Constructing Maximal Abelian Extensions with Lubin-Tate Theory

A Proof of the Local Kronecker-Weber Theorem

Pranav Konda

Columbia University, Mathematics and Computer Science*

May 15, 2024

Abstract

In this article, we build the theory of Lubin-Tate formal groups, which provide an elementary way to derive the results known as local class field theory. In particular, by assuming Artin reciprocity, we prove the local Kronecker-Weber theorem, and by extension, obtain the existence theorem. We assume knowledge of local field theory and Galois theory. Some extra requisite results are briefly explained (as necessary) in the appendix. We base our discussion on [CJ16].

Contents

*pvk2108@columbia.edu

1. Introduction

We begin our discussion with the notion of a formal group. Fix a ring R. Recall that the **ring of formal power series** (in n variables) $R[[X_1, X_2, \dots, X_n]]$ is defined as

$$\left\{ \sum_{(k_1,k_2,\dots,k_n):k_i\in\mathbb{Z}_{\geq 0}} \left(a_{k_1k_2\cdots k_n} \prod_{i=1}^{n} x_i^{k_i} \right) : a_{k_1k_2\cdots k_n} \in R \right\},$$

where addition and multiplication operations are formal addition and multiplication of the above series. We use the term *formal* to emphasize that questions of convergence are not considered when handling such series. This readily generalizes to an infinite number of variables, in which we may also construct the ring of formal power series $R[[X]]$] (in general) as the inverse limit

$$R[[X]] = \varprojlim_i R[X]/(X^i).$$

We now define a one-dimensional commutative (as this is all we will need for the following discussion on Lubin-Tate formal groups) formal group law.

Definition 1.1 (Formal Group Law). A one-dimensional commutative **formal group law** over a ring R is a a power series $F \in R[[X, Y]]$ such that the following hold:

i. **Commutativity**: $F(X, Y) = F(Y, X)$.

ii. **Associativity**: $F(X, F(Y, Z)) = F(F(X, Y), Z) \in R[[X, Y, Z]]$.

iii. $F(X, 0) = X$, and $F(0, Y) = Y$. Equivalently, we have that

$$F(X, Y) \equiv X + Y \mod \mathcal{O}(2),$$

where $\mathcal{O}(2)$ represents degree 2 terms.

Note that an immediately obvious example is $F(X, Y) = X + Y$, the *formal additive group.* Such formal groups laws do indeed have a group structure:

Theorem 1.2. There exists a power series $i(X) \in XR[[X]]$ such that $F(X, i(X)) = 0$.

Proof. We proceed by inductively building i. Clearly $F(X, Y)$ can have no (extra) terms of the form X^i, Y^j for $i, j > 0$ as otherwise $F(X, Y) \not\equiv X + Y \mod \mathcal{O}(2)$. Thus we may write

$$F(X, Y) = X + Y + \sum_{i,j\geq 1} c_{ij} X^i Y^j.$$

We now construct solutions to the equations

$$F(X, i_k(X)) \equiv 0 \mod \mathcal{O}(k).$$

For our base case, note that for $k = 2$ we have

$$i_2(X) = c_{11}X^2 - X.$$

Suppose we have a n-th degree solution $i_n(X)$ such that

$$F(X, i_n(X)) \equiv 0 \mod \mathcal{O}(n).$$

Then note that we have for $n+1$

$$F(X, a_{n+1}X^{n+1} + i_n(X)) \equiv 0 \mod \mathcal{O}(n+1).$$

But this simply amounts to a solvable linear equation in the coefficients, and thus we may construct the solution to i_{n+1}, and the result follows by induction. □

We now define homomorphisms of formal groups.

Definition 1.3 (Homomorphisms of Formal Groups)**.** Fix a ring R, and let F and G be formal groups over R. A **homomorphism of formal groups** $\varphi : F \to G$ is a power series $\varphi \in R[[X]]$ such that $\varphi(X) \equiv 0 \mod X$ and

$$\varphi(F(X,Y)) = G(\varphi(X), \varphi(Y)).$$

As usual, we have a ring of endomorphisms on F $\mathrm{End}_R(F)$ where addition is defined by

$$\begin{aligned} +_F : \mathrm{End}_R(F) \times \mathrm{End}_R(F) &\to \mathrm{End}_R(F) \\ (\varphi, \psi) &\mapsto F(\varphi(x), \psi(x)), \end{aligned}$$

and multiplication is defined by composition. With this, we can define the notion of a formal module:

Definition 1.4 (Formal Modules)**.** A **formal module** $(F, [a]_F)$ is a formal group F with a ring homomorphism $[a]_R \in \hom(R, \mathrm{End}_R(F))$, $a \mapsto [a]_F$ such that

$$[a]_F(X) \equiv aX \mod X^2.$$

2. Lubin-Tate Modules

Concretely, we are interested in the case where $R = \mathcal{O}_K$ where K is a local field. Let $\pi \in \mathcal{O}_K$ be a uniformizer.

Definition 2.1 (Lubin-Tate Module)**.** A **Lubin-Tate module** is a formal $\mathcal{O}_K$-module $(F, [\pi]_F)$ such that

$$[\pi]_F(X) \equiv X^{|k_K|} \mod \pi.$$

We further define a **Lubin-Tate series** as a series $e[X] \in \mathcal{O}_K[[X]]$ such that

$$e(X) \equiv X^{|k_K|} \mod \pi, \text{ and } e(X) \equiv \pi X \mod X^2.$$

In particular, $[\pi]_F$ is a Lubin-Tate series.

We will denote the set of Lubin-Tate series of F by $\mathcal{F}_\pi$. We will now collect some results on these modules.

Theorem 2.2. Let $e_1, e_2 \in \mathcal{F}_\pi$. Suppose we have a linear form

$$L(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i X^i,$$

where the $a_i \in \mathcal{O}_K$. Then there exists a unique power series

$$F(x_1, \dots, x_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$$

such that

$$F(x_1, \dots, x_n) \equiv L(x_1, \dots, x_n) \mod (x_1, \dots, x_n)^2,$$

and

$$e_1(F(x_1, \dots, x_n)) = L(e_2(x_1), \dots, e_2(x_n)).$$

Proof. We will construct our series inductively. Denote the solution for F in degree n by F_n. Note that in degree 2, if $F_2 = L$, then $L \equiv L \mod (x_1, \dots, x_n)^2$. Note also that by definition as e_1 and e_2 are Lubin-Tate series that

$$e_1(F(X = (x_1, \dots, x_n))) \equiv \pi X \mod X^2,$$

and as L is a linear form, that by linearity

$$L(e_2(X = (x_1, \dots, x_n))) \equiv \pi X \mod X^2.$$

But notice that this implies that

$$e_1 \circ F \equiv L \circ e_2 \mod (x_1, \dots, x_n)^2,$$

as desired. Thus in degree 2 we have $F_2 = L$, which is unique by construction. Suppose we have for degree k a unique solution F_k. Then similar to the proof of theorem 1.2, we will write $f_{k+1} = f_k + g$, where $g \in \mathcal{O}_K[X_1, \dots, X_n]$ is a homogeneous polynomial of degree $k+1$.

We have

$$e_1(F_{k+1}(X)) = e_1(F_k(X)) + \pi g(X) + \mathcal{O}(k+2),$$

and

$$F_{k+1}(e_2(X)) = F_k(e_2(X)) + \pi^{k+1} g(X) + \mathcal{O}(k+2),$$

where $\mathcal{O}(k+2)$ represents the terms of $\deg k+2$ and higher. Then in accordance with the second criterion on F_{k+1} (that $e_1(F(X)) = F(e_2(X))$) we have

$$g(X) = \frac{e_1(F_k(X)) - F_k(e_2(X))}{\pi(-1+\pi^k)} + \mathcal{O}(k+2).$$

Note that $-1+\pi^k$ is a unit as π generates the maximal ideal of $\mathcal{O}_K$. Thus it suffices to check whether $\pi \mid e_1(F_k(X)) - F_k(e_2(X))$. Note that as e_1, e_2 are Lubin-Tate series that

$$e_1(F_k(X)) - F_k(e_2(X)) \equiv e_1(F_k(X^{|k_K|})) - F_k(e_2(X^{|k_K|})) \mod \pi.$$

But the latter is $0 \mod \pi$ by definition. Thus $g(X)$ is valid, and the result follows by induction. □

Now, let $L = X + Y$.

Corollary 2.3. We have that for a Lubin-Tate series $e \in \mathcal{F}_\pi$, there is a unique power series $F_e(X,Y) \in \mathcal{O}_K[[X,Y]]$ such that

$$F_e(X,Y) \equiv X + Y \mod \mathcal{O}(2),$$

and

$$e(F(X,Y)) = F_e(e(X), e(Y)).$$

Similarly, we will define for $a \in \mathcal{O}_K$, $e_1, e_2 \in \mathcal{F}_\pi$, the unique power series $[a]_{e_1,e_2} \in \mathcal{O}_K[[X]]$ such that

$$[a]_{e_1,e_2}(X) \equiv aX \mod X^2,$$

and

$$e_1([a]_{e_1,e_2}(X)) = [a]_{e_1,e_2}(e_2(X)).$$

If $e_1 = e_2 = e$, we write $[a]_{e_1,e_2} = [a]_e$.

We now discuss a result that roughly shows the only parameter that is significant is the uniformizer.

Theorem 2.4. Let $e, e_1, e_2, e_3 \in \mathcal{F}_\pi$, and let $a, b \in \mathcal{O}_K$. Then we have

i. $F_e(X,Y) = F_e(Y,X)$.

ii. $F_e(F_e(X,Y),Z) = F_e(X, F_e(Y,Z))$.

iii. $F_{e_1}([a]_{e_1,e_2}(X), [a]_{e_1,e_2}(Y)) = [a]_{e_1,e_2}(F_{e_2}(X,Y))$.

iv. $[ab]_{e_1,e_3}(X) = [a]_{e_1,e_2}([b]_{e_2,e_3}(X))$.

v. $[a+b]_{e_1,e_2}(X) = [a]_{e_1,e_2}(X) + [b]_{e_1,e_2}(X)$.

vi. $[\pi]_e(X) = e(X)$.

Proof. The crux of the following proofs is by theorem 2.2.

i. By theorem 2.2, where $L = X+Y$, we have that as $F_e(X,Y) \equiv X+Y \equiv Y+X \equiv F(Y,X) \mod \mathcal{O}(2)$, by uniqueness $F_e(X,Y) = F_e(Y,X)$.

ii. Similarly, by uniqueness, the result follows.

All of the proofs follow by theorem 2.2, and proving them is not englightening to the further discussion at hand. Instead, we show a stronger result that follows. □

From the above, we have the following:

Corollary 2.5 (Classification of Lubin-Tate Modules)**.** Fix a uniformizer $\pi \in \mathfrak{m}_K$. Then the Lubin-Tate $\mathcal{O}_K$-modules are precisely the Lubin-Tate series F_e, for $e \in \mathcal{F}_\pi$, with the formal $\mathcal{O}_K$-module structure given by the following (let $a \in \mathcal{O}_K$):

$$a \mapsto [a]_e.$$

Furthermore, for $e_1, e_2 \in \mathcal{O}_K$, we have the map $[a]_{e_1,e_2}$ is a homomorphism from F_{e_2} to F_{e_1}. If a is a unit in $\mathcal{O}_K$, then this homomorphism is an isomorphism with inverse $[a^{-1}]_{e_2,e_1}$.

Proof. Note that if F is also a Lubin-Tate $\mathcal{O}_K$-module for π, then by definition we have that $e = [\pi]_F \in \mathcal{F}_\pi$. As F satisfies the properties of the Lubin-Tate series F_e, by theorem 2.2 $F = F_e$. The result then follows from the above theorem. □

3. Local Class Field Theory

We now work in an algebraic closure $\overline{K}/K$. Let $\overline{\mathfrak{m}}$ be the maximal ideal of $\mathcal{O}_{\overline{K}}$. Let $q = |k_K|$, the dimension of the residue field of K.

Suppose F is a formal $\mathcal{O}_K$ module. Then we can give $\overline{\mathfrak{m}}$ a true module structure (over F) by the following, for all $x, y \in \overline{\mathfrak{m}}$, and $a \in \mathcal{O}_K$.

i. **Addition**: we define
$$+_F : (x, y) \mapsto F(x, y).$$

ii. **Scalar multiplication**: we define
$$\cdot : (a, x) \mapsto [a]_F(x).$$

Note that if $x, y \in \overline{\mathfrak{m}}$, then $F(x, y) \in K(x, y) \subseteq \overline{K}$, and as $K(x, y)$ is a finite field extension and K is complete, $K(x, y)$ is also complete. Note that $\overline{K}$ is not necessarily complete, but since the terms in the sum are bounded absolutely by 1, the series converges to an element in $\mathfrak{m}_{K(x,y)}$, which lies in $\overline{\mathfrak{m}}$ by definition. Thus $+_F$ is indeed valid. The module axioms then follow as $[a]_F$ is a ring homomorphism. Thus $\overline{\mathfrak{m}_F}$ is indeed a module.

We now define a useful object, which is of interest to us in getting class field theoretic results.

Definition 3.1 (π^n-Division Points)**.** Given a Lubin-Tate $\mathcal{O}_K$-module F for a uniformizer π, for $n > 0$ we can define the group of π^n**-division points** $F(n)$ as

$$F(n) = \{x \in \overline{\mathfrak{m}_F} : [\pi^n]_F = 0\}.$$

Notice that this is just the kernel of the morphism $[\pi^n]_F$, and thus that $F(n)$ is a group follows (under the operation given by F itself).

Since $F(n) \subseteq \overline{\mathfrak{m}_F}$, it also has an inherited structure of it being an $\mathcal{O}_K$-module as it is a group.

In fact, we have that $F(n)$ is free:

Theorem 3.2. *$F(n)$ is a free $\mathcal{O}_K/\pi^n\mathcal{O}_K$ module of rank 1, with q^n elements.*

Proof. Note that by corollary 2.5, all Lubin-Tate modules for π are isomorphic to eachother. Then by definition all of the π^n-division point modules $F(n)$ must also be isomorphic to each other. So we can choose without penalty to work in a specific instance. We choose $F = F_e$ where $e = X^q + \pi X$. Since by definition $e(X) \equiv \pi X \mod X^2$, and $e(X) \equiv X^q \mod \pi$, note that the points of $F(n)$ are the roots of the polynomial $e^n(X)$.

Claim. *$e^n(X)$ has no repeated roots.*

Proof. Suppose that $x \in \overline{K}$. We will proceed by induction on the degree of compositions, n. We will show the result by showing that if $|e^i(x)| < 1$ for $i = 0, 1, \ldots, n-1$, then the formal derivative $e'^i(x)$ does not have x as a root. Note that $e^0 = \text{id}$. Assume thus for this discussion that $|x| < 1$. Then

$$e'(x) = qx^{q-1} + \pi.$$

But note that as $\frac{q}{\pi} \in \mathcal{O}_K$ has $|\frac{q}{\pi}| \leq 1$ and as $|x| < 1$, $|x^{q-1}| < 1$, $e'(x) \neq 0$.

Suppose we have that $e'^k(x) \neq 0$, and that $|e^n(x)| < 1$. Then note

$$e'^{k+1} = (qe^n(x)^{q-1} + \pi)e'^n(x) = \pi(1 + \frac{q}{\pi}e^n(x)^{q-1})e'^n(x).$$

But this clearly cannot be equal to 0. Thus by induction if $|e^i(x)| < 1$ for $i = 0, 1, \ldots, n-1$, then $e'^n(x) \neq 0$.

Assume that $e^n(x) = 0$. Inductively we can build

$$e^n(x) = e \circ e \circ \cdots \circ e(x) = x^{q^n} + \pi f_n(x),$$

for some polynomial $f_n \in \mathcal{O}_K[x]$. If $e^n(x) = 0$, then we must have $|x| < 1$ (otherwise, the function would be increasing). This, however, implies that $|e^i(x)| < 1$ for all $i = 0, 1, \ldots, n-1$. But by the above argument, this implies that $e'^n(x) \neq 0$, and thus the root x has multiplicity 1.

The result follows. □

Note that the above implies that $|F(n)| = q^n$, as $e^n(x)$ has no repeated roots.

Suppose that $\lambda_n \in F(n) \setminus F(n-1)$. Then we have a homomorphism $\varphi : \mathcal{O}_K \to F(n)$ given by $\varphi(a) = a \cdot \lambda_n$. Note that thus $\ker \varphi = \pi^n\mathcal{O}_K$, and by the first isomorphism theorem we have

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \cong F(n).$$

Thus $F(n) \in \mathsf{Mod}_{\mathcal{O}_K/\pi^n\mathcal{O}_K}$ and is free with rank 1. □

Fixing a Lubin-Tate $\mathcal{O}_K$ module F for π, we will denote the field of π^n-division points of F by $L_{n,\pi} = L_n = K(F(n))$. There is clearly an inclusion of fields $L_n \subseteq L_{n+1}$.

Theorem 3.3. The field L_n is determined by π. In particular, it is not dependent on F.

Proof. Let G be another Lubin-Tate $\mathcal{O}_K$ module. As these are all isomorphic to eachother, let $\varphi : F \to G$ be an isomorphism. Then we have $G(n) = \varphi(F(n)) \subseteq K(F(n))$, as the coefficients of the isomorphism f must lie in K. This implies that $K(G(n)) \subseteq K(F(n)) = L_n$.

Similarly, by considering that $F(n) = \varphi^{-1}(G(n)) \subseteq K(G(n))$, we have $L_n = K(F(n)) \subseteq K(G(n))$. In particular, this implies $K(F(n)) = L_n = K(G(n))$, namely that the Lubin-Tate series F does not impact the field L_n. □

We will now assume the results in appendix A for the rest of our discussion.

Let us consider the field

$$L_\infty = \bigcup_{n=1}^{\infty} L_n.$$

The extension L_∞/K is Galois, and we have

$$G_\infty = \mathrm{Gal}(L_\infty/K) \cong \varprojlim_n \mathrm{Gal}(L_n/K),$$

with the inclusion maps $L_n \subseteq L_{n+1}$.

We now identify the Galois groups of these extensions:

Theorem 3.4. Consider the extension L_n/K. Then we have the following:

i. L_n/K is a totally ramified abelian extension of degree $q^{n-1}(q-1)$.

ii. The Galois group

$$\mathrm{Gal}\,(L_n/K) \cong \mathrm{Aut}_{\mathcal{O}_K}(F(n)) \cong U_K/U_K^{(n)}.$$

iii. Given a $\sigma \in \mathrm{Gal}\,(L_n/K)$, there exists a unique $u \in U_K/U_K^{(n)}$ such that for all $x \in F(n)$,

$$\sigma(x) = [u]_F(x).$$

iv. We have for $m \geq n$, that

$$\mathrm{Gal}\,(L_m/L_n) \cong U_K^{(n)}/U_K^{(m)}.$$

v. If $F = F_e$ where $e(X) = X^q + \pi(a_{q-1}X^{q_1} + \cdots + a_2X^2) + \pi X$, where $\lambda_n \in F(n) \setminus F(n-1)$, then λ_n is a uniformizer of L_n and

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = X^{q^{n-1}(q-1)} + \cdots + \pi$$

is the minimal polynomial of λ_n.

vi. We have

$$N_{L_n/K}(-\lambda_n) = \pi.$$

Proof. Let $\sigma \in \mathrm{Gal}\,(L_n/K)$. The induced permutation on $F(n)$ by the action of σ also permutes the roots of $e^n(X)$. Note that we have

$$\sigma(x) +_F \sigma(y) = F(\sigma(x), \sigma(y)) = \sigma(F(x, y)) = \sigma(x +_F y).$$

We also have

$$\sigma(ax) = \sigma([a]_F(x)) = [a]_F(\sigma(x)) = a\sigma(x).$$

This implies that the action of σ on F is linear in $\mathcal{O}_K$, i.e. that we have an injection (as σ was arbitrary)

$$\mathrm{Gal}\,(L_n/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(F(n)).$$

But by theorem 3.2, we have that

$$\mathrm{Aut}_{\mathcal{O}_K}(F(n)) \cong U_K/U_K^{(n)}.$$

Thus (i) follows.

Note that $\phi_n(X)$ is clearly Eisenstein as all of its terms are divisible by π but the constant term $\pi \notin \mathfrak{m}_K^2$. Thus $\lambda_n \in F(n) \setminus F(n-1)$ is a root of $\phi_n(X)$ (as necessarily $e^n(\lambda_n) = 0$) and clearly as $q^n - q^{n-1} = q^{n-1}(q-1)$ ϕ_n is of degree $q^{n-1}(q-1)$. Then this implies that as $\phi_n(\lambda_n) = 0$ that $K(\lambda_n)/K$ is a totally ramified extension of degree $\deg \phi_n$. Since the norm is the constant coefficient of the minimal polynomial, we have that

$$N_{K(\lambda_n)/K}(-\lambda_n) = \pi,$$

and that λ_n is a uniformizer. Thus (v), (vi) follow.

Thus we have

$$\left|U_K/U_K^{(n)}\right| = q^{n-1}(q-1) = [K(\lambda_n) : K] \leq [L_n : K] = |\,\mathrm{Gal}\,(L_n/K)|.$$

But our earlier injection of groups implies that $|\,\mathrm{Gal}\,(L_n/K)| \leq \left|U_K/U_K^{(n)}\right|$, so we must have equality and that implies the injection is thus an isomorphism and $K(\lambda_n) = L_n$.

(iv) follows from noting that the restrictions $\mathrm{Gal}\,(L_m/K) \to \mathrm{Gal}\,(L_n/K)$ and $U_K/U_K^{(m)} \to U_K/U_K^{(n)}$ commute with the above isomorphism. $\square$

Note that thus we have explicitly that

$$G_\infty \cong \varprojlim_n \mathrm{Gal}\,(L_n/K) \cong \varprojlim_n U_K/U_K^{(n)} \cong U_K = \mathcal{O}_K^\times.$$

4. Local Kronecker-Weber

We will assume the statements of Artin reciprocity for this discussion[1]. We now aim to show that, independent of a uniformizer π, that

$$K^{\mathrm{ab}} = K^{\mathrm{ur}} L_\infty.$$

We assume the formulation discussed in appendix B. We will base our discussion on some results discussed in [Li12]. In particular, let ϕ be the induced isomorphism between $G_\infty \to U_K$. We define the reciprocity map $r_\infty : K^\times \to \mathrm{Gal}\,(K^{\mathrm{ur}} L_\infty / K)$ by $\pi^m \cdot u \mapsto (\phi^{-1}(u^{-1}), \mathrm{Frob}^m)$.

We will assume the result of theorem 12 in [Li12], which states that $L^{\mathrm{ur}} L_\infty$ is independent of the choice of uniformizer π.

Then we have the main result:

Theorem 4.1 (Local Kronecker-Weber)**.** We have that

$$K^{\mathrm{ur}} L_\infty = K^{\mathrm{ab}}.$$

Proof. Note that clearly $K^{\mathrm{ur}} L_\infty \subseteq K^{\mathrm{ab}}$, so we have a valid map

$$\mathrm{Art}_{K^{\mathrm{ur}} L_\infty / K} : K^\times \to \mathrm{Gal}\,(K^{\mathrm{ur}} L_\infty / K) \cong \mathrm{Gal}\,(K^{\mathrm{ur}}/K) \times \mathrm{Gal}\,(L_\infty / K).$$

For notational simplicity we will refer to the above Artin map by Art. Note that as π is a norm for L_n/K, for any $\psi = u\pi$, and $m \geq 1$, we have that ψ is a norm for $L_{\psi,m}$. Then by the properties of the Artin map, $\mathrm{Art}(\psi)|_{L_{\infty,\psi}} = \mathrm{id}$, and $\mathrm{Art}(\psi)|_{K^{\mathrm{ur}}} = \mathrm{Frob}$. By lemma 6 in [Li12], this implies that $r(\psi) = \mathrm{Art}(\psi)$, and thus $\mathrm{Art} = r$.

Now assume for the sake of contradiction that $K^{\mathrm{ur}} L_\infty \neq K^{\mathrm{ab}}$. Then the extension $K^{\mathrm{ab}}/K^{\mathrm{ur}} L_\infty$ would be totally ramified and then $\mathrm{Gal}\,(K^{\mathrm{ab}}/K^{\mathrm{ur}} L_\infty) \leq I_{K^{\mathrm{ab}}/K}$. But by the properties of the Artin map, $I_{K^{\mathrm{ab}}/K} = \mathrm{Art}_K(U_K)$. Choose $a \in U_K$ where $a \neq 1$ such that $\mathrm{Art}_K(a)|_{K^{\mathrm{ur}} L_\infty} = \mathrm{id}$, and $\mathrm{Art}_K(a) \neq \mathrm{id}_{K^{\mathrm{ab}}}$. But we have

$$\mathrm{Art}\,|_{K^{\mathrm{ur}} L_\infty} = \mathrm{Art}_{K^{\mathrm{ur}} L_\infty / K}(a) = r(a) \neq 1,$$

as $r|_{U_K}$ is an isomorphism on the group of units, a contradiction by our choice. This implies thus that

$$K^{\mathrm{ab}} = K^{\mathrm{ur}} L_\infty,$$

as desired. ∎

From the above, we obtain the existence theorem of local class field theory:

Theorem 4.2 (Existence Theorem)**.** We have that

i. Art_K induces an isomorphism $K^\times \to W(K^{\mathrm{ab}}/K)$.

[1] It is possible to prove Artin reciprocity using Lubin-Tate theory, which can be seen in [Rie06]. The more conventional way to prove this is using group cohomology.

ii. Any open finite index subgroup of $K^\times$ has the form $N_{L/K}(L^\times)$ for some finite abelian extension L/K.

Proof. The above follows from the isomorphism induced by restricting r to U_K: namely, we have

$$r|_{U_K} = \text{Art}_K|_{U_K} : U_K \cong I_K.$$

□

Thus we have shown that by developing the theory of Lubin-Tate formal groups, we are able to derive some of the results in local class field theory in an elementary manner, without relying on algebraic topology.

References

[Rie06] Emily Riehl. "Lubin-Tate Formal Groups and Local Class Field Theory". Bachelor's Thesis. Harvard University, 2006.

[Li12] Chao Li. *Class Field Theory*. 2012. URL: https://www.math.columbia.edu/~chaoli/docs/ClassFieldTheory2.html#sec18 (visited on 05/15/2024).

[CJ16] Dexter Chua and H. C. Johansson. *Part III - Local Fields*. 2016. URL: https://dec41.user.srcf.net/h/III_M/local_fields/ (visited on 05/15/2024).

[Oh24] Gyujin Oh. *Algebraic Number Theory*. 2024. URL: https://math.columbia.edu/~gyujinoh/Spring2024/ANT.pdf (visited on 05/15/2024).

A. Ramification Theory

We present a brief overview of ramification theory, which generalizes the theory of ramification over Dedekind domains to arbitrary field extensions. In particular, we present filtrations of the Galois groups and generalizations of the inertia group.

Fix a field K. We will denote the **unit group** $U_K = \mathcal{O}_K^\times$. We do this for indexing purposes.

Definition A.1 (Filtration (of Groups)). A **filtration** of groups is a descending chain of groups

$$\cdots \subseteq G_{n+1} \subseteq G_n \subseteq \cdots \subseteq G_1 \subseteq G_0 \subseteq \cdots .$$

Filtrations are a common object seen in algebraic contexts. We now define the groups $U_K^{(s)}$ we have alluded to before (let π_K be a uniformizer)

Definition A.2 (Higher Unit Groups). We define the **higher unit groups** $U_K^{(s)}$ as

$$U_K^{(s)} = 1 + \pi_K^s \mathcal{O}_K,$$

where $U_K^{(0)} = U_K$.

Then notice that we have a filtration

$$\cdots \subseteq U_K^{(s+1)} \subseteq U_K^{(s)} \subseteq \cdots \subseteq U_K^{(1)} \subseteq U_K.$$

The higher unit groups have the following nice property of their quotients:

Theorem A.3. Let $s \geq 1$. Then we have the following:

i. $U_K / U_K^{(1)} \cong k_K^\times$ as a multiplicative group.

ii. $U_K^{(s)} / U_K^{(s+1)} \cong k_K$ as an additive group.

Proof. For (i), we have the surjective projection $a \mapsto a \mod \pi_K$ from $U_K \to U_K^{(1)}$. This projection has kernel $\{a : a \equiv 1 \mod \pi_K\}$, but this is just equal to $U_K^{(1)}$, and the result follows.

For (ii), we will define a surjective homomorphism $\varphi : 1 + \pi_K^s x \mapsto x \mod \pi_K$. Note that

$$(1 + \pi_K^s x)(1 + \pi_K^s y) = 1 + \pi^s(x + y + \pi^s xy) \mapsto x + y + \pi^s xy \equiv x + y \mod \pi_K.$$

Thus φ is indeed a group homomorphism. Then note that the kernel of this map is

$$\ker \varphi = \{a : a \in 1 + \pi_K^{(s+1)} \mathcal{O}_K\} = U_K^{(s+1)},$$

as anything in this set will be mapped to a multiple of π_K and will hence be sent to 0. But then once again by the first isomorphism theorem we have

$$U_K^{(s)} / U_K^{(s+1)} \cong k_K.$$

□

We will now give the corresponding filtration on the Galois groups.

Definition A.4 (Higher Ramification Groups)**.** Fix a finite Galois extension L/K, where L, K are local. Let ν_L be the normalized valuation on L. For $s \geq -1$ we define

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}\,(L/K) : \nu_L(\sigma(x) - x) \geq s + 1 \text{ for all } x \in \mathcal{O}_L\}.$$

Some of the ramification groups have special names, as they can tell us information about the ramification of L/K. As we have defined above, $G_{-1}(L/K) = \mathrm{Gal}\,(L/K)$. We now generalize the notion of the intertia group from Dedekind domains.

Definition A.5 (Inertia Group)**.** Let L/K be a finite Galois extension of local fields. The **inertia group** of L/K, $I_{L/K}$, is the kernel of the homomorphism induced by reduction of

$$\mathrm{Gal}\,(L/K) \to \mathrm{Gal}\,(k_L/k_K).$$

Note that $G_0(L/K) = I_{L/K}$.

If L/K is unramified, then $I_{L/K} = 0$.

B. Artin Reciprocity

For reference, refer to chapter 15 in [Oh24]. We will, for the sake of reference, state the local version of the reciprocity map that we use. First, we must define the Weil group, as this fixes the cases where the local reciprocity map may fail to be an isomorphism.

Definition B.1 (Weil Group)**.** Let K be a local field, and let the extension M/K be Galois. Suppose T^{ur} is the maximal unramified *subextension* of M/K. Then we define the **Weil group** of M/K as

$$W(M/K) = \{\sigma \in \mathrm{Gal}\,(M/K) : \sigma|_{T^{\mathrm{ur}}/K} = \mathrm{Frob}^n_{T^{\mathrm{ur}}/K}\}$$

for some $n \in \mathbb{Z}$. Notice that $W(M/K) \leq \mathrm{Gal}\, M/K$.

In particular, $W(M/K)$ is dense in $\mathrm{Gal}\,(M/K)$. Then we have

Theorem B.2 (Local Artin Reciprocity)**.** Let K be a local field. Then we define the **local Artin map** as the isomorphism

$$\mathrm{Art} : K^\times \to W(K^{\mathrm{ab}}/K) : (\pi^m, u) \mapsto (\mathrm{Frob}^m_k, \sigma_{u^{-1}}),$$

where $\sigma_u(\lambda) = [u]_F(\lambda)$ for all $\lambda \in \cup_n F(n)$. The local Artin map satisfies the properties noted in theorem 15.10 of [Oh24] (adjusted appropriately to account for use of the Weil group instead of $\mathrm{Gal}\, K^{\mathrm{ab}}/K$).

Note that the definition of the map is given by the isomorphism

$$W(K^{\mathrm{ab}}/K) \cong \mathrm{Frob}^{\mathbb{Z}}_K \times \mathrm{Gal}\,(L_\infty/K).$$

Then as a corollary we obtain the following result on norms:

Corollary B.3. We have, for π a uniformizer and $L_n = L_{n,\pi}$,

$$N(L_n/K) = \langle \pi \rangle \times U_K^{(n)}.$$

For the proof, see the sketch idea in section 8.3 of [CJ16].

Index