LUBIN-TATE THEORY

TRISTAN SHIN

Abstract. In this expository paper, we present some concepts in Lubin-Tate theory. Lubin-Tate formal group laws were created by Lubin and Tate as part of their work on generalizing the Kronecker-Weber theorem to local fields. We introduce these group laws and demonstrate some structure that allows us to look at the endomorphism rings of these formal group laws. Then we dive into an explanation of how to construct totally ramified abelian extensions of $\mathbb{Q}_p$, akin to the complex multiplication construction of abelian extensions of imaginary quadratic fields.

1. Introduction

In algebraic number theory, the celebrated Kronecker-Weber theorem states that every algebraic integer with abelian Galois group can be written as a linear combination of roots of unity with coefficients in $\mathbb{Q}$. Translated into field theory terms, we have the following theorem:

Theorem 1.1 (Kronecker-Weber)**.** *Every finite abelian extension $L/\mathbb{Q}$ is a subfield of a cyclotomic field.*

Here, a cyclotomic field is a field extension of $\mathbb{Q}$ formed by adjoining a root of unity.

David Hilbert provided the first known complete proof of this theorem and shortly thereafter asked for generalizations to other base number fields besides $\mathbb{Q}$, as the twelfth of his 23 famed problems [2].

In the case of $\mathbb{Q}(\sqrt{-d})$ for $d > 0$, also known as imaginary quadratic fields, this was resolved by the theory of complex multiplication. The idea behind this is that given an imaginary quadratic field K, there exists an elliptic curve E with endomorphism ring equal to the whole ring of integers $\mathcal{O}_K$ of K. Then the torsion points with order dividing a fixed n form a cyclic $\mathcal{O}_K$-module. From this, we can adjoin these torsion points to K to get abelian extensions of K.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139

E-mail address: shint@mit.edu.

Date: 9 Dec 2021.

This is essentially the only known generalization of the Kronecker-Weber theorem to other number fields. But if we look away from number fields and towards the local fields, it turns out that we can imitate this method to prove a local version of the Kronecker-Weber theorem. This is what Lubin and Tate did in their groundbreaking 1965 paper by introducing a formal group law with special properties [3].

While Lubin and Tate studied arbitrary local fields, we will focus on the familiar p-adic setting of $\mathbb{Q}_p$. This turns out to encapsulate a good amount of the story, as all local fields are isomorphic to one of the following:

- (archimedean, characteristic 0) $\mathbb{R}$, $\mathbb{C}$;
- (non-archimedean, characteristic 0) finite extensions of $\mathbb{Q}_p$; and
- (non-archimedean, non-zero characteristic) $\mathbb{F}_q((T))$ where q is a prime power.

There are some differences, but much of our discussion will be easily generalizable to the arbitrary local field case.

To mirror the tale of imaginary quadratic fields, we will use a formal group law (defined in Section 2) in place of an elliptic curve's group structure. This is because a formal group law is somewhat of a local version of an algebraic group defined on an elliptic curve. These act similarly in that they induce a group structure with large endomorphism ring, which is what complex multiplication deals with. It turns out that to mimic what happens with imaginary quadratic fields, we would like an endomorphism that

- has derivative at 0 equal to p (as an artifact of generalizing to arbitrary local fields which have more primes); and
- acts like the Frobenius endomorphism $x \mapsto x^p$ when reduced modulo p (for reasons related to the roots of its iterates forming cyclic modules).

In Section 2, we will define a family $\mathcal{F}_p$ of power series that have these desired properties.

Why do we consider the whole set $\mathcal{F}_p$ instead of just fixing a single power series? It turns out that all of these Lubin-Tate power series will act isomorphically to each other when we apply them, so the differences will not matter. And, as we will see, there are times when different $f \in \mathcal{F}_p$ are useful.

This paper is split into several sections. In Section 2, we define formal group laws and state their properties. Then we construct specific formal group laws using the Lubin-Tate power series. We then show that these formal groups have useful $\mathbb{Z}_p$-module structures that are isomorphic for different Lubin-Tate power series. In Section 3, we take advantage of the structure of these formal groups to construct totally ramified abelian extensions of $\mathbb{Q}_p$. To do so, we look at what happens when we iterate a Lubin-Tate power series and adjoin the roots to $\mathbb{Q}_p$. In Section 4, we discuss a sketch of the implications of the

results that we demonstrated in the prior sections. Much of the results and ideas are taken from [4] and [5], with original reference to [3].

1.1. **Acknowledgements.** The author would like to thank Tony Feng for providing resources and advice throughout the process of writing this paper, as well as suggesting the topic. The author would also like to thank Anqi Li and Mark Jabbour for providing useful feedback in peer review. This paper was written as part of MIT's Undergraduate Seminar in Number Theory (18.784).

2. Formal Group Laws

In this section, we construct Lubin-Tate formal group laws and prove that their resulting structures are isomorphic. Before this, we review the basic principles of formal group laws and their structure.

2.1. **Basics of formal group laws.** We say that two power series or polynomials (possibly in multiple variables) are congruent modulo $\deg n$ whenever their terms of degree less than n are the same. For example, $X + 2Y + 3X^2 \equiv X + 2Y + 5XY \pmod{\deg 2}$.

A (commutative) **formal group law** over a ring R is a power series $F \in R[[X, Y]]$ such that

- $F(X, Y) \equiv X + Y \pmod{\deg 2}$;
- $F(F(X, Y), Z) = F(X, F(Y, Z))$; and
- $F(X, Y) = F(Y, X)$.

Example 2.1. The simplest example of a formal group law is just $X + Y$, which makes sense – the group structure defined by this formal group law is just the additive group structure of the original ring. Another example of a formal group law is $X + Y + XY = (1 + X)(1 + Y) - 1$. We can directly verify the conditions for this polynomial.

Proposition 2.2. *Given a formal group law F over a ring R, we have that $(XR[[X]], F)$ is an abelian group with identity 0.*

Proof. Commutativity and associativity are implied by the definition. For the identity element, observe that $F(X, 0) \equiv X \pmod{\deg 2}$ and $F(F(X, 0), 0) = F(X, F(0, 0)) = F(X, 0)$. Let $d(X) \coloneqq F(X, 0) - X \equiv 0 \pmod{\deg 2}$. Then $d(X + d(X)) = 0$. But $X + d(X) \equiv X \pmod{\deg 2}$, so if $d(X) \neq 0$ then $d(X+d(X)) \neq 0$, contradiction. Thus $F(X, 0) = X$ and similarly $F(0, Y) = Y$. For inverses, we can compute an inverse coefficient-by-coefficient. Details of the computation are left as an exercise to the reader. □

Given two formal group laws F and G, let $\mathrm{Hom}(F, G)$ denote the set of **homomorphisms** from $(XR[[X]], F)$ to $(XR[[X]], G)$. These are the $f \in XR[[X]]$ such that $f(F(X, Y)) = G(f(X), f(Y))$, also written as $f \circ F = G \circ f$. In the

case that $F = G$, we let $\mathrm{End}(F) = \mathrm{Hom}(F, G)$ denote the set of **endomorphisms**. It is straightforward to check that $\mathrm{End}(F)$ is a ring when using F as addition and composition as multiplication.

Example 2.3. If $F = X + Y$ and $G = X + Y + XY$, we can check that

$$\exp(X) - 1 = \sum_{n=1}^{\infty} \frac{1}{n!} X^n$$

is a homomorphism from the group structure on F to that of G.

2.2. **Lubin-Tate formal group laws.** The discussion about elliptic curves and the resolution to a version of Kronecker-Weber over imaginary quadratic fields motivates us to consider the set of power series $f \in \mathbb{Z}_p[[X]]$ such that

- $f(X) \equiv pX \pmod{\deg 2}$; and
- $f(X) \equiv X^p \pmod{p}$.

We will let $\mathcal{F}_p$ denote this set of power series, and say that any $f \in \mathcal{F}_p$ is a **Lubin-Tate power series**. The simplest example of a Lubin-Tate power series is $pX + X^p$. A less direct example is

$$(1 + X)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i$$

because the binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, \ldots, p-1$ and is 1 for $i = p$.

We can use Lubin-Tate power series to construct formal group laws. To do so, we require the following lemma:

Lemma 2.4. *Let $f, g \in \mathcal{F}_p$ and $L(X_1, \ldots, X_n)$ be a linear form in $\mathbb{Z}_p$. Then there exists a unique $F \in \mathbb{Z}_p[[X_1, \ldots, X_n]]$ such that*

- $F \equiv L \pmod{\deg 2}$*; and*
- $f \circ F = F \circ g$.

Proof. We will prove that for all integers $i \geq 2$, there is an $F_i \in \mathbb{Z}_p[X]$, unique modulo $\deg i$, such that

- $F_i \equiv L \pmod{\deg 2}$; and
- $f \circ F_i \equiv F_i \circ g \pmod{\deg i}$.

For $i = 2$, we can take $F_2 = L$ (which is unique modulo $\deg 2$ by definition), as

$$\begin{aligned} f \circ L &\equiv p \cdot L(X_1, \ldots, X_n) \pmod{\deg 2} \\ &\equiv L(pX_1, \ldots, pX_n) \pmod{\deg 2} \\ &\equiv L \circ g \pmod{\deg 2}. \end{aligned}$$

Now, we can perform induction on i to obtain the other F_i. Suppose that we have constructed F_i for some $i \geq 2$. Then F_{i+1} reduced modulo $\deg i$ must satisfy the same criterion as F_i, so $F_{i+1} = F_i + D_i$ for some $D_i \equiv 0 \pmod{\deg i}$. Then

$$\begin{aligned} f \circ F_{i+1} &= f(F_i + D_i) \\ &\equiv f(F_i) + f'(F_i)D_i \pmod{\deg(i+1)} \end{aligned}$$

by Taylor expansion. But $f'(X) \equiv p \pmod{\deg 1}$, so

$$f \circ F_{i+1} \equiv f \circ F_i + pD_i \pmod{\deg(i+1)}.$$

Similarly,

$$\begin{aligned} F_{i+1} \circ g &= F_i \circ g + D_i \circ g \\ &\equiv F_i \circ g + p^i \cdot D_i \pmod{\deg(i+1)} \end{aligned}$$

because $g(X) \equiv pX \pmod{\deg 2}$. So we must have

$$D_i \equiv \frac{f \circ F_i - F_i \circ g}{p^i - p} \pmod{\deg(i+1)}.$$

We can check that

$$f \circ F_i - F_i \circ g \equiv F_i(X_1, \ldots, X_n)^p - F_i(X_1^p, \ldots, X_n^p) \equiv 0 \pmod{p}$$

by Fermat's little theorem, so $\frac{f \circ F_i - F_i \circ g}{p^i - p}$ has coefficients in $\mathbb{Z}_p$. Thus F_{i+1} is uniquely determined modulo $\deg(i+1)$. Then we can take $F \in \mathbb{Z}_p[[X]]$ to be the limit of $F_i \in \mathbb{Z}_p[X]$, which exists because $F_{i+1} \equiv F_i \pmod{\deg i}$. □

Fix an $f \in \mathcal{F}_p$. We can directly apply the lemma to retrieve a unique $F_f(X, Y) \in \mathbb{Z}_p[[X, Y]]$ satisfying

- $F_f(X, Y) \equiv X + Y \pmod{\deg 2}$; and
- $f \circ F_f = F_f \circ f$.

Proposition 2.5. *The power series F_f is a formal group law.*

Proof. The first axiom is true by definition of F_f. For the second axiom, observe that

- $F_f(F_f(X, Y), Z) \equiv X + Y + Z \pmod{\deg 2}$; and
- $f(F_f(F_f(X, Y), Z)) = F_f(F_f(f(X), f(Y)), f(Z))$,

and similarly with $F_f(X, F_f(Y, Z))$, so the uniqueness part of Lemma 2.4 implies that $F_f(F_f(X, Y), Z) = F_f(X, F_f(Y, Z))$. A similar argument holds for the third axiom. □

This group law F_f is called a **Lubin-Tate formal group law**. By definition, it satisfies $f \in \mathrm{End}(F_f)$.

Example 2.6. When $f = (1+X)^p - 1$, we can check that the Lubin-Tate formal group law is $F_f(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$.

For $a \in \mathbb{Z}_p$ and $f, g \in \mathcal{F}_p$, we also introduce $[a]_{f,g}(X) \in \mathbb{Z}_p[[X]]$ using the lemma to be the unique power series such that

- $[a]_{f,g}(X) \equiv aX \pmod{\deg 2}$; and
- $f \circ [a]_{f,g} = [a]_{f,g} \circ g$.

For shorthand, let $[\,\cdot\,]_f = [\,\cdot\,]_{f,g}$.

Example 2.7. When $f = (1+X)^p - 1$, we can check that

$$[a]_f = \sum_{m=1}^{\infty} \binom{a}{m} X^m = (1+X)^a - 1.$$

This can be done by verifying the conditions on $[a]_f$ when $a \in \mathbb{Z}$ and applying continuity.

The following three propositions can be proved in a similar fashion as Proposition 2.5.

Proposition 2.8. *For all $a \in \mathbb{Z}_p$ and $f, g \in \mathcal{F}_p$, we have that $[a]_{f,g}$ is in $\mathrm{Hom}(F_g, F_f)$. In particular, $[a]_f$ is in $\mathrm{End}(F_f)$.*

The next proposition demonstrates that composition of this constructed homomorphism acts like multiplication over $\mathbb{Z}_p$.

Proposition 2.9. *For all $a, b \in \mathbb{Z}_p$ and $f, g, h \in \mathcal{F}_p$, we have the equality $[a]_{f,g} \circ [b]_{g,h} = [ab]_{f,h}$.*

The third proposition describes a situation that we call **complex multiplication** by $\mathbb{Z}_p$, much similar to the corresponding situation in imaginary quadratic fields.

Proposition 2.10. *The map $[\,\cdot\,]_f \colon \mathbb{Z}_p \to \mathrm{End}(F_f)$ is an injective ring homomorphism satisfying $[p]_f = f$.*

These three propositions have key implications. For a ring R, we say that a **formal R-module** is a pair (F, ρ) where F is a formal group law and ρ is a ring homomorphism from $R \hookrightarrow \mathrm{End}(F)$ such that $\rho(a) \equiv aX \pmod{\deg 2}$. Then Proposition 2.10 implies that $(F_f, [\,\cdot\,]_f)$ is a formal $\mathbb{Z}_p$-module, and the definition of $[\,\cdot\,]_f$ implies that this is the unique $\mathbb{Z}_p$-module with formal group F_f. Thus it is clear what context we refer to when saying that F_f is a formal $\mathbb{Z}_p$-module.

Theorem 2.11. *For any $f, g \in \mathcal{F}_p$, the formal $\mathbb{Z}_p$-modules F_f and F_g are isomorphic.*

Proof. By Proposition 2.9, we know that $[1]_{f,g} \circ [1]_{g,f} = [1]_f = X$, so it follows that $[1]_{g,f} \colon F_f \to F_g$ is an isomorphism. □

This is particularly important, because it means that the formal group and formal $\mathbb{Z}_p$-modules generated through this process are isomorphic, regardless of which $f \in \mathcal{F}_p$ was chosen at the start.

3. Generating Extensions

In this section, we analyze the roots of the power series given by iterating the Lubin-Tate formal group law. We then demonstrate that these roots generate special abelian extensions of $\mathbb{Q}_p$. The purpose of generating these extensions is as a piece of the larger picture to construct a maximal abelian extension of local fields in local class field theory, as well as prove the local version of the Kronecker-Weber theorem.

3.1. **Generating $\mathbb{Z}_p$-modules isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.** Fix an $f \in \mathcal{F}_p$, though the choice is not important as demonstrated by Theorem 2.11. Then the formal $\mathbb{Z}_p$-module F_f induces a $\mathbb{Z}_p$-module on $\mathfrak{m}^{\mathrm{al}} \coloneqq \left\{\alpha \in \overline{\mathbb{Q}_p} : |\alpha| < 1\right\}$ with addition given by F_f and scalar multiplication given by $a \cdot \alpha = [a]_f(\alpha)$ for $a \in \mathbb{Z}_p, \alpha \in \mathfrak{m}^{\mathrm{al}}$. Here, $\overline{\mathbb{Q}_p}$ represents the algebraic closure of $\mathbb{Q}_p$.

Define $\Lambda_{f,n}$ to be the set of roots of $[p^n]_f = f^n$ in $\mathfrak{m}^{\mathrm{al}}$, where the notation $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$ denotes iteration. Then $\Lambda_{f,n}$ is a submodule of $\mathfrak{m}^{\mathrm{al}}$. These $\mathbb{Z}_p$-modules turn out to have nice structure.

Proposition 3.1. *The $\mathbb{Z}_p$-module $\Lambda_{f,n}$ is isomorphic to $\mathbb{Z}_p/p^n\mathbb{Z}_p$.*

Proof. It suffices to prove this statement for a single Lubin-Tate power series f, as the structure of $\Lambda_{f,n}$ will be the same because of the isomorphism of Theorem 2.11. We can choose $f(X) = (1+X)^p - 1$. Then $f^n(X) = (1+X)^{p^n} - 1$, so $\Lambda_{f,n} = \left\{-1 + \zeta : \zeta^{p^n} = 1\right\}$. Recall that the group law is $F(X,Y) = (1+X)(1+Y) - 1$. Thus addition in $\Lambda_{f,n}$ corresponds to multiplication on the set of (p^n)th roots of unity, so $\Lambda_{f,n} \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$. □

We provide a brief sketch of a different, albeit longer and more technical, proof. The benefit of this proof is that it generalizes nicely to the scenario where $\mathbb{Q}_p$ is replaced by an arbitrary local field.

Sketch of alternative proof. We can choose $f(X) = pX + X^p$. Then we can apply the structure theorem for finitely generated modules to get that

$$\Lambda_{f,n} \cong (\mathbb{Z}_p/p^{k_1}\mathbb{Z}_p) \times \cdots \times (\mathbb{Z}_p/p^{k_m}\mathbb{Z}_p)$$

for some unique $1 \le k_1 \le \cdots \le k_m$. For $n = 1$, we can check that f has p distinct roots in $\mathfrak{m}^{\mathrm{al}}$, so $\Lambda_{f,1} \cong \mathbb{Z}_p/p\mathbb{Z}_p$. Then we can proceed by induction.

We can show that f restricted to $\Lambda_{f,n} \to \Lambda_{f,n-1}$ is surjective. This allows us to deduce that $|\Lambda_{f,n}| = p^n$ and that $\Lambda_{f,n}$ must be cyclic. Thus $\Lambda_{f,n}$ must be isomorphic to $\mathbb{Z}_p/p^n\mathbb{Z}_p$. □

3.2. **Totally ramified abelian extensions of $\mathbb{Q}_p$.** Let K be a local field. We say that a finite extension L/K is **totally ramified** if π_K, π_L are prime elements of L, K and $\pi_K = \pi_L^{[L:K]}$. It turns out that totally ramified extensions can be characterized by adjoining roots of certain polynomials.

Let $\mathcal{O}_K \coloneqq \{\alpha \in K : v_K(\alpha) \geq 0\}$ be the ring of integers of K, where v_K is the valuation over K. We say that a polynomial in $\mathcal{O}_K[X]$ is an **Eisenstein polynomial** if takes the form $X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$ where $v_K(a_i) \geq 1$ for $i = 1, \ldots, m-1$ and $v_K(a_0) = 1$. It can be shown that an Eisenstein polynomial is irreducible over K [1]. Then it can be shown that L/K is totally ramified if and only if $L = K[\alpha]$, where α is a root of an Eisenstein polynomial.

Now, we consider the field $L_n \coloneqq \mathbb{Q}_p[\Lambda_{f,n}]$, the field extension of $\mathbb{Q}_p$ generated by $\Lambda_{f,n}$. Note that while the submodule $\Lambda_{f,n}$ depends on f, this field extension does not because $\mathbb{Q}_p[\Lambda_{f,n}]/\mathbb{Q}_p$ is the splitting field of f^n and is thus Galois.

Remark 3.2. This is a key parallel to the setup of complex multiplication in imaginary quadratic fields. In that setting, we adjoin the torsion points of the elliptic curve to the original field to generate extensions. Here, we adjoin points that are killed by the p^n map.

This extension turns out to have desired properties. The proof of the following theorem is based on that as written in Milne's notes on Class Field Theory [4].

Theorem 3.3. *The field extension $L_n/\mathbb{Q}_p$ is totally ramified abelian extension of degree $p^{n-1}(p-1)$. Furthermore, the Galois group of this extension is congruent to $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$.*

Proof. We can choose $f(X) = pX + X^p$ for simplicity. Inductively construct a sequence such that α_1 is a nonzero root of f and α_{i+1} is a root of $f - \alpha_i$ for $i \geq 2$. We can easily verify that $f - \alpha_i$ is Eisenstein over $\mathbb{Q}_p[\alpha_i]$, so $\mathbb{Q}_p[\alpha_{i+1}]/\mathbb{Q}_p[\alpha_i]$ is totally ramified of degree p. Similarly $\mathbb{Q}_p[\alpha_1]/\mathbb{Q}_p$ is totally ramified of degree $p-1$. Thus $\mathbb{Q}_p[\alpha_n]/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$.

Now recall that L_n is the splitting field of f^n, so $\mathrm{Gal}(L_n/\mathbb{Q}_p)$ corresponds to a subgroup of $\mathrm{Sym}(\Lambda_{f,n})$. We can check that the elements of $\mathrm{Gal}(L_n/\mathbb{Q}_p)$ act on $\Lambda_{f,n}$ as an automorphism, so the subgroup must also be a subgroup of $\mathrm{Aut}(\Lambda_{f,n})$. Using Proposition 3.1, we can show that $\mathrm{Aut}(\Lambda_{f,n}) \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$. Thus $\mathrm{Gal}(L_n/\mathbb{Q}_p)$ is isomorphic to a subgroup of $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$.

But all of this implies that

$$\begin{aligned} p^{n-1}(p-1) = [\mathbb{Q}_p[\alpha_n] : \mathbb{Q}_p] &\leq [\mathbb{Q}_p[\Lambda_{f,n}] : \mathbb{Q}_p] = \mathrm{Gal}(L_n/\mathbb{Q}_p) \\ &\leq |(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times| = p^{n-1}(p-1), \end{aligned}$$

so equality must hold at every step.

In particular:

- $L_n = \mathbb{Q}_p[\Lambda_{f,n}] = \mathbb{Q}_p[\alpha_n]$, so
- $[L_n : \mathbb{Q}_p] = p^{n-1}(p-1)$; and
- $\mathrm{Gal}(L_n/\mathbb{Q}_p) \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$.

As $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$ is cyclic, $L_n/\mathbb{Q}_p$ is totally ramified abelian extension of degree $p^{n-1}(p-1)$. □

As a result, we have generated several totally ramified abelian extensions of $\mathbb{Q}_p$. We can also consider what happens as $n \to \infty$. Let $L_\infty = \cup L_n$. To analyze L_∞, we need to consider an idea that generalizes the construction of $\mathbb{Z}_p$.

Let $\{A_i\}$ be a sequence of groups, and suppose we have a set of homomorphisms $f_{i,j} \colon A_j \to A_i$ satisfying

(1) $f_{i,i}$ is the identity; and
(2) $f_{i,k} = f_{i,j} \circ f_{j,k}$ for all $i \leq j \leq k$.

Then we say that the **inverse limit** of this system is the set of sequences $\{a_i\}$ with $a_i \in A_i$ such that $a_i = f_{i,j}(a_j)$ for all $i \leq j$. We denote this by $\varprojlim A_i$.

Example 3.4. If $A_i = \mathbb{Z}/p^i\mathbb{Z}$ and $f_{i,j}$ is the map that reduces modulo p^i, then the inverse limit is $\mathbb{Z}_p$. Indeed, the sequences that we want are the "coherent sequences" such that later terms match earlier terms when we take them modulo powers of p.

Using the notion of an inverse limit, we can show that

$$\mathrm{Gal}(L_\infty/\mathbb{Q}_p) = \varprojlim \mathrm{Gal}(L_n/\mathbb{Q}_p) \cong \varprojlim (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

But we can see that the construction of $\mathbb{Z}_p$ using an inverse limit works similarly if we remove all non-invertible elements, so we actually get that $\mathrm{Gal}(L_\infty/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$.

4. Conclusion

In this section, we describe how the preceding facts tie in with local class field theory and the local Kronecker-Weber theorem.

4.1. **Maximal abelian extension and local Kronecker-Weber.** Recall our definition of a totally ramified extension of a local field K. We can go the other direction and say that a finite extension L/K is **unramified** if the prime elements of K are still prime in L. Then local class field theory provides that K^{un}, the maximal unramified abelian extension of $\mathbb{Q}_p$, is the union of the field extensions formed by adjoining the nth roots of unity to $\mathbb{Q}_p$ for n relatively prime to p.

If we know K_p, the maximal totally ramified abelian extension of $\mathbb{Q}_p$, then local class field theory also provides that $K^{\text{ab}} = K^{\text{un}}K_p$, where K^{ab} is the maximal abelian extension of $\mathbb{Q}_p$. So if we can generate K_p, then we can generate K^{ab}.

Fortunately, the work that we have done with Lubin-Tate theory provides us exactly that. With more work, we can prove that the infinite extension $L_\infty = \cup L_n$ that we constructed in Section 3 is actually K_p. Thus Lubin-Tate theory allows us to explicitly construct the maximal abelian extension of $\mathbb{Q}_p$.

A consequence of this construction is that every finite abelian extension $L/\mathbb{Q}_p$ is a subfield of a cyclotomic field over $\mathbb{Q}_p$. This is the local Kronecker-Weber theorem. As an added bonus, it can be shown that the local Kronecker-Weber theorem implies the global (original) version. This is described in more detail in [6]. It follows that the simple structure of the Lubin-Tate power series over $\mathbb{Z}_p$ provides much grander structures that pave the way for important results about abelian extensions of $\mathbb{Q}_p$.

References

[1] G. Eisenstein. Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *J. Reine Angew. Math.*, 39:160–179, 1850.

[2] D. Hilbert. Ein neuer beweis des kronecker'schen fundamentalsatzes über abel'sche zahlkörper. *Gött. Nachr.*, pages 29–39, 1896.

[3] J. Lubin and J. Tate. Formal complex multiplication in local fields. *Ann. of Math. (2)*, 81:380–387, 1965.

[4] J. Milne. Class Field Theory. 1997.

[5] E. Riehl. Lubin-Tate Formal Groups and Local Class Field Theory. 2006.

[6] A. Sutherland. The Kronecker-Weber theorem. 2015.