H) = G_x/H_x$$

and similarly $(G/H)_0 \cong G_0/H_0$, so

$$\varphi'_{L/K}(\varphi_{M/L}(x)) \cdot \varphi'_{M/L}(x) = \frac{\operatorname{card}\left(G_x\right) / \operatorname{card}\left(H_x\right)}{\operatorname{card}\left(G_0\right) / \operatorname{card}\left(H_0\right)} \cdot \frac{\operatorname{card}\left(H_x\right)}{\operatorname{card}\left(H_0\right)} = \frac{\operatorname{card}\left(G_x\right)}{\operatorname{card}\left(G_0\right)} = \frac{1}{\left(G_0 : G_x\right)}$$

and thus $(\varphi_{L/K} \circ \varphi_{M/L})' = \varphi'_{M/K}$, finishing the proof. □

Proof of Theorem 4.2.8. Let x be the preimage of y under $\varphi_{M/K}$: that is, $\varphi_{M/K}(x) = y$. By Herbrand's theorem (Lemma 4.2.13), we have

$$G^y H/H = G_x H/H = (G/H)_{\varphi_{M/L}(x)}.$$

Applying now that $G/H = \operatorname{Gal}(L/K)$ and the definition of the upper numbering, it follows that

$$(G/H)_{\varphi_{M/L}(x)} = (G/H)^{\varphi_{L/K}(\varphi_{M/L}(x))}$$

and using that $\varphi_{M/K}(x) = \varphi_{L/K}(\varphi_{M/L}(x))$ by Lemma 4.2.14 gives the desired result. □

The Hasse-Arf theorem

The behavior of the upper numbering when passing to quotients allows us to define filtrations of ramification groups even when the extensions involved are infinite. If L is a Galois extension of K, and $G = \mathrm{Gal}(L/K)$, then an automorphism $\sigma \in G$ satisfies $\sigma \in G^y$ if and only if $\sigma \in \mathrm{Gal}(M/K)^y$ for all finite Galois M/K. For the lower numbering, we had, by definition, that if $G_i \neq G_{i+\epsilon}$ for all $\epsilon > 0$, then necessarily i was an integer. We would like to have a similar result for the upper numbering; specifically, that if $G^y \neq G^{y+\epsilon}$ for all $\epsilon > 0$, then $y \in \mathbf{Z}$. This is not be true in general, but fortunately it will be for the cases we care about here, as shown below.

Theorem 4.2.15 (Hasse-Arf)**.** *Let L/K be an Abelian extension, $G = \mathrm{Gal}(L/K)$. Then, if $G^y \neq G^{y+\epsilon}$ for all $\epsilon > 0$, then $y \in \mathbf{Z}$. Equivalently, if $G_i \neq G_{i+1}$ for integer i, then $\varphi(i)$ is an integer.*

The Hasse-Arf theorem will be the last ingredient we need in order to prove the local Kronecker-Weber theorem. However, in spite of the risk of seeming inconsistent to the reader, we will not give a complete proof of this theorem. It requires proving certain properties about the action of the norm map on the filtration $\left\{U_L^{(m)}\right\}$ of unit groups of an extension L/K; while interesting, it would require a lot of space and it is not as directly related to our goal as other results we have proved. However, we can show how the theorem reduces to a simpler case if we assume one key result. This simplification is done in [Ser68, ch.V, §7]; the interested reader may want to consult the whole of [Ser68, ch.V] for a more detailed account of the proof of this theorem.

Proposition 4.2.16. *Let L/K be a cyclic, totally ramified extension, and let $G = \mathrm{Gal}(L/K)$. Suppose that y is the largest index of a non-trivial ramification group of L/K, i.e. $G^y \neq \{\mathrm{id}\}$ but $G^{y+\epsilon} = \{\mathrm{id}\}$ for all $\epsilon > 0$. Then y is an integer.*

Proof of the Hasse-Arf Theorem 4.2.15. (See [Ser68, p.101, Théorème 1].) The theorem results from the following chain of simplifications and the application of Proposition 4.2.16.

- The upper numbering for infinite extensions is defined from that of its finite subextensions, so it suffices to prove the theorem for the case where L/K is finite Abelian.
- Since $G_0 = G^0$, we can assume that $y > 0$ or, equivalently, that $G = G_0$ and L/K is totally ramified.
- Denote by $G^{y+\epsilon}$ the largest ramification group different to G^y, and consider the quotient $G/G^{y+\epsilon}$. As a consequence of Theorem 4.2.8, the ramification group $(G/G^{y+\epsilon})^y$ is the smallest non-trivial ramification group of $G/G^{y+\epsilon}$. Since $G/G^{y+\epsilon}$ is the Galois

group of a finite, Abelian, totally ramified extension of K, we may assume that G^y is the smallest non-trivial ramification group of the extension L/K.

- Being G a finite Abelian group, it can be decomposed as a product of cyclic groups: $G = \prod_i C_i$. Since $G^y \neq \{\mathrm{id}\}$, there exists a cyclic subgroup C_j such that $C_j \cap G^y \neq \{\mathrm{id}\}$. Let $H = \prod_{i \neq j} C_i$. Then the quotient group $G/H \cong C_j$ corresponds to a cyclic, totally ramified extension M/K for which $(C_j)^y = G^y H/H$ is the smallest non-trivial ramification group.

The extension M/K satisfies the conditions of Proposition 4.2.16, so $y \in \mathbf{Z}$ as desired. □

To better prepare for the final proof of the local Kronecker-Weber theorem, it is useful to examine a consequence of the Hasse-Arf theorem when the extension is similar to the ones we are interested in.

Corollary 4.2.17. *Let L/K be a finite, Abelian, totally ramified extension, and let $G = \mathrm{Gal}(L/K)$. Then we have*

$$(G^0 : G^1) \,\big|\, (q-1), \qquad (G^i : G^{i+1}) \,\big|\, q \ \text{ for } i \in \mathbf{Z}_{\geqslant 1}.$$

In particular, $(G : G^{m+1}) \,\big|\, q^m(q-1)$.

Proof. Let $i \geqslant 0$. If $G^i = G^{i+1}$, then it is clear. Otherwise, there is a jump, and $G^{i+\epsilon} = G^{i+1}$ for all $0 < \epsilon \leqslant 1$ by the Hasse-Arf Theorem 4.2.15. So they correspond to consecutive ramification groups G_j and G_{j+1} in the upper numbering, and the corollary follows from expression (4.2.1). □

4.3 Proof of the Local Kronecker-Weber theorem

Theorem 4.3.1 (Local Kronecker-Weber Theorem)**.** *Let π be any uniformizer of K. Then $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot K_\pi$, where K^{Ab} denotes the Abelian closure of K.*

We are now in position to show that $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot K_\pi$, where π is any uniformizer of K. Recall that in Theorem 3.3.2 it was shown that $K^{\mathrm{nr}} \cdot K_\pi$ was in itself independent of the choice of π.

Theorem 4.3.2. *Let $\phi \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ be the Frobenius element, and let $\psi \in \mathrm{Gal}(K^{\mathrm{Ab}}/K)$ be a lift of ϕ. Let F be the fixed field of ψ inside K^{Ab}. Then F contains K_π for some uniformizer π of K.*

Proof. (See [Iwa86, p.86, (i)].) Denote by σ the restriction of ψ to $K^{\mathrm{nr}} \cdot K_\pi$. Since $\sigma|_{K^{\mathrm{nr}}} = \phi$ by definition of σ and ψ, and $\sigma|_{K_\pi}$ corresponds to an element of $\mathcal{O}_K^\times$ as seen in

Section 3.3, following the reciprocity map it must be the case that $\sigma = \rho_K(\pi)$ for some uniformizer π of K. Now, $\rho_K(\pi)$ leaves K_π fixed, so K_π is contained in the fixed field of σ, which must be $(K^{\mathrm{nr}} \cdot K_\pi) \cap F$. Hence, $K_\pi \subseteq F$. □

Proof of the local Kronecker-Weber Theorem 4.3.1. (See [Iwa86, p.115].) It remains to be shown that, in the notation of the previous theorem, the equality $F = K_\pi$ holds. To see this, let $\alpha \in F$, and consider the subextension $K(\alpha) \subseteq F$. We can assume $K(\alpha)$ to be normal over K; otherwise, it suffices to use the splitting field of the minimum polynomial of α over K. Then $K(\alpha)/K$ is finite and Galois, and there exists some $m \geqslant 0$ such that $\mathrm{Gal}(K(\alpha)/K)^{m+1} = 1$, since $K(\alpha)/K$ is totally ramified. The extension $K_{\pi,m}/K$ also has the property that $\mathrm{Gal}(K_{\pi,m}/K)^{m+1} = 1$, by Proposition 4.2.7. Hence, for the compositum $K_{\pi,m} \cdot K(\alpha)$ it also holds that $\mathrm{Gal}(K_{\pi,m} \cdot K(\alpha)\,/K)^{m+1} = 1$: By Proposition 4.2.8 on the upper ramification and quotients, we see that all maps in $\mathrm{Gal}(K_{\pi,m} \cdot K(\alpha)/K)^{m+1}$ become the identity on $K_{\pi,m}$ and $K(\alpha)$ when restricted to the respective field, so they must be all equal to the identity.

Now, $K_{\pi,m} \cdot K(\alpha)$ is finite, Abelian, and totally ramified, due to it being contained in F. By the Corollary 4.2.17 to the Hasse-Arf theorem, we must have that the cardinality of $\mathrm{Gal}(K_{\pi,m} \cdot K(\alpha)/K)$ divides $q^m(q-1)$. Hence, so does the degree of the extension $K_{\pi,m} \cdot K(\alpha)/K$. However, this contains $K_{\pi,m}$, whose degree as an extension of K is precisely $q^m(q-1)$. Thus, the two extensions must be equal, so $K(\alpha) \subseteq K_{\pi,m} \subseteq K_\pi$. This shows that $K_\pi = F$; since F was the fixed field of Frobenius from the decomposition theorem applied to K^{Ab}, we finally find that $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot K_\pi$. □

5 Reciprocity revisited

In this final chapter we collect some of the results fundamental to local class field theory that were not mentioned in the previous pages. More specifically, we examine the reciprocity map and derive its properties regarding finite extensions of K and their norm groups. This leads to the local existence theorem, linking finite Abelian extensions of K with the open subgroups of finite index in $K^\times$.

5.1 Relative Lubin-Tate extensions

So far we have worked with the Lubin-Tate extensions defined in Section 2: totally ramified extensions of K associated to a given prime π of K via a formal group. It turns out that we can introduce a generalization of these Lubin-Tate extensions that will allow us to, quite easily, show some of the interesting properties of the reciprocity map. The reason we are introducing these extensions so late in this exposition is twofold. First, it is maybe more pedagogical to begin with the regular Lubin-Tate extensions as originally defined, and introduce the generalization when it becomes useful; this also simplifies the notation. Second, the proofs for the relevant properties of the generalized extensions can be modelled after the ones done for the original Lubin-Tate extensions, so with this approach we do not need to prove everything twice, thus sparing ourselves some unnecessary redundancy. Of course, the reason we can remit ourselves to the earlier proofs is because some extra work has been done already; and indeed, the attentive reader will have noticed that —and wondered why— we have described many of the properties for formal groups in terms of power series with coefficients in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$. It is for this reason that we have done so: in order to quickly generalize later on. These extensions were first introduced by de Shalit [Sha85] and Iwasawa [Iwa86], where they are studied together with the original Lubin-Tate extensions; the article of Yoshida [Yos08] expands on this treatment.

Definition 5.1.1. Let K_n^{nr} denote the unramified extension of K of degree n, and let ϖ be a prime element of K_n^{nr}. Let f be a power series in $\mathcal{O}_{K_n^{\mathrm{nr}}}[[X]]$ such that $f \equiv X^q \bmod \varpi$ and $f \equiv \varpi X \bmod X^2$. For $m \geqslant 1$, let $f^{(m)}$ be the power series defined as in Definition 2.1.1, i.e.

$$f^{(1)} = f, \quad f^{(m+1)} = f^{\phi^m} \circ f^{(m)}$$

where $\phi \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ is the Frobenius automorphism. Let λ_m be a root of $f^{(m)}$ that is not a root of $f^{(m-1)}$. We define the **m-th relative Lubin-Tate extension to K_n^{nr}/K** to be the extension

$$K_{\varpi,m}^n := K_n^{\mathrm{nr}}(\lambda_m)$$

over K.

Proposition 5.1.2. *The extension $K_{\varpi,m}^n/K$ is independent of the choice of f.*

Proof. Similar to Proposition 2.1.3, using now that the power series $[1]_{f,g}$ has coefficients in K_n^{nr} and that $f^{(r)} \circ [1]_{f,g} = [1]_{f,g}^{\phi^r} \circ g^{(r)}$ for all r. □

Proposition 5.1.3. *For any m and any n, the extension $K_{\varpi,m}^n/K_n^{\mathrm{nr}}$ is totally ramified.*

Proof. Similar to Proposition 2.1.5. The new definition of $f^{(m)}$ still implies that $f^{(m-1)}$ divides $f^{(m)}$, and if $a \in (\varpi)^r \backslash (\varpi)^{r+1}$ for some r, we have $\phi(a) \in (\varpi)^r \backslash (\varpi)^{r+1}$, so that the quotient is an Eisenstein polynomial. □

We now need to show that these extensions are Galois over K_n^{nr}, and find their Galois group. For this, we turn to our argument in Section 3.3, where we showed how to see the original Lubin-Tate extensions in terms of torsion data. However, this would require us to define something like $[\varpi]_f$, which we have not defined so far. We extend our definition of $[a]$ as in Theorem 1.2.6 to include cases where $a \notin \mathcal{O}_K$.

Definition 5.1.4. Let π and π' be uniformizers of $\widehat{K^{\mathrm{nr}}}$ and let f and g be in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that

$$f(X) \equiv g(X) \equiv X^q \bmod \pi \qquad f(X) \equiv \pi X \bmod X^2 \qquad g(X) \equiv \pi' X \bmod X^2.$$

Let $a \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$ be such that $\pi a = \pi' \phi(a)$. We denote by $[a]_{f,g}$ the unique power series in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that

$$f \circ [a]_{f,g} = [a]_{f,g}^{\phi} \circ g$$
$$[a]_{f,g}(X) \equiv aX \bmod X^2.$$

If f and g have coefficients in $\mathcal{O}_{K_n^{\mathrm{nr}}}$ and $a \in K_n^{\mathrm{nr}}$ for some n, then $[a]_{f,g}$ has coefficients in K_n^{nr} as well.

The definition makes sense thanks to the generality of Theorem 1.2.2. Moreover, by uniqueness, we also get a generalization of Corollary 1.2.7.

Proposition 5.1.5. *Let π, π' and π'' be uniformizers of $\widehat{K^{\mathrm{nr}}}$, and let f and g be in $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that*

$$f(X) \equiv g(X) \equiv h(X) \equiv X^q \bmod \pi$$
$$f(X) \equiv \pi X \bmod X^2 \qquad g(X) \equiv \pi' X \bmod X^2 \qquad h(X) \equiv \pi'' X \bmod X^2.$$

Let a and b be elements of $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$ such that $\pi a = \pi' \phi(a)$ and $\pi' b = \pi'' \phi(b)$. Then the power series $[ab]_{f,h}$ is well-defined, and

$$[a]_{f,g} \circ [b]_{g,h} = [ab]_{f,h}.$$

Proof. The power series is well defined since $\pi ab = \phi(a)\pi' b = \phi(ab)\pi''$, and the relation follows by uniqueness. □

Example 5.1.6. (i) In the context of relative Lubin-Tate extensions, $f = [\varpi]_{f^\phi,f}$ trivially, as $f^\phi \equiv \phi(\varpi)X \bmod X^2$ and setting $a = \varpi$ gives the necessary relations.

(ii) Let f and g be as in Definition 5.1.4 above. By Theorem 3.2.2 there exists a power series $\theta \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}[[X]]$ such that $g \circ \theta = \theta^\phi \circ f$ and $\theta(X) \equiv \epsilon X \bmod X^2$ for some ϵ with the property $\phi(\epsilon)\epsilon^{-1} = \pi'\pi^{-1}$. Then, under the new notation, $\theta = [\epsilon]_{g,f} = [\epsilon^{-1}]_{f,g}$.

Lemma 5.1.7. *Let ϖ be a uniformizer of K_n^{nr}, and let $f \in \mathcal{O}_{K_n^{\mathrm{nr}}}[X]$ be such that*

$$f \equiv X^q \bmod \varpi \qquad f \equiv \varpi X \bmod X^2.$$

Then, for all $m \geqslant 1$,

$$f^{(m)} = \left[\varpi \prod_{j=1}^{m-1} \phi^j(\varpi) \right]_{f^{\phi^m},f}. \tag{5.1.1}$$

Proof. Equation (5.1.1) follows by induction. It is clear for $m = 1$ by Example 5.1.6. If it holds for some $m \geqslant 1$, then

$$f^{(m+1)} = f^{\phi^m} \circ f^{(m)} = [\varpi]_{f^\phi,f}^{\phi^m} \circ \left[\varpi \prod_{j=1}^{m-1} \phi^j(\varpi) \right]_{f^{\phi^m},f},$$

so it suffices to show that

$$[\varpi]_{f^\phi,f}^{\phi^m} = [\phi^m(\varpi)]_{f^{\phi^{m+1}},f^{\phi^m}}. \tag{5.1.2}$$

However, this follows since these power series defined in Definition 5.1.4 are unique. Note that the left-hand side of (5.1.2) equals f^{ϕ^m}; as a result, the power series on both sides

of the equation are congruent with $\phi^m(\varpi)X$ modulo X^2 and

$$f^{\phi^{m+1}} \circ [\varpi]^{\phi^m}_{f^\phi,f} = [\varpi]^{\phi^{m+1}}_{f^\phi,f} \circ f^{\phi^m}$$
$$f^{\phi^{m+1}} \circ [\phi^m(\varpi)]_{f^{\phi^{m+1}},f^{\phi^m}} = [\phi^m(\varpi)]^{\phi}_{f^{\phi^{m+1}},f^{\phi^m}} \circ f^{\phi^m},$$

so they must be the same by uniqueness. Using now Proposition 5.1.5 proves (5.1.1). □

Lemma 5.1.8. *Let ϖ be a uniformizer of K_n^{nr}, and let $f \in \mathcal{O}_{K_n^{\mathrm{nr}}}[X]$ be such that*

$$f(X) \equiv X^q \bmod \varpi \qquad\qquad f(X) \equiv \varpi X \bmod X^2.$$

Let π be a uniformizer of K. Then the zeroes of $f^{(m)}$ are exactly those of $[\pi^m]_f$ for all $m \geqslant 1$.

Proof. Since $\pi \in K$, we know that $[\pi]_f$ is well-defined —use the original definition in Theorem 1.2.6 for this, or the fact that K is fixed under Frobenius for the general Definition 5.1.4. As a result, $[\pi^m]_f$ is also well-defined. Moreover, let

$$u := \frac{\pi^m}{\varpi \prod_{j=1}^{m-1} \phi^j(\varpi)},$$

then $u\varpi = \phi(u)\phi^m(\varpi)$, so $[u]_{f,f^{\phi^m}}$ is also well-defined and Lemma 5.1.7 implies that

$$[\pi^m]_f = [u]_{f,f^{\phi^m}} \circ f^{(m)}.$$

By construction, $u \in \mathcal{O}^\times_{K_n^{\mathrm{nr}}}$, so $[u]_{f,f^{\phi^m}}$ cannot vanish on any point of the maximal ideal $\mathfrak{m}_{K^{\mathrm{sep}}}$ of the separable closure K^{sep} of K. Hence, the zeroes of $f^{(m)}$ are exactly those of $[\pi^m]_f$, and the proof is complete. □

Now we can properly show that the relative Lubin-Tate extensions are Galois. Let ϖ be a prime of K_n^{nr}, and $f = X^q + \varpi X \in \mathcal{O}_{K_n^{\mathrm{nr}}}[X]$. Let F be its associated Lubin-Tate formal group as in Theorem 1.2.3, i.e., the unique power series with

$$f(F(X,Y)) = F^\phi(f(X), f(Y)).$$

Then the set of roots of $f^{(m)}$ inside the maximal ideal $\mathfrak{m}_{K^{\mathrm{sep}}}$ of the separable closure K^{sep} of K has a $\mathcal{O}_K$-module structure: If λ and μ are roots of $f^{(m)}$, then so are

$$\lambda +_F \mu = F(\lambda, \mu), \qquad\qquad a \cdot_F \lambda = [a]_f(\lambda)$$

for any $a \in \mathcal{O}_K$, by Lemma 5.1.8. In order for the extension $K^n_{\varpi,m}/K_n^{\mathrm{nr}}$ to be Galois, it suffices to check that every root of $f^{(m)}$ is of the form $[a]_f(\lambda)$ for some fixed root λ.

Theorem 5.1.9. *Let ϖ be a prime of K_n^{nr}. The extension $K_{\varpi,m}^n/K_n^{\mathrm{nr}}$ is Galois, with Galois group isomorphic to $(\mathcal{O}_K/\mathfrak{p}_K^m)^\times \cong U_K/U_K^{(m)}$.*

Proof. Let $f = X^q + \varpi X$, and fix a generator λ_m of $K_{\varpi,m}^n/K_n^{\mathrm{nr}}$ – that is, $f^{(m)}(\lambda_m) = 0$ but $f^{(m-1)}(\lambda_m) \neq 0$. The map sending $a \in \mathcal{O}_K$ to $[a]_f(\lambda_m)$ is a homomorphism of $\mathcal{O}_K$-modules. By Lemma 5.1.8, its kernel is precisely the ideal $(\pi^m) = \mathfrak{p}_K^m$ where π is a prime of K. Hence, we can factor this map through $\mathcal{O}_K/\mathfrak{p}_K^m$. The map from $\mathcal{O}_K/\mathfrak{p}_K^m$ to the set of roots of $f^{(m)}$ is now injective, and since $\operatorname{card}(\mathcal{O}_K/\mathfrak{p}_K^m) = q^m$ and $f^{(m)}$ has degree q^m, it must also be surjective. So all the roots of $f^{(m)}$ can be expressed as $[a]_f(\lambda_m)$ for some $a \in \mathcal{O}_K$. The power series $[a]_f$ has coefficients in $\mathcal{O}_{K_n^{\mathrm{nr}}}$ and $K_{\varpi,m}^n$ is complete, being a finite extension of a local field. As a result, $[a]_f(\lambda_m) \in K_{\varpi,m}^n$, and the extension is Galois.

This argument also shows that the group of endomorphisms of the set of roots of $f^{(m)}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}_K$; therefore, its group of automorphisms is isomorphic to $(\mathcal{O}_K/\mathfrak{p}_K)^\times$, and by continuity of the elements of the Galois group we get that $\mathrm{Gal}(K_{\varpi,m}^n/K_n^{\mathrm{nr}}) \cong (\mathcal{O}_K/\mathfrak{p}_K)^\times$. □

Taking the union of all these relative Lubin-Tate extensions associated to the same prime of K_n^{nr}, we obtain a new field:

$$K_\varpi^n = \bigcup_{m \geqslant 1} K_{\varpi,m}^n.$$

Let π denote a prime of K, then the set of roots of a polynomial $f^{(m)}$ defining the extension $K_{\varpi,m}^n/K_n^{\mathrm{nr}}$ is isomorphic to the torsion points $\mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m]$ inside the maximal ideal of the separable closure of K. As a result, $K_\varpi^n/K_n^{\mathrm{nr}}$ is generated by the corresponding Tate module,

$$T_\pi(\mathfrak{m}_{K^{\mathrm{sep}}}) = \varprojlim_m \mathfrak{m}_{K^{\mathrm{sep}}}[\pi^m],$$

and has Galois group

$$\mathrm{Gal}(K_\varpi^n/K_n^{\mathrm{nr}}) = \varprojlim_m \mathrm{Gal}(K_{\varpi,m}^n/K_n^{\mathrm{nr}}) \cong \varprojlim_m (\mathcal{O}_K/\mathfrak{p}_K^m)^\times = \mathcal{O}_K^\times = U_K.$$

This is the same Galois group as that of the Lubin-Tate extension K_π/K, as shown in Section 3.3. As a result, the compositum $K_\varpi^n \cdot K^{\mathrm{nr}}$ is isomorphic to $K_\pi \cdot K^{\mathrm{nr}}$, which is in turn isomorphic to the Abelian closure K^{Ab} of K by the local Kronecker-Weber Theorem 4.3.1. Since $K_\varpi^n \cdot K^{\mathrm{nr}}$ is Abelian over K, it is contained in K^{Ab}, and thus $K_\varpi^n \cdot K^{\mathrm{nr}} = K^{\mathrm{Ab}}$. This has implications when considering the reciprocity map, and we will study some of those below.

5.2 Norm groups and the reciprocity map

Let us go back to the reciprocity map ρ_K: Given a uniformizer π of K, we have a map

$$\rho_K : K^\times \to \mathrm{Gal}(K^{\mathrm{nr}} \cdot K_\pi) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_\pi/K) \cong \widehat{\mathbf{Z}} \times U_K.$$

Since every element of $K^\times$ can be written in the form $u\pi^m$ for some $m \geqslant 0$, the image of ρ_K will be the subgroup $W_K^{\mathrm{Ab}} = \langle \phi \rangle \times U_K$ where ϕ is the Frobenius automorphism, generator of $\widehat{\mathbf{Z}}$. This is a dense subgroup of $\mathrm{Gal}(K^{\mathrm{Ab}}/K)$, and it is called the **Abelianized Weil group of** K. The reader interested in knowing more about this group can consult [Tat79, §1].

The identification $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot K_\pi$ for any uniformizer π of K allows us to write the reciprocity map as a map

$$\rho_K : K^\times \to \mathrm{Gal}(K^{\mathrm{Ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{Ab}}.$$

We will show that this map is functorial in the following sense. Let L/K be a finite separable extension of local fields; for L we have a similar map

$$\rho_L : L^\times \to \mathrm{Gal}(L^{\mathrm{Ab}}/L).$$

Every Abelian extension of K defines an Abelian extension of L, so $K^{\mathrm{Ab}} \subseteq L^{\mathrm{Ab}}$. Then we can show that the diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\rho_L} & \mathrm{Gal}(L^{\mathrm{Ab}}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \cdot|_{K^{\mathrm{Ab}}}} \\ K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{Ab}}/K) \end{array}$$

is commutative, where the downward arrows represent the norm map $N_{L/K} : L \to K$ and the restriction map to K^{Ab}. Now, since L/K is finite, we can take the inertia field of L/K and split the extension into an unramified extension and a totally ramified extension. Hence, it suffices to show that the diagram is commutative for finite unramified extensions, and for finite totally ramified extensions, separately.

Norm groups

Definition 5.2.1. Let L/K be a finite separable extension of local fields. We define the **norm group of** L, $\mathrm{Norm}(L/K)$, as the image of $L^\times$ under the norm map $N_{L/K}$. As a

result, $\mathrm{Norm}(L/K)$ is a subgroup of $K^\times$. Let now L/K be an algebraic extension of local fields. We define the **norm group of** L as

$$\mathrm{Norm}(L/K) = \bigcap_{\substack{K\subseteq M\subseteq L \\ M/K \text{ finite}}} \mathrm{Norm}(M/K).$$

In the case where L/K is an algebraic extension with $L = \bigcup_{m>0} L_m$ and L_m/K finite, then it holds that $\mathrm{Norm}(L/K) = \bigcap_{m>0} \mathrm{Norm}(L_m/K)$. To see this, note that the obvious containment is obvious, and for the other, it suffices to see that every finite subextension M/K is contained in some L_m: if $y = N_{L_m/K}(x_m)$ for some $x_m \in L_m^\times$, then $y = N_{M/K}(N_{L_m/M}(x_m)) \in \mathrm{Norm}(M/K)$.

Let us recall what we know about the norm groups of the Lubin-Tate tower of extensions. We know from Corollary 2.2.4 that $\mathrm{Norm}(K_{\pi,m}/K) = U_K^{(m)} \times \langle\pi\rangle$, where $K_{\pi,m}$ is the extension of degree $(q-1)q^{m-1}$ inside K_π. Since $K_\pi = \bigcup_m K_{\pi,m}$, we deduce that $\mathrm{Norm}(K_\pi/K) = \langle\pi\rangle$. Moreover, any totally ramified extension of K_π will have its norm group contained in $\langle\pi\rangle$. We can say something more based on the following results:

Proposition 5.2.2. *Let L/K be an algebraic extension of local fields. If L/K is totally ramified, then* $\mathrm{Norm}(L/K)$ *contains a prime element of K.*

Proof. (See [Iwa86, p.42, Proposition 3.8].) Suppose L/K is totally ramified. Let M/K be a finite extension of K contained in L, so that it is also totally ramified. Then the image of any prime of M under the norm map $N_{M/K}$ is also a prime of K. Let $S(M)$ denote the set of primes of K that lie in the image of $N_{M/K}$, then if π_M is a prime of M we have $S(M) = N_{M/K}(\pi_M U_M)$. Since U_M is compact in $M^\times$, so is $\pi_M U_M$ and its image under $N_{M/K}$, which is a continuous map, is also compact. So $S(M)$ is a compact subset of $S(K) = \pi_K U_K$ for a prime π_K of K. It is also non-empty. Moreover, if M_1 and M_2 are finite extensions of K inside L, then its compositum is also finite inside L, so it is totally ramified and $S(M_1 \cdot M_2) \subseteq S(M_1) \cap S(M_2)$ is compact and non-empty. We have that $S(K)$ is compact, and that the family of extensions $K \subseteq M \subseteq L$ give rise to compact, non-empty subsets of $S(K)$ for which all finite intersections are non-empty. This implies that the intersection of all $S(M)$ is non-empty; as a result, $\mathrm{Norm}(L/K)$ must contain a prime of K. □

Corollary 5.2.3. *If L/K_π is totally ramified, necessarily* $\mathrm{Norm}(L/K) = \langle\pi\rangle$.

Proof. We have shown that, as a consequence of Corollary 2.2.4, we have that $\mathrm{Norm}(K_\pi/K) = \langle\pi\rangle$ for any uniformizer π of K. This implies that $\mathrm{Norm}(L/K) \subseteq \langle\pi\rangle$, and Proposition 5.2.2 shows that equality holds. □

Totally ramified extensions

Using the previous result, we can begin to attack the problem of functoriality.

Theorem 5.2.4. *Let L/K be a finite, separable, totally ramified extension of local fields. Then*

$$\rho_L(x)|_{K^{\mathrm{Ab}}} = \rho_K(N_{L/K}(x))$$

for every $x \in L^\times$.

Proof. (See [Iwa86, p.83, Lemma 6.4].) It suffices to prove the equality for the case where x is any prime of L. To see this, note that, if $u \in U_L$ and Π is a prime of L, then $u\Pi$ is also a prime of L. Hence, $u = u\Pi \cdot \Pi^{-1}$, so $L^\times$ is generated by the set of primes of L, and the theorem follows since all the maps are group homomorphisms.

Let now Π be a prime of L, and consider $\rho_L(\Pi) \in \mathrm{Gal}(L^{\mathrm{Ab}}/L)$. By definition of the reciprocity map (Theorem 3.3.2) and the proof of the local Kronecker-Weber theorem (Section 4.3), we know that $\rho_L(\Pi)$ acts as the Frobenius automorphism in $\mathrm{Gal}(L^{\mathrm{nr}}/L)$ and that its fixed field inside L^{Ab} is the Lubin-Tate extension L_Π. Since L/K is totally ramified, the restriction map induces an isomorphism $\mathrm{Gal}(L^{\mathrm{nr}}/L) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$, so $\rho_L(\Pi)|_{K^{\mathrm{nr}}}$ is the Frobenius automorphism in $\mathrm{Gal}(K^{\mathrm{nr}}/K)$. This means that $\rho_L(\Pi)|_{K^{\mathrm{Ab}}}$ is an element of $\mathrm{Gal}(K^{\mathrm{Ab}}/K)$ which equals the Frobenius over K^{nr}. As a result, it lies in the Abelianized Weil group W_K^{Ab} of K, which is the image of ρ_K, so

$$\rho_L(\Pi)|_{K^{\mathrm{Ab}}} = \rho_K(\pi)$$

for some prime π of K. The fixed field of $\rho_K(\pi)$ must then be contained inside that of $\rho_L(\Pi)$, so $K_\pi \subseteq L_\Pi$. Since both L_Π/L and L/K are totally ramified, so must be L_Π/K, hence L_Π/K_π, and thus $\mathrm{Norm}(L_\Pi/K) = \langle\pi\rangle$ by Corollary 5.2.3. Considering also the norm group of L_Π/L, what we have is

$$\langle\Pi\rangle = \bigcap_{\substack{L\subseteq M\subseteq L_\Pi \\ M/L \text{ finite}}} N_{M/L}(M^\times) = \bigcap_{m>0} \mathrm{Norm}(L_{\Pi,m}/L)$$

where $L_{\Pi,m}$ denotes the m-th extension of L in the Lubin-Tate tower associated to Π, and thus

$$\begin{aligned}\langle\pi\rangle =& \bigcap_{\substack{K\subseteq M\subseteq L_\Pi \\ M/K \text{ finite}}} N_{M/K}(M^\times) \\ =& N_{L/K}(L^\times) \cap \bigcap_{m>0} N_{L/K}(\mathrm{Norm}(L_{\Pi,m}/L)) \supseteq N_{L/K}(L^\times \cap \langle\Pi\rangle)\end{aligned}$$

which implies that $N_{L/K}(\Pi) \in \langle \pi \rangle$. However, again L/K is totally ramified, so by Proposition 5.2.2 it must hold that $N_{L/K}(\Pi) = \pi$. This finishes the proof, as now

$$\rho_K(N_{L/K}(\Pi)) = \rho_K(\pi) = \rho_L(\Pi)|_{K^{\mathrm{Ab}}}$$

which is the desired result. □

Corollary 5.2.5. *Let L/K be a finite, Abelian, totally ramified extension of local fields. Then the kernel of the map $K^\times \to \mathrm{Gal}(L/K)$ induced by ρ_K and the restriction to L is the norm group* $\mathrm{Norm}(L/K)$.

Proof. By Theorem 5.2.4, we have $\rho_K(N_{L/K}(x)) = \rho_L(x) \in \mathrm{Gal}(K^{\mathrm{Ab}}/L)$ for every $x \in L^\times$, so in particular it is the identity on L. □

Unramified extensions

Having settled the property for totally ramified extensions, it remains to prove it for the unramified extensions. Here is where it will be of use that we have generalized the concept of Lubin-Tate extensions.

Lemma 5.2.6. *Let $n \geqslant 1$, and let K_n^{nr} be the unramified extension of K of degree n. Let ϖ be a uniformizer of K_n^{nr}, and let K_ϖ^n be the relative Lubin-Tate extension associated to ϖ. Then $\rho_K(N_{K_n^{\mathrm{nr}}/K}(\varpi))$ is the unique element of* $\mathrm{Gal}(K^{\mathrm{Ab}}/K)$ *such that*

$$\rho_K(N_{K_n^{\mathrm{nr}}/K}(\varpi))|_{K^{\mathrm{nr}}} = \phi^n, \qquad \rho_K(N_{K_n^{\mathrm{nr}}/K}(\varpi))|_{K_\varpi^n} = \mathrm{id},$$

where ϕ is the Frobenius automorphism of K^{nr}.

Proof. (See [Iwa86, p.81, Lemma 6.1].) As shown at the end of Section 5.1, we can write $K^{\mathrm{Ab}} = K^{\mathrm{nr}} \cdot K_\varpi^n$, so there exists a unique element in $\mathrm{Gal}(K^{\mathrm{Ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_\varpi^n/K_n^{\mathrm{nr}})$ with the above properties. Since $\varpi \in K_n^{\mathrm{nr}}$, its norm is of the form $N_{K_n^{\mathrm{nr}}/K}(\varpi) = u\pi^n$ for some uniformizer $\pi \in K$, so $\rho_K(u\pi^n)|_{K^{\mathrm{nr}}} = \phi^n$. It remains to be checked that $\rho_K(u\pi^n)$ is the identity over K_ϖ^n. The strategy to follow is similar to that of Theorem 3.3.2. Namely, let $f = X^q + \pi X$ and $g = X^q + \varpi X$, then we know by Theorem 3.2.2 that there exists an isomorphism of $\mathcal{O}_K$-modules

$$\theta : T_\pi(\mathfrak{m}_{K^{\mathrm{sep}}}) \to T_\varpi(\mathfrak{m}_{K^{\mathrm{sep}}}).$$

Since it suffices to show that $\rho_K(u\pi^n)(\lambda) = \lambda$ for every generator of $K_\varpi^n/K_n^{\mathrm{nr}}$, we only

need to show that $\rho_K(u\pi^n)(\theta(\mu)) = \theta(\mu)$ for every $\mu \in T_\pi(\mathfrak{m}_{K^{\text{sep}}})$. Then

$$\begin{aligned}
\rho_K(u\pi^n)(\theta(\mu)) &= \left(\rho_K(u) \circ \rho_K(\pi^n) \circ \theta\right)(\mu) \\
&= \left(\rho_K(u) \circ \theta^{\phi^n}\right)(\mu) \\
&= \left(\theta^{\phi^n} \circ \rho_K(u)\right)(\mu) \\
&= \left(\theta \circ [u]_f \circ [u^{-1}]_f\right)(\mu) \\
&= \theta(\mu),
\end{aligned}$$

so $\rho_K(u\pi^n)$ leaves the generators of $K_\varpi^n/K_n^{\text{nr}}$ fixed. Since both $[u^{-1}]_f$ and ϕ^n fix K_n^{nr}, this implies that $\rho_K(u\pi^n)$ is the identity on $K_\varpi^n/K_n^{\text{nr}}$, finishing the proof. □

Theorem 5.2.7. *Let K_n^{nr} be the unramified extension of K of degree n. Then*

$$\rho_{K_n^{\text{nr}}}(x) = \rho_K(N_{K_n^{\text{nr}}/K}(x))$$

for every $x \in (K_n^{\text{nr}})^\times$. In particular, the norm group $\text{Norm}(K_n^{\text{nr}}/K)$ is the kernel of the map $K^\times \to \text{Gal}(K_n^{\text{nr}}/K)$ induced by ρ_K and the restriction to K_n^{nr}.

Proof. (See [Iwa86, p.90, Theorem 6.9].) As in the totally ramified case (Theorem 5.2.4), it suffices to see that the equality holds for the primes of K_m^{nr}. Let ϖ be such a prime. By Lemma 5.2.6, it suffices to check that $\rho_{K_n^{\text{nr}}}(x)$ equals ϕ^m over K^{nr} and the identity over K_ϖ^n. We know that $\rho_{K_m^{\text{nr}}}(\varpi)|_{K^{\text{nr}}}$ is the Frobenius element of $\text{Gal}(K^{\text{nr}}/K_m^{\text{nr}})$, which equals the m-th power of the Frobenius of $\text{Gal}(K^{\text{nr}}/K)$, that is, ϕ^m. Moreover, for any $m \geqslant 1$, the m-th relative Lubin-Tate extension $K_{\varpi,m}^n/K_n^{\text{nr}}$ is finite, Abelian, and totally ramified, so we may use Corollary 5.2.5 to determine that $\rho_{K_n^{\text{nr}}}(\varpi)$ is trivial on $K_{\varpi,m}^n$. As a result, it is trivial on the whole K_ϖ^n, so it must equal $\rho_K(N_{K_n^{\text{nr}}/K})(x)$, as desired. □

Theorem 5.2.8. *Let L/K be a finite, separable extension of local fields. Then the following diagram commutes:*

$$\begin{array}{ccc}
L^\times & \xrightarrow{\rho_L} & \text{Gal}(L^{\text{Ab}}/L) \\
{\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \cdot|_{K^{\text{Ab}}}} \\
K^\times & \xrightarrow{\rho_K} & \text{Gal}(K^{\text{Ab}}/K)
\end{array}$$

Moreover, if L/K is Abelian, there is an isomorphism

$$K^\times/\text{Norm}(L/K) \to \text{Gal}(L/K).$$

Proof. (See [Iwa86, p.89, Theorem 6.9].) Let L^{in} be the inertia field of L/K, that is, the maximal unramified extension of K inside L. Then the extension L/L^{in} is finite and

totally ramified, so by Theorem 5.2.4 we have that

$$\rho_L(x)|_{(L^{\text{in}})^{\text{Ab}}} = \rho_{L^{\text{in}}}(N_{L/L^{\text{in}}}(x)).$$

On the other hand, $L^{\text{in}} = K_n^{\text{nr}}$ for some n, so by Theorem 5.2.7 we have that

$$\rho_{L^{\text{in}}}(N_{L/L^{\text{in}}}(x))|_{K^{\text{Ab}}} = \rho_K(N_{L^{\text{in}}/K}(N_{L/L^{\text{in}}}(x))).$$

Using now that $N_{L/K} = N_{L^{\text{in}}/K} \circ N_{L/L^{\text{in}}}$ gives the desired result. In the case where L/K is Abelian, this also implies that the image of $\text{Norm}(L/K)$ under ρ_K is trivial on L. Since the restriction map is surjective, this gives the right isomorphism. □

5.3 The local existence theorem

Let L be a finite Abelian extension of K (inside a fixed Abelian closure K^{Ab} of K). Theorem 5.2.8 shows how its norm group $\text{Norm}(L/K)$ arises from the reciprocity map. This gives it certain interesting properties with respect to the topology in $K^\times$. Recall that K comes with a topology induced by the non-Archimedean norm; as a result, $K^\times$ obtains a topology induced by the one in K. Since the topology on K made it into a topological field —the inversion map is continuous—, the topology on $K^\times$ makes it into a topological group. In this topology, the groups $U_K^{(m)}$ form a fundamental system of neighborhoods of 1. As for the Galois group, it comes equipped with the Krull topology. In this topology, it is the subgroups $\text{Gal}(K^{\text{Ab}}/L)$, for L/K finite Abelian, the ones that constitute a fundamental system of neighborhoods of the identity. For more details on the Krull topology or infinite Galois theory, see [Neu99, Chapter IV.1].

Proposition 5.3.1. *The reciprocity map $\rho_K : K^\times \to \text{Gal}(K^{\text{Ab}}/K)$ is injective and continuous.*

Proof. (See [Iwa86, p.82, Proposition 6.3(i)].) Let π be a uniformizer of K, and let $a = u\pi^m \in K^\times$ be such that $\rho_K(a) = \text{id}$. Then $\rho_K(a)|_{K^{\text{nr}}} = \text{id}$, but this equals ϕ^m where ϕ is the Frobenius of $\text{Gal}(K^{\text{nr}}/K)$. So necessarily $m = 0$. Now $\rho_K(a)|_{K_\pi} = \text{id}$, but this equals $[u^{-1}]$, which is only the identity if $u = 1$. So $a = 1$, and ρ_K is injective.

To see that it is continuous, note that $\text{Gal}(K_{\pi,m}/K) \cong U_K/U_K^{(m)}$ as groups, but also as topological spaces —they are both finite and discrete. As a result, the group isomorphism $U_K \cong \text{Gal}(K_\pi/K) \cong \text{Gal}(K^{\text{Ab}}/K^{\text{nr}})$ is also a homeomorphism. Since this map is the restriction of ρ_K to U_K, injectivity now implies continuity. Indeed, if V is open in $\text{Gal}(K^{\text{Ab}}/K)$ and $a = u\pi^m \in \rho_K^{-1}(V)$, then $\rho_K(u) \in \rho_K(\pi^{-m})V \cap \text{Gal}(K^{\text{Ab}}/K^{\text{nr}})$, which is open in $\text{Gal}(K^{\text{Ab}}/K^{\text{nr}})$. So $u \in \pi^{-m}\rho_K^{-1}(V) \cap U_K$, also open in U_K, and hence a is

contained in the open set $\rho_K^{-1}(V) \cap \pi^m U_K$. So $\rho_K^{-1}(V)$ is a neighborhood of any of its points, and hence open. □

Proposition 5.3.2. *Let L/K be finite Abelian (inside K^{Ab}). Then its norm group* $\mathrm{Norm}(L/K)$ *is an open subgroup of finite index in $K^\times$; to be precise,* $(K^\times : \mathrm{Norm}(L/K)) = [L : K]$.

Proof. (See [Mil13, p.21, Lemma 1.3].) The condition on the index follows immediately from Theorem 5.2.8, as $K^\times \cong \mathrm{Gal}(L/K)$. It remains to show that $\mathrm{Norm}(L/K)$ is open in $K^\times$. To do this, we show that it is a neighborhood of all its points, i.e. it contains an open set around any of its points. Let U_L be the unit group of $\mathcal{O}_L$; by definition, $U_L = \{a \in L : |a| = 1\}$, so it is compact in L. The norm map $N_{L/K}$ is continuous, so its image is also compact inside K, and hence, a closed set in $K^\times$ and U_K (by definition of the norm map as a determinant of a multiplication map, the norm of a unit of L is a unit of K). Now, $N_{L/K}(U_L)$ has finite index in $K^\times$; this means that its complement in $K^\times$ is a finite union of translations of the (closed) set $N_{L/K}(U_L)$, hence closed, so $N_{L/K}(U_L)$ must also be open. As a result, $N_{L/K}(U_L) \subseteq \mathrm{Norm}(L/K)$ is an open set containing some of its points; by translation, $\mathrm{Norm}(L/K)$ is a neighborhood of all of its points, and therefore open in $K^\times$. □

Thus, for L/K finite Abelian, the norm group $\mathrm{Norm}(L/K)$ is an open subgroup of finite index in $K^\times$. The converse, that every open subgroup of finite index in $K^\times$ is the norm group of some extension of K, is called the *local existence theorem*. We proceed to prove this statement.

Lemma 5.3.3. *Let L and M be finite Abelian extensions of K. Then $L \subseteq M$ if and only if* $\mathrm{Norm}(M/K) \subseteq \mathrm{Norm}(L/K)$. *In particular, the two extensions are equal if and only if their norm groups are also equal.*

Proof. (See [Mil13, p.20, Corollary 1.2].) If $L \subseteq M$, then $\mathrm{Norm}(M/K) \subseteq \mathrm{Norm}(L/K)$ by transitivity of the norms. As a result, applying this to $L \cdot M$ shows that $\mathrm{Norm}(L \cdot M/K)$ is contained in the norm groups of both L/K and M/K. We actually have $\mathrm{Norm}(L \cdot M/K) = \mathrm{Norm}(L/K) \cap \mathrm{Norm}(M/K)$. Assuming this, if $\mathrm{Norm}(M/K) \subseteq \mathrm{Norm}(L/K)$, this shows that $\mathrm{Norm}(L \cdot M/K) = \mathrm{Norm}(M/K)$. Since their indices inside $K^\times$ are the degrees of the respective extensions, this implies that $L \cdot M = M$, which means that $L \subseteq M$.

It remains to show that $\mathrm{Norm}(L \cdot M/K) \supseteq \mathrm{Norm}(L/K) \cap \mathrm{Norm}(M/K)$. For K'/K finite Abelian, let $\rho_{K'/K}$ denote the isomorphism $K^\times / \mathrm{Norm}(K'/K) \cong \mathrm{Gal}(K'/K)$. Let $a \in K^\times$ be an element of $\mathrm{Norm}(L/K) \cap \mathrm{Norm}(M/K)$. Then both $\rho_{L/K}(a)$ and $\rho_{M/K}(a)$ are the identity in their respective Galois groups. Consider now $\rho_{L \cdot M/K}(a)$: Its restriction to both L and M is trivial, but since $\mathrm{Gal}(L \cdot M/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, then this means that $\rho_{L \cdot M/K}(a)$ is the identity element of $\mathrm{Gal}(L \cdot M/K)$, and hence $a \in \mathrm{Norm}(L \cdot M/K)$. □

Lemma 5.3.4. *Let K_n^{nr} be the unramified extension of K of degree n, and let ϖ be a uniformizer of K_n^{nr}. Then* $\mathrm{Norm}(K_{\varpi,m}^n/K) = U^{(m)} \times \langle \pi^n \rangle$, *where π is a uniformizer of K.*

Proof. We begin by showing that $\mathrm{Norm}\, K_n^{\mathrm{nr}}/K = U_K \times \langle \pi^n \rangle$. Certainly the former is contained in the latter, since the norm of a unit is a unit and $N_{K_n^{\mathrm{nr}}/K}(\varpi) = \pi^n$. By Proposition 5.3.2, we know that the index of $\mathrm{Norm}\, K_n^{\mathrm{nr}}/K$ equals n, which is also the index of $U_K \times \langle \pi^n \rangle$ inside $K^\times = U_K \times \langle \pi \rangle$. Hence, they are equal.

We can now show the result for the case where $\varpi = \pi \in K$. Now $K_{\pi,m}^n = K_n^{\mathrm{nr}} \cdot K_{\pi,m}$, and $N_{K_{\pi,m}^n/K}(x) = (N_{K_{\pi,m}/K}(x))^n$ for all $x \in K_{\pi,m}$. We know from Corollary 2.2.4 that $\mathrm{Norm}(K_{\pi,m}/K) = U_K^{(m)} \times \langle \pi \rangle$. Then by transitivity of the norms,

$$\begin{aligned}\mathrm{Norm}(K_{\pi,m}^n/K) &\subseteq \mathrm{Norm}(K_{\pi,m}/K) \cap \mathrm{Norm}(K_n^{\mathrm{nr}}/K) = \left(U_K^{(m)} \times \langle \pi \rangle\right) \cap \left(U_K \times \langle \pi^n \rangle\right) \\ &= U_K^{(m)} \times \langle \pi^n \rangle.\end{aligned}$$

This is a subgroup of $K^\times = U_K \times \langle \pi \rangle$ of index $q^{m-1}(q-1)n$, which is also the degree of the extension $K_{\pi,m}^n/K$ and, hence, the index of $\mathrm{Norm}(K_{\pi,m}^n/K)$ in $K^\times$. Therefore they must be equal. The result now follows for all the relative Lubin-Tate extensions, since by Theorem 3.2.2 there exists an isomorphism θ mapping them to an extension of the form $K_{\pi,m} \cdot K_n^{\mathrm{nr}}$. □

Lemma 5.3.5. *Every subgroup of $K^\times$ that contains the norm group of a finite Abelian extension of K is itself a norm group.*

Proof. (See [Mil13, p.20, Corollary 1.2].) Let H be such a subgroup, and let L/K be finite Abelian such that $\mathrm{Norm}(L/K) \subseteq H$. Then $H/\mathrm{Norm}(L/K)$ is a subgroup of $K^\times/\mathrm{Norm}(L/K)$, and hence isomorphic to a subgroup of $\mathrm{Gal}(L/K)$, which by Galois theory corresponds to a finite extension $K \subseteq M \subseteq L$. Since $\mathrm{Gal}(L/K)$ is Abelian, we have that M/K is Galois. Consider the composite map

$$K^\times \to K^\times/\mathrm{Norm}(L/K) \cong \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K).$$

Its kernel is H, since the map $K^\times \to \mathrm{Gal}(M/K)$ has kernel $H/\mathrm{Norm}(L/K)$ and we have $\mathrm{Norm}(L/K) \subseteq H$. At the same time, by reciprocity, its kernel must be $\mathrm{Norm}(M/K)$. So $H = \mathrm{Norm}(M/K)$. □

Theorem 5.3.6 (Local existence theorem)**.** *Every open subgroup of $K^\times$ with finite index is a norm group of a finite Abelian extension of K.*

Proof. (See [Iwa86, p.100, Theorem 7.5].) Let H be an open subgroup of $K^\times$ with finite index. Let π be a uniformizer of K, then π^n must lie in H for some $n \geqslant 1$, since $K^\times/H$ is

finite. Being open and a subgroup, H is a neighborhood of the identity, so it must contain $U_K^{(m)}$ for some $m \geqslant 1$. Hence $H \supseteq \langle \pi^n \rangle \times U_K^{(m)}$, which is the norm group of $K_{\pi,m}^n/K$ by Lemma 5.3.4. Thus, by Lemma 5.3.5 we have $H = \mathrm{Gal}(L/K)$ for some finite Abelian L/K. □

5.4 Final remarks

Characterization and class field theory

Theorem 5.4.1. *Let K be a non-Archimedean local field. Then the reciprocity map*

$$\rho_K : K^\times \to \mathrm{Gal}(K^{\mathrm{Ab}}/K)$$

is uniquely characterized by

(i) $\rho_K(\pi)|_{K^{\mathrm{nr}}} = \phi$ where π is any uniformizer of K and ϕ is the Frobenius automorphism of K^{nr},

(ii) given L/K a finite Abelian extension, then the image of $\mathrm{Norm}(L/K)$ is trivial when restricted to L and ρ_K induces an isomorphism

$$K^\times/\mathrm{Norm}(L/K) \to \mathrm{Gal}(L/K).$$

Proof. (See [Mil13, p.24, Theorem 1.13].) Suppose ρ' is another such morphism. Let π be a uniformizer of K, then $\pi \in \mathrm{Norm}(K_{\pi,m}/K)$ for all m, so $\rho'(\pi)$ is trivial when restricted to $K_{\pi,m}$ for all m. As a result, it is trivial on K_π. We also have that $\rho'(\pi)|_{K^{\mathrm{nr}}} = \phi$, so by definition of ρ_K we have that $\rho'(\pi) = \rho_K(\pi)$. This holds for any uniformizer of K; since $K^\times$ is generated by the set of uniformizers of K and the maps are group homomorphism, we find that $\rho' = \rho_K$. □

This characterization shows that the reciprocity map ρ_K we have defined coincides with the so-called *local Artin symbol* found through local class field theory via cohomological methods, see for example [Mil13, Chapter III, §3]. As a result, the Artin map found in global class field theory, which can be constructed from the local Artin symbols of local class field theory —see [Mil13, Chapter V, §5]—, is compatible with the local map we have defined.

Reciprocity as a natural transformation

A consequence of this characterization of the reciprocity map is that it allows us to see it as a natural transformation of functors. Let $\mathcal{NALF}$ denote the category of non-Archimedean local fields, defined as follows: Its objects are pairs (K, K^{sep}) of a non-Archimedean local field K and a separable closure K^{sep}, and its morphisms $(K, K^{\text{sep}}) \to (L, L^{\text{sep}})$ are pairs of an injective morphism of fields $K \to L$ and an extension to an isomorphism $K^{\text{sep}} \to L^{\text{sep}}$. Note that an injective morphism of fields $K \to L$ can be seen as a generalized inclusion $K \subseteq L$. Since these are local fields, they are either finite extensions of $\mathbf{Q}_p$ for some p or isomorphic to $\mathbf{F}_q((T))$ for $q = p^r$ for some p; in both cases, the resulting extension L/K is separable and as a result $K^{\text{sep}} \cong L^{\text{sep}}$.

Let $\mathcal{G}$ denote the category of groups. The association $K \to K^\times$ becomes a functor $M : \mathcal{NALF}^{\text{opp}} \to \mathcal{G}$ by sending a morphism $\sigma : K \to L$ to the norm map $N_{L/K} : L^\times \to K^\times$. Note that this satisfies the properties of a functor, since $N_{K/K} = \text{id}$ and the norm is transitive.

At the same time, the association $K \to W_K$ sending K to its Abelianized Weil group can also be seen as a functor $W : \mathcal{NALF}^{\text{opp}} \to \mathcal{G}$, by sending $\sigma : K \to L$ to the conjuation map $\alpha \in W_L \mapsto \tilde{\sigma}^{-1}\alpha\tilde{\sigma} \in W_K$, where $\tilde{\sigma} : K^{\text{sep}} \to L^{\text{sep}}$ is an extension of σ. Note that this definition does not depend on the choice of extension $\tilde{\sigma}$: If $\bar{\sigma}$ is another extension, then setting $g = \bar{\sigma}\tilde{\sigma}^{-1}$ and $h = \alpha$ gives

$$(\tilde{\sigma}^{-1}\alpha\tilde{\sigma})(\bar{\sigma}^{-1}\alpha^{-1}\bar{\sigma}) = \bar{\sigma}^{-1}(ghg^{-1}h^{-1})\bar{\sigma} = 1$$

since $g, h \in \text{Gal}(L^{\text{sep}}/L)$, so $ghg^{-1}h^{-1} = 1 \in W_L \subseteq \text{Gal}(L^{\text{sep}}/L)^{\text{Ab}}$. The functor axioms are satisfied since the given map $W_L \to W_K$ is a group homomorphism.

With this in mind, then the commutativity of the diagram in Theorem 5.2.8 implies that there is a natural tranformation of functors $\rho : M \to W$. Using that the reciprocity map is injective by Proposition 5.3.1, we actually have the following.

Corollary 5.4.2. *There exists a unique isomorphism of functors $\rho : M \to W$ such that, if K is a non-Archimedean local field and $\pi \in K^\times$ is a uniformizer of K, then $\rho_K(\pi)$ acts on K^{nr} as the Frobenius automorphism.*

Bibliography

[Frö67] A. Fröhlich. Local fields. In J.W.S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 1–41. Academic Press Inc., 1967.

[Gol81] R. Gold. Local class field theory via Lubin-Tate groups. *Indiana University Mathematics Journal*, 30(5):795–798, 1981.

[Haz75] M. Hazewinkel. Local class field theory is easy. *Advances in Mathematics*, 18(2):148–181, November 1975.

[Iwa86] K. Iwasawa. *Local Class Field Theory*. Oxford University Press, 1986.

[Lan90] S. Lang. *Cyclotomic Fields I and II (Combined Second Edition)*. Springer, 1990.

[LT65] J. Lubin and J. Tate. Formal complex multiplcation in local fields. *Annals of Mathematics*, 81(2):380–387, March 1965.

[Lub81] J. Lubin. The local Kronecker-Weber theorem. *Transactions of the American Mathematical Society*, 267(1):133–138, September 1981.

[Mil13] J.S. Milne. Class Field Theory (v4.02), 2013. Available at `www.jmilne.org/math/`.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999. Translated from the original German version *Algebraische Zahlentheorie*, Springer, 1992.

[Ros81] M. Rosen. An elementary proof of the local Kronecker-Weber theorem. *Transactions of the American Mathematical Society*, 295(2):599–605, June 1981.

[Ser68] J.-P. Serre. *Corps Locaux*. Hermann, third edition, 1968.

[Sha85] E. de Shalit. Relative Lubin-Tate groups. *Proceedings of the American Mathematical Society*, 95(1):1–4, September 1985.

[Tat79] J. Tate. Number theoretic background. In A. Borel and W. Casselman, editors, *Proceedings of Symposia in Pure Mathematics*, volume 33.1, pages 3–26. American Mathematical Society, 1979.

[Yos08] T. Yoshida. Local class field theory via Lubin-Tate theory. *Annales de la Faculté des Sciences de Toulouse*, XVII(2):411–438, 2008.