universität
wien

MASTERARBEIT

Titel der Masterarbeit

"Lubin-Tate extensions and division points on the elliptic curve $y^2 = x^3 + x$"

verfasst von

Jakob Preininger BSc

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2013

Studienkennzahl lt. Studienblatt:	A 066 821
Studienrichtung lt. Studienblatt:	Masterstudium Mathematik
Betreut von:	ao. Univ.-Prof. Dr. Joachim Mahnkopf

Contents

1. Introduction 3

2. Local Fields 6

2.1. Absolute values and valuations 6

2.2. Completions of absolute values 9

2.3. Residue class degree, ramification index and discrete valuations 11

2.4. Unramified and totally ramified extensions 13

2.5. The definition and the list of local fields 15

2.6. Ramification and solubility of local field extensions 16

2.7. The multiplicative group of local fields 17

3. Local Class Field Theory 20

3.1. The local reciprocity law and the norm residue symbol 20

3.2. Formal groups and Lubin-Tate modules 22

4. Elliptic Curves and Complex Multiplication 28

4.1. Basic facts about elliptic curves 28

4.2. Addition on elliptic curves and $E(\mathbb{C})$ as complex Lie group 30

4.3. Isogenies and complex multiplication 31

4.4. Division points and Galois actions 33

5. Abelian Extensions of $\mathbb{Q}(i)$ and Ramification of Prime Ideals in these Extensions 35

5.1. Abelian extensions of $\mathbb{Q}(i)$ 35

5.2. Division polynomials 36

5.3. The criterion of Néron-Ogg-Shafarevic 37

5.4. Ramification of primes in the extension $\mathbb{Q}(i)(E[n])/\mathbb{Q}(i)$ 39

5.5. Lubin-Tate prime elements 56

6. Summary and conclusion 61

6.1. Summary of the results 61

6.2. Conclusion 63

Appendix: Mathematica Listing 64

References 73

Abstract 74

Zusammenfassung 75

Curriculum Vitae 77

1. Introduction

The aim of this thesis is to compare the theory of Lubin-Tate modules, which describe ramified abelian extensions of local fields, to the theory of elliptic curves with complex multiplication, which also can be used to generate abelian extensions of (global) imaginary quadratic fields, and thereby establish a more explicit understanding of class field theory.

Lubin-Tate modules are a generalization of the local version of the Theorem of Kronecker-Weber (Thm. 62), which says that any finite abelian extension of $\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$ for some root of unity ζ. The existence theorem (Thm. 59) of local class field theory tells us that there is a one-to-one inclusion reversing correspondence between the finite abelian extensions L of the local field K and the open subgroups of finite index in the group K^* via the map $L \mapsto N_{L/K}(L^*)$. The structure of K^* is given by $K^* = \langle \pi \rangle \times U$ (cf. Prop. 50) where π is an arbitrary prime in the valuation ring O_K and $U := O_K^*$ the group of units of O_K. Hence, every open subgroup of finite index contains a subgroup $G_{f,k}(\pi)$ of the form $\langle \pi^f \rangle \times U^{(k)}$ for some $f, k \in \mathbb{N}$ where $U^{(k)} = \{x \in U : x \equiv 1 \mod \mathfrak{p}_K^k\}$ and π is some prime in O_K, which is not uniquely determined (for example one can replace π by πu for any $u \in U^{(k)}$). While the subgroups $G_{f,0}(\pi)$ correspond to unramified extensions K_f, which do not depend on the prime π chosen and can be obtained easily by adjoining certain roots of unity (cf. Thm. 35), the groups $G_{1,k}(\pi)$ correspond to totally ramified extensions $K_{\pi,k}$ which can be described explicitly by adjoining π^k division points of some Lubin-Tate module w.r.t. π (cf. Ch 3.2). The product $K_{f,k}(\pi)$ of these two extensions K_f and $K_{\pi,k}$ then corresponds to the subgroup $G_{f,k}(\pi)$ of K^* and in this case we call π a "Lubin-Tate prime element" of $K_{f,k}(\pi)$. In total we get that every finite abelian extension is only contained in such a field $K_{f,k}(\pi)$, that can be described explicitly via Lubin-Tate modules.

For imaginary quadratic fields (i.e. fields of the form $K = \mathbb{Q}(\sqrt{d})$ with d squarefree and $d < 0$) there is a global way to construct abelian extensions explicitly (cf. [9, Ch 2]): For the ring of integers O_K of K we take an elliptic curve $\tilde{E}$ over $\mathbb{C}$ with endomorphism ring $End(\tilde{E}) = O_K$

(i.e. E has complex multiplication; cf. Ch. 4.3) and determine its j-invariant $j(\tilde{E})$. Then one can show (cf. [9, Ch 2 Thm 4.3]) that the field $K(j(\tilde{E}))$ is the Hilbert class field of K (i.e. the maximal extension that is unramified in all prime ideals of O_K) and that we can construct an isomorphic elliptic curve E (i.e. with the same j-invariant but different Weierstrass equation) which is defined over $K(j(\tilde{E}))$. Now the maximal abelian extension of K can be obtained by adjoining the torsion points of E to $K(j(E))$ (cf. [9, Ch 2 Kor 5.7]).

To examine the connection between these two methods that yield abelian extensions more explicitly we consider the imaginary quadratic field $K = \mathbb{Q}(i)$. A suitable elliptic curve E with $End(E) \cong \mathbb{Z}[i]$ is given by the equation $y^2 = x^3 + x$, which has j-invariant $j(E) = 1728$ and is defined over $\mathbb{Q}(i)$. Its division points, which generate abelian extensions $K[n]/\mathbb{Q}(i)$, can be described as roots of the so called division polynomials for E (see Ch. 5.2). If we want to compare these extensions $K[n]/\mathbb{Q}(i)$ with Lubin-Tate extensions we have to look at those primes where $K[n]/\mathbb{Q}(i)$ ramifies. This can be done via the Criterion of Néron-Ogg-Shafarevic (see 5.3). Now if $\mathfrak{p}$ is a prime that ramifies in $K[n]$ and $\mathfrak{P}$ is a prime in $K[n]$ lying over $\mathfrak{p}$ then we want to find whether there is a Lubin-Tate prime element π of $\mathbb{Q}(i)_\mathfrak{p}$ and $f, k \in \mathbb{N}$ such that $K[n]_\mathfrak{P}$ corresponds to the subgroup $G_{f,k}(\pi)$ of $\mathbb{Q}(i)_\mathfrak{p}^*$. As a first step to this end we need to find the ramification index e and the residue class field degree f of the extension $K[n]_\mathfrak{P}/\mathbb{Q}(i)_\mathfrak{p}$. This limits us to 3- and 4-divison points because there is no general way to determine the values e and f explicitly by just knowing the field extension via a minimal polynomial. For $n = 3, 4$ however one can describe generators for the extensions $K[n]/\mathbb{Q}(i)$ explicitly and hence one can obtain the needed ramification indices, residue class field degrees and the generators of the prime ideals $\mathfrak{P}$ via calculating generators of the rings of integers of these extensions and Kummer's theorem (cf. Thm. 114). If $K[n]_\mathfrak{P}$ corresponds to some $G_{f,k}(\pi)$ then the value f has to be the residue class field degree and for k and the ramification index e we have the relation $e = [U : U^{(k)}]$. When we have determined the indices f, k we use the theory of Lubin-Tate modules to find out whether a suitable Lubin-Tate prime element π exists (i.e. whether $N(K[n]_\mathfrak{P}^*) = G_{f,k}(\pi)$ for some $\pi \in \mathbb{Q}(i)_\mathfrak{p}$).

We summarize our results as follows: We get that there are 3 pairs $(n, \mathfrak{p})$ where the extension $K[n]_{\mathfrak{P}}/\mathbb{Q}(i)_{\mathfrak{p}}$ ramifies: $(3,(3)), (3,(1+i))$ and $(4,(1+i))$. While for $(n,\mathfrak{p}) = (3,(3))$ the extension $K[3]_{\mathfrak{P}}/\mathbb{Q}(i)_{\mathfrak{p}}$ corresponds to the subgroup $G_{1,1}(\pi)$, where $\pi = -3$ (i.e. the extension is a Lubin-Tate extension), for $(n,\mathfrak{p}) = (3,(1+i)), (4,(1+i))$ the subgroups $N_{K[n]_{\mathfrak{P}}/\mathbb{Q}(i)_{\mathfrak{p}}} K[n]^*_{\mathfrak{P}}$ of $\mathbb{Q}(i)^*_{\mathfrak{p}}$ are not of the form $G_{f,k}(\pi)$. The residue class field degree f and the ramification index e of these extensions would suggest that the subgroups would be of the form $G_{2,3}(\pi)$ for $n = 3$ resp. $G_{1,2}(\pi)$ for $n = 4$ but there does not exist any suitable prime π in either case. (cf. Ch. 5.5).

The fact that not all the ramified extensions $K[n]_{\mathfrak{p}}$ are Lubin-Tate extensions does not suggest that there is any easy connection between those two methods that generate maximal abelian extensions. Unfortunately the number of results we could calculate here is not large enough to specify this statement any further and the methods used in this paper to obtain the necessary ramification data are not easily generalizable to extensions of higher degrees.

I would like to express my gratitude to my supervisor Professor Joachim Mahnkopf, for his constant support on this thesis.

2. Local Fields

This chapter is a brief summary of the definitions and results needed for the notion of a local field and its structure. For a more detailed introduction with proofs see [5, §23-25] or [7, Ch 2].

2.1. **Absolute values and valuations.**

In analogy to norms in vector spaces we define the notion of an absolute value for fields K in the following way:

Definition 1. Let K be a field. A map $|\cdot| : K \to \mathbb{R}_0^+$ is called *absolute value* on K if the following conditions are satisfied[1]:

(i) $\forall a \in K : |a| = 0 \Leftrightarrow a = 0$
(ii) $\forall a, b \in K : |ab| = |a| \cdot |b|$
(iii) $\forall a, b \in K : |a + b| \leq |a| + |b|$ (triangular inequality).

Axiom (ii) of the above definition implies that $|\cdot|$ is a homomorphism from the multiplicative group K^* to the multiplicative group $\mathbb{R}^+$. The image of this homomorphism is called the value group of $|\cdot|$.

Example 2. On $\mathbb{C}$ (and every subfield of $\mathbb{C}$) there is the *usual absolute value* which we denote by $|\cdot|_\infty$.

Example 3. If $|\cdot|$ is an absolute value on a field L and K a subfield of L. Then by restriction we get an absolute value on K which we also denote by $|\cdot|$.

Example 4. For every field K there is the *trivial absolute value* given by

$$|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}.$$

Conversely since $\mathbb{R}^+$ is torsion free every torsion element of K has to have absolute value 1. Especially every finite field has no nontrivial absolute value.

Example 5. If $|\cdot|$ is an absolute value on K and $\rho \in \mathbb{R}$ with $0 < \rho \leq 1$. Then $|\cdot|^\rho$ is also an absolute value on K.[2]

[1] We write $\mathbb{R}^+$ for the set of positive real numbers and $\mathbb{R}_0^+$ for the set of non-negative real numbers.

[2] In fact in most cases $|\cdot|^\rho$ is an absolute value for all $\rho > 0$. Cf. Prop. 11(iv)

Example 6. Let $K \subset \mathbb{C}$ be an algebraic field extension of $\mathbb{Q}$ and $\sigma \in Gal(K/\mathbb{Q})$ then $|\cdot|_\sigma$ given by $|x|_\sigma = |\sigma(x)|_\infty$ (where $|\cdot|_\infty$ is the restriction of the usual absolute value $|\cdot|_\infty$ on $\mathbb{C}$) is an absolute value on K, which in general differs from $|\cdot|_\infty$ on K.

Example 7. Let p be a prime and for $x \in \mathbb{Q}^*$ let $\nu_p(x)$ denote the exponent of p in the prime factorization of x. Then define an absolute value on $\mathbb{Q}$ by $|x|_p = \begin{cases} p^{-\nu_p(x)} & x \in \mathbb{Q}^* \\ 0 & x = 0 \end{cases}$. One calls $|\cdot|_p$ the *p-adic absolute value* on $\mathbb{Q}$.

Like norms an absolute value $|\cdot|$ on a field K defines a metric and hence a topology on K. In particular we have the notions of convergence, Cauchy-sequences, open sets, continuity, etc. on K. For example one can easily verify that addition and multiplication and their inversions on K become continuous functions on K and therefore K becomes a *topological field.*

Definition 8. Two absolute values $|\cdot|_1$, $|\cdot|_2$ are called *equivalent* ($|\cdot|_1 \sim |\cdot|_2$) if they induce the same notions of convergence (i.e. every null-sequence of $|\cdot|_1$ is a null-sequence of $|\cdot|_2$ and vice versa).

One has the following criterion for equivalence of absolute values:

Proposition 9. *(cf.* [5, §23 p.56f]*) For nontrivial absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K there are equivalent:*
(i) $|\cdot|_1 \sim |\cdot|_2$.
(ii) There exists $\rho \in \mathbb{R}^+$such that $|\cdot|_1 = |\cdot|_2^\rho$.
(iii) For any $x \in K$ we have $|x|_1 < 1$ implies $|x|_2 < 1$.

One can distinguish between two different important types of absolute values:

Definition 10. An absolute value $|\cdot|$ on a field K is called *archimedean* if the set $\{|n| = |n \cdot 1_K| : n \in \mathbb{N}\} \subset \mathbb{R}$ is unbounded. Otherwise $|\cdot|$ is called *non-archimedean.*

Non-archimedean absolute values have some important properties given in the following proposition.

Proposition 11. *(cf.* [5, §23 p.58]*) Let $|\cdot|$ be an absolute value on a field K. Then the following statements are equivalent:*

(i) $|n| \leq 1$ *for every* $n \in \mathbb{N}$*.*

(ii) $|\cdot|$ *is non-archimedean.*

(iii) $|\cdot|$ *fulfills the strong triangular inequality:*

$$\forall a, b \in K : \ |a+b| \leq max(|a|, |b|).$$

(For $|a| \neq |b|$ *we even get* $|a+b| = max(|a|, |b|)$*.)*

(iv) For every real number $\rho > 0$ *we have that* $|\cdot|^{\rho}$ *is an absolute value on* K*.*

For the field $\mathbb{Q}$ there are only those absolute values already mentioned above.

Theorem 12. *(cf.* [5, §23 p.59]*) Every non-trivial absolute value on* $\mathbb{Q}$ *is either equivalent to some p-adic absolute value* $|\cdot|_p$ *or to the usual archimedean absolute value* $|\cdot|_{\infty}$*.*

Now we can define the important notions of valuation ring, valuation ideal and residue class field which are fundamental for the definition of local fields.

Definition 13. Let $|\cdot|$ be a non-archimedean absolute value on a field K.

(i) The set $R := \{x \in K : |x| \leq 1\}$ is a local ring with $K = Quot(R)$ called the *valuation ring* of K w.r.t. $|\cdot|$.

(ii) $\mathfrak{p} := \{x \in K : |x| < 1\}$ is the maximal ideal in R called the *valuation ideal* of K w.r.t. $|\cdot|$.

(iii) $\kappa := R/\mathfrak{p}$ is hence a field and is called the *residue class field* of K w.r.t. $|\cdot|$.

Example 14. For $|\cdot|_p$ on $\mathbb{Q}$ the valuation ring is given by $R = \mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$. The valuation ideal is the principal ideal pR of R and the residue class field is canonically isomorphic to the field $\mathbb{F}_p$.

For non-archimedean absolute values it is sometimes useful to change from the multiplicative function $|\cdot|$ to an additive function.

Definition 15. Let K be a field. A *valuation* on K is a map $\nu : K \to \mathbb{R} \cup \{\infty\}$ with the following properties:

(i) $\nu(a) = \infty \iff a = 0$.

(ii) $\forall a, b \in K : \nu(ab) = \nu(a) + \nu(b)$.
(iii) $\forall a, b \in K : \nu(a+b) \geq min\{\nu(a), \nu(b)\}$.
The Image of K^* under ν is a subgroup of the additive group of $\mathbb{R}$ and is called the *value group* of ν.

If ν is a valuation on K one gets a non-archimedean absolute value by setting $|x| = c^{\nu(x)}$ for some real number $0 < c < 1$. If we use a different c we get an equivalent absolute value. Conversely: Given a non-archimedean absolute value $|\cdot|$ and a real number $0 < c < 1$ one gets a valuation by setting $\nu(x) = \log_c |x|$ for $x \neq 0$ and $\nu(0) = \infty$.

Example 16. For any prime p the exponent map ν_p given in the definition of $|\cdot|_p$ defines a valuation on $\mathbb{Q}$ with value group $\mathbb{Z}$.

2.2. **Completions of absolute values.** Like the real numbers, local fields will be complete:

Definition 17. Let $|\cdot|$ be an absolute value on K. Then K is called *complete* w.r.t. $|\cdot|$ if every Cauchy-sequence in K converges to some element in K.

To obtain a complete field one starts with some field K and an absolute value $|\cdot|$. Then one "adds" some elements to K so that K becomes complete:

Definition 18. Let $|\cdot|$ be an absolute value on K. Then a field extension $\hat{K}$ of K with absolute value $|\hat{\cdot}|$ is called *completion* of K if the following conditions are satisfied:
(i) $|\hat{\cdot}|$ is an extension of $|\cdot|$ (i.e.: $|\hat{\cdot}|$ restricts on K to $|\cdot|$).
(ii) K is dense in $\hat{K}$ w.r.t. $|\hat{\cdot}|$.
(iii) $\hat{K}$ is complete w.r.t. $|\hat{\cdot}|$.

Theorem 19. *(cf.* [5, §23 p.63ff]*) Up to isometric K-isomorphism there is exactly one completion $\hat{K}$ of K w.r.t. $|\cdot|$.*

Example 20. The field $\mathbb{R}$ is defined to be the completion of $\mathbb{Q}$ w.r.t. the usual absolute value $|\cdot|_\infty$ on $\mathbb{Q}$.

Similarly we can define the field of p-adic numbers:

Definition 21. Let p be a prime.

(a) By $\mathbb{Q}_p$ we denote the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ and call it the *field of p-adic numbers.*

(b) By $\mathbb{Z}_p$ we denote the valuation ring of $\mathbb{Q}_p$ and call it the ring of *p-adic integers.*

An explicit description of the elements of $\mathbb{Q}_p$ is given in the following proposition.

Proposition 22. *(cf.* [5, §23 p.68f]*) For every $x \in \mathbb{Q}_p$ there is a unique representation given by*

$$x = \sum_{-\infty \ll k} x_k p^k \textit{ where } x_k \in \{0, 1, \ldots, p-1\}$$

and its valuation is given by $\nu_p(x) = min\{k \in \mathbb{Z} : x_k \neq 0\}$.

Because of the uniqueness of $\hat{K}$ we can write $|\cdot|$ for the absolute values of both K and $\hat{K}$. We have the following proposition for completions of fields w.r.t. non-archimedean absolute values:

Proposition 23. *(cf.* [5, §23 p.66f]*) Let $\hat{K}$ be the completion of the field K w.r.t. a non-archimedean absolute value $|\cdot|$. Then K and $\hat{K}$ have got the same value group and canonically isomorphic residue class fields.*

Proposition 24. *(cf.* [5, §23 p.76f]*) Let L/K be a finite field extension and $|\cdot|$ an absolute value on K such that K is complete w.r.t. $|\cdot|$. Then there is exactly one absolute value $|\cdot|'$ on L that extends $|\cdot|$. Additionally L is complete w.r.t. $|\cdot|'$.*

If $|\cdot|$ is an archimedean absolute value on K, then $\mathrm{char}(K) = 0$ and hence we can see $\mathbb{Q}$ as a subfield of K. Then $|\cdot|$ is equivalent to $|\cdot|_\infty$ on $\mathbb{Q}$ (cf. Thm.12). If K is now complete w.r.t. $|\cdot|$ then we can see $\mathbb{R}$ as a subfield of K (cf. Ex.20). As one can show K has to be algebraic over $\mathbb{R}$ and hence we get the theorem of Ostrowski:

Theorem 25. *(Theorem of Ostrowski) (cf.* [5, §23 p.72]*)*

(a) Let K be a complete field w.r.t. an archimedean absolute value $|\cdot|$. Then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$ and $|\cdot|$ is equivalent to the usual absolute value $|\cdot|_\infty$.

(b) If K is an arbitrary (not necessarily complete) field with archimedean absolute value $|\cdot|$ then K is isomorphic to a subfield of $\mathbb{C}$ and $|\cdot|$ is equivalent to the restriction of the usual absolute value $|\cdot|_\infty$ on $\mathbb{C}$.

2.3. **Residue class degree, ramification index and discrete valuations.** In the following let L/K be a field extension and $|\cdot|$ a non-archimedean absolute value on L. Let A resp. R denote the valuation rings, $\mathfrak{P}$ resp. $\mathfrak{p}$ the valuation ideals and $\lambda = A/\mathfrak{P}$ resp. $\kappa = R/\mathfrak{p}$ the residue class fields of L resp. K. Since $R \cap \mathfrak{P} = \mathfrak{p}$ the natural homomorphism $R/\mathfrak{p} \to A/\mathfrak{P}$ is injective and hence we can see κ as a subfield of λ.

Definition 26. (a) The degree $f = f(L/K) = [\lambda : \kappa]$ is called the *residue class degree* of L/K.

(b) The index $e = e(L/K) = [|L^*| : |K^*|]$ is called the *ramification index* of L/K.

Residue class degree and ramification index have the following properties:

Proposition 27. *(cf.* [5, §24 p.89f]*) (a) Let M be an intermediate field in L/K. Then*

$$f(L/K) = f(L/M)f(M/K)$$

and

$$e(L/K) = e(L/M)e(M/K).$$

(b) Let $\hat{L}$ be the completion of L and $\hat{K}$ the completion of K embedded in $\hat{L}$. Then

$$f(\hat{L}/\hat{K}) = f(L/K)$$

and

$$e(\hat{L}/\hat{K}) = e(L/K).$$

(c) If L/K is finite then $[\hat{L} : \hat{K}] \leq [L : K]$.

Definition 28. An absolute value $|\cdot|$ of a field K is called *discrete* if $|K^*|$ is a nontrivial discrete subgroup of $\mathbb{R}^+$.

In the following we will discuss discrete absolute values only. Those have the following properties:

Proposition 29. *(cf.* [5, §24 p.91f]*) Let $|\cdot|$ be a discrete absolute value on K.*

(a) The absolute value $|\cdot|$ is non-archimedean since otherwise $\mathbb{Q}$ would be a subfield of K whose value group $|\mathbb{Q}^*|$ is always dense in $\mathbb{R}^+$.

(b) Since every nontrivial discrete subgroup of $\mathbb{R}^+$ is cyclic there is some $0 < c < 1$ such that $|K^*| = \{c^n : n \in \mathbb{Z}\}$. We can now define a valuation on K with value group $\mathbb{Z}$ by $\nu(x) = log_c|x|$. This valuation is called the normalized valuation on K w.r.t $|\cdot|$. We can now choose an arbitrary element $\pi \in K$ with $\nu(\pi) = 1$ and call it a prime element of K. Now every element $x \in K^*$ can be uniquely written in the form

$$x = \pi^n u$$

for some $n \in \mathbb{Z}$ and $u \in R^*$ (i.e. $\nu(u) = 0$). Therefore R is a principal ideal domain and all its nontrivial ideals are given by (π^k) with $k \in \mathbb{N}$.

(c) Let L/K be a field extension with $e(L/K)$ finite. Then the absolute value on L is discrete if and only if the absolute value on K is discrete.

Let K be complete w.r.t. a discrete absolute value. If we fix $\pi \in K$ prime and some system $S \subset K$ of representatives of elements in κ with $0 \in S$ every $x \in K$ has the unique representation

$$x = \sum_{-\infty \ll k} x_k \pi^k$$

with $x_k \in S$.

Example 30. For the field $\mathbb{Q}_p$ and $S = \{0, 1, \dots, p-1\} \subset \mathbb{Z}$ this representation becomes the representation given above.

Example 31. Let F be a field and $F(X)$ be the field of rational functions over F. For every polynomial $0 \neq f \in F[X]$ define $\nu(f) = \deg(f)$. (Hence $X \in F[X]$ is prime.) Then ν can uniquely be expanded to a normalized valuation on $F(X)$. Completion of $F(X)$ w.r.t. this valuation gives the field $F((X))$ of formal Laurent series over F. An element $f \in F((X))$ can then uniquely be written as

$$f = \sum_{-\infty \ll k} a_k X^k$$

where $a_k \in F$.

For discrete valuations on complete fields we now get a connection between the residue class degree and the ramification index by the following theorem:

Theorem 32. *(cf.* [5, §24 p.94]*) Let L/K be a field extension. Let $|\cdot|$ be a discrete absolute value on both L and K and let K (and hence also L) be complete w.r.t. $|\cdot|$. If both $e(L/K)$ and $f(L/K)$ are finite then L/K is finite and for its degree $n = [L : K]$ we have*

$$n = e(L/K)f(L/K).$$

2.4. **Unramified and totally ramified extensions.**

Definition 33. Let L/K be a finite field extension with an absolute value $|\cdot|$ on L. Let $\hat{L}$ resp. $\hat{K}$ be completions of L resp. K w.r.t. $|\cdot|$ such that $\hat{K} \subseteq \hat{L}$. We call L/K *unramified* if

$$[\hat{L} : \hat{K}] = [\lambda : \kappa]$$

and λ/κ is separable, where λ resp. κ are the residue class fields of $\hat{L}$ resp. $\hat{K}$.

If the absolute value $|\cdot|$ on K is discrete then this definition becomes equivalent to $e(L/K) = 1$ and λ/κ separable.

If K is complete we have the following theorem:

Theorem 34. *(cf.* [5, §24 p.95ff]*) Let K be a complete field w.r.t. the non-archimedean absolute value $|\cdot|$ and let $\bar{K}$ be an algebraic closure of K.*

(a) The residue class field $\bar{\kappa}$ of $\bar{K}$ is an algebraic closure of the residue class field κ of K.

(b) For every finite extension λ/κ there is a unique extension L/K (which is unramified) in $\bar{K}/K$ such that λ is the residue class field of L and $[L : K] = [\lambda : \kappa]$.

(c) The function that maps every intermediate field of $\bar{K}/K$ onto its residue class field, gives a bijection from the set of all finite unramified extensions L/K onto the set of all finite separable extensions λ/κ which respects inclusion.

(d) For every finite extension L/K there is a maximal unramified subextension M/K. If for the residue class fields λ resp. κ of L resp. K the extensionλ/κ is separable then λ is also the residue class field of M and $[M : K] = [\lambda : \kappa]$.

(e) If L/K is unramified then L/K is a Galois extension if and only if λ/κ is. In this case there is a natural isomorphism $Gal(L/K)\tilde{\rightarrow}Gal(\lambda/\kappa)$ between the corresponding Galois groups.

If the residue class field κ of K is finite one can use this theorem to get information about the unramified extensions of K:

Theorem 35. *(cf.* [5, §24 p.97f]*) Let K be a complete field w.r.t. the non-archimedean absolute value $|\cdot|$ such that the residue class field κ of K is a finite field with q elements.*

(a) For every $n \in \mathbb{N}$ there is exactly one unramified extension of K with degree n. It is the extension $K(\zeta)/K$ where ζ is a primitive $(q^n - 1)$-th root of unity.

(b) Let $m \in \mathbb{N}$ be relatively prime to $p := char(\kappa)$ and let ζ_m denote a primitive m-th root of unity. Then the extension $K(\zeta_m)/K$ is unramified and its degree is the smallest $n \in \mathbb{N}$ such that $m \mid (q^n - 1)$. In particular the group $W_{p'}(K)$ of roots of unity in K with order relatively prime to p is isomorphic to κ^*.

(c) Every finite unramified extension L/K is a cyclic Galois extension and in its Galois group there is exactly one element $\varphi_{L/K} \in Gal(L/K)$ that maps to the Frobenius automorphism $x \mapsto x^q$ in $Gal(\lambda/\kappa)$. Hence we also call $\varphi_{L/K}$ the Frobenius automorphism of L/K.

Proof. (Sketch) (a) Since for the finite field $\kappa \cong \mathbb{F}_q$ there is exactly one field extension $\lambda \cong \mathbb{F}_{q^n}$ of degree n (which is also separable) there is exactly one unramified extension of K of degree n. The multiplicative group λ^* is cyclic of degree $q^n - 1$ and so $\lambda = \kappa(\zeta')$ where ζ' is a primitive $(q^n - 1)$-th root of unity. One can show that in every field extension $\tilde{L}$ of K with a residue class field containing ζ' there is some (q^n-1)-th rootζ in $\tilde{L}$ which reduces to ζ' (and hence is also primitive). So $L = K(\zeta)$ is the smallest field extension of K with residue class field λ and is therefore unramified.

(b) Since $K(\zeta_m) \subseteq K(\zeta)$ (ζ as in (a)), the residue class field of $K(\zeta_m)$ is contained in λ. Since ζ_m is a power of ζ, the root ζ_m reduces to a primitive m-th root of unity. So the residue class field of $K(\zeta_m)$ is equal to λ and $K(\zeta_m) = K(\zeta)$. For $\lambda = \kappa$ one gets the structure of $W_{p'}(K)$.

(c) Since λ/κ is cyclic so is L/K and we can define the Frobenius automorphism $\varphi_{L/K}$ on L/K. □

Example 36. The field $\mathbb{Q}_p$ fulfills the conditions of the theorem. The unramified extension of $\mathbb{Q}_p$ of degree n is the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ where ζ is a primitive $p^n - 1$-th root of unity. Its Frobenius automorphism

φ is given by $\varphi(\zeta) = \zeta^p$. The group $W_{p'}(\mathbb{Q}_p)$ is the group of $p-1$-th roots of unity and is isomorphic to $\mathbb{F}_p^*$.

Definition 37. An extension L/K of fields with non-archimedean absolute values is called *totally ramified* if $e(L/K) = [L : K]$.

Definition 38. Let $|\cdot|$ be a discrete absolute value on K and ν its normalized valuation. A monic polynomial $f = X^d + \sum_{i=0}^{d-1} a_i X^i \in K[X]$ is called an *Eisenstein polynomial* if $\nu(a_i) \geq 1 = \nu(a_0)$.

Proposition 39. *(cf.* [5, §24 p.98f]*) Let $|\cdot|$ be a discrete absolute value on K and ν its normalized valuation.*

(a) Let $f \in K[X]$ be an Eisenstein polynomial of degree d and $\Pi \in \bar{K}$ a zero of f. Then there is exactly one continuation of $|\cdot|$ onto $L = K(\Pi)$[3] *and L/K is totally ramified of degree d. Furthermore f is irreducible and Π is prime in L.*

(b) If conversely L/K is a totally ramified extension of K then $L = K(\Pi)$ for any prime Π of L and the minimal polynomial of Π is an Eisenstein polynomial.

Example 40. Let ζ be a p^k-th root of unity ($k \geq 1$). Then the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is totally ramified of degree $(p-1)p^{k-1}$ and $\zeta - 1$ is prime in $\mathbb{Q}_p(\zeta)$ with Eisenstein polynomial $f(X) = g(X+1)$ where $g(X) = \frac{X^{p^k}-1}{X^{p^{k-1}}-1}$ is the minimal polynomial of ζ.

2.5. **The definition and the list of local fields.** The shortest definition of a local field is the following:

Definition 41. A field K that is locally compact[4] w.r.t. a nontrivial absolute value $|\cdot|$ is called a *local field*.

If K is a local field and $\{a_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence then almost all terms a_n lie in a compact set and hence the sequence is convergent. So K is complete. If now $|\cdot|$ is archimedean then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$ and $|\cdot| \sim |\cdot|_\infty$.[5] If $|\cdot|$ is non-archimedean then we have the following proposition:

[3] Contrary to Prop. 48 the field K need not be complete here.

[4] I.e. every $x \in K$ has a compact neighborhood.

[5] Cf. Thm. 25.

Proposition 42. *(cf.* [5, §25 p.114]*) (a) Let K be a local field w.r.t. a non-archimedean absolute value $|\cdot|$ then*

(i) K is complete.

(ii) The absolute value $|\cdot|$ is discrete.

(iii) The residue class field κ of K is finite.

(b) Conversely if $|\cdot|$ is an absolute value on K such that (i)-(iii) are satisfied then K is a local field w.r.t. $|\cdot|$.

The conditions (i)-(iii) in the above proposition are rather strong and allow us to list all possible local fields.

Theorem 43. *(cf.* [5, §25 p.115]*) Let K be a local field. Then K isomorphic to one of the following fields*

(a) $\mathbb{R}$ or $\mathbb{C}$ (in the archimedean case).

(b) A finite extension of a p-adic number field $\mathbb{Q}_p$ (in the non-archimedean case and char$(K) = 0$).

(c) The field $\mathbb{F}_q((X))$ of formal Laurent series over the finite field $\mathbb{F}_q$ for some prime power q (in the non-archimedean case and char$(K) \neq 0$).[6]

We now define another kind of field which is closely related to local fields.

Definition 44. The following fields are called *global fields*:

(a) algebraic number fields (i.e. the finite extensions of $\mathbb{Q}$).

(b) function fields in one variable over a finite field (i.e. finite extensions of $\mathbb{F}_p(X)$.

Theorem 45. *(cf.* [5, §25 p.117ff]*) The local fields are the completions of global fields w.r.t. non-trivial absolute values.*

2.6. **Ramification and solubility of local field extensions.** We can use the notion of ramification in local field extensions to show that their Galois groups are always solvable. At first we define tame and wild ramification.

Definition 46. Let L/K be an extension of non-archimedean local fields. Then L/K is called *tamely ramified* if $e(L/K)$ is relatively prime to $p = \text{char}(\kappa)$. Otherwise L/K is called *wildly ramified.*

[6] Any finite extension K of $\mathbb{F}_q((X))$ is also a local field with $K \cong \mathbb{F}_{q^k}((Y))$ for some $k \in \mathbb{N}$ and $Y \in K$ prime. Cf. [5, §25 p.115]

Tamely ramified extensions are easy to understand.

Proposition 47. *(cf.* [5, §25 p.120f]*) Let L/K be a totally and tamely ramified extension of non-archimedean local fields of degree e. Fix a prime $\pi \in K$. Then there is some $(q-1)$-th root of unity ζ (where $q = |\kappa|$) such that for the prime $\pi_0 = \zeta\pi \in K$ we have $L = K(\sqrt[e]{\pi_0})$. If additionally L/K is Galois then $e \mid (q-1)$ and Gal(L/K) is cyclic.*

Furthermore one has:

Proposition 48. *(cf.* [5, §25 p.121]*) Let L/K be a totally ramified extension of non-archimedean local fields. Then there is a unique maximal tamely ramified subextension T/K of L/K.*

Hence for a finite extension L/K of local fields we have two important intermediate fields. The maximal unramified subextension M/K of L/K (cf. Thm.34(d)) and the maximal tamely ramified extension T/M of L/M (cf. Prop.48).

$$\begin{tikzcd}
L \arrow[d, dash] \\
T \arrow[d, dash] \\
M \arrow[d, dash] \\
K
\end{tikzcd}$$

If now L/K is Galois then $\mathrm{Gal}(M/K)$ is cyclic (cf. Thm.35(c)) and $\mathrm{Gal}(T/M)$ is cyclic (cf. Prop.47). The extension L/T has no tamely ramified subextension and hence is of degree p^r for some $r \in \mathbb{N}$. So its Galois group $\mathrm{Gal}(L/T)$ is a p-group and therefore solvable. Hence in the series of normal subgroups

$$\mathrm{Gal}(L/K) \trianglerighteq \mathrm{Gal}(L/M) \trianglerighteq \mathrm{Gal}(L/T) \trianglerighteq 1$$

all the factors are solvable groups. So we have the following theorem:

Theorem 49. *(cf.* [5, §25 p.121]*) Let L/K be a Galois extension of local fields. Then Gal(L/K) is solvable.*

2.7. **The multiplicative group of local fields.** Let K be a non-archimedean local field and let $q = p^r = |\kappa|$ be the order of its residue class field. Denote by $W_m = \{\zeta \in K : \zeta^m = 1\}$ the group of roots of unity of order m in K by $U = R^*$ the units of its valuation ring R and by $U^{(n)} = 1 + \mathfrak{p}^n$ the balls around 1 with radius p^{-n}. Then the following proposition describes the multiplicative structure of K.

Proposition 50. *(cf.* [5, §25 p.124]*) Let $\pi \in K$ be a prime. Then we have*

$$K^* \cong \langle \pi \rangle \times U = \langle \pi \rangle \times W_{q-1} \times U^{(1)}$$

as topological groups. Additionally we have $W_{q-1} = W'$ where $W' = \{\zeta \in K : \zeta^n = 1 \text{ mit } (n,p) = 1\}$ is the group of roots of unity in K with order relatively prime to p. We have the isomorphy

$$U/U^{(1)} \cong W_{q-1} \cong \kappa^*$$

and for every $n \geq 1$

$$U^{(n)}/U^{(n+1)} \cong \kappa.$$

We want to find out a little bit more about the structure of $U^{(1)}$.

Proposition 51. *(cf.* [5, §25 p.126f]*) Let $a \in U^{(1)}$ and $x \in \mathbb{Z}_p$. For every sequence of integers $(x_n)_{n \in \mathbb{N}}$ with $x = \lim_{n\to\infty} x_n$ the sequence $(a^{x_n})_{n \in \mathbb{N}}$ is convergent in K. If we define*

$$a^x := \lim_{n\to\infty} a^{x_n},$$

then $U^{(1)}$ gets a $\mathbb{Z}_p$-module structure via the map $(x, a) \mapsto a^x$.

Proof. Let $b \in U^{(n)}$. Then we have $b^p \in U^{(n+1)}$ and hence for any $z \in \mathbb{Z}$ we get $b^z \in U^{(n+\nu_p(z))}$. So if $\{z_n\}_n$ is a p-adic nullsequence and $a \in U^{(1)}$ then

$$\lim_{n\to\infty} a^{z_n} = 1.$$

If now $\{x_n\}_n$is a p-adic Cauchy sequence in $\mathbb{Z}$ convergent to $x \in \mathbb{Z}_p$, then

$$\lim_{n\to\infty} a^{x_{n+1}} - a^{x_n} = \lim_{n\to\infty} a^{x_n}(a^{x_{n+1}-x_n} - 1) = 0.$$

Hence $\{a^{x_n}\}_n$ is a Cauchy sequence and therefore convergent in K. Since $U^{(1)}$ is closed we get

$$\lim_{n\to\infty} a^{x_n} \in U^{(1)}.$$

If $\{y_n\}$ is another p-adic Cauchy sequence converging to x, then

$$\lim_{n\to\infty} a^{y_n} - a^{x_n} = \lim_{n\to\infty} a^{x_n}(a^{y_n - x_n} - 1) = 0.$$

So a^x is well defined and one can easily check that the map $(x, a) \mapsto a^x$ makes $U^{(1)}$ a $\mathbb{Z}_p$-module. □

For char$(K) = 0$ one can show a little bit more:

Theorem 52. *(cf. [5, §25 p.130f]) Let char$(K) = 0$, $n = [K : \mathbb{Q}_p]$ and $W_{p^\infty} = \{\zeta \in K : \zeta^{p^k} = 1$ for some $k \in \mathbb{N}\}$. Then W_{p^∞} is finite and we have*

$$U^{(1)} \cong W_{p^\infty} \times \mathbb{Z}_p^n$$

as $\mathbb{Z}_p$-modules.

Example 53. For $K = \mathbb{Q}_p$ one can describe the multiplicative group in the following way:

If $p \neq 2$ then the multiplicative group of $\mathbb{Q}_p$is given by

$$\mathbb{Q}_p^* = \langle p \rangle \times W_{p-1} \times U^{(1)}$$

where

$$U^{(1)} = (1+p)^{\mathbb{Z}_p}.$$

So every element $a \in \mathbb{Q}_p^*$ can uniquely be written as

$$a = p^n \zeta (1+p)^x$$

with $n \in \mathbb{Z}$, $\zeta \in W_{p-1}$ and $x \in \mathbb{Z}_p$.

If $p = 2$ then $U^{(1)} = U$ and so

$$\mathbb{Q}_2^* = \langle 2 \rangle \times U^{(1)} = \langle 2 \rangle \times \{\pm 1\} \times U^{(2)}$$

where

$$U^{(2)} = (1+4)^{\mathbb{Z}_2} = 5^{\mathbb{Z}_2}.$$

Every element $a \in \mathbb{Q}_2^*$ can uniquely be written as

$$a = 2^n \varepsilon 5^x$$

where $n \in \mathbb{Z}$, $\varepsilon \in \{\pm 1\}$ and $x \in \mathbb{Z}_2$.

3. Local Class Field Theory

This chapter starts with the main results of local class field theory and then gives an introduction into Lubin-Tate modules, a tool to describe local class field theory explicitly. For more details and proofs see [7, Ch 4-5] or [2, Ch 7].

3.1. The local reciprocity law and the norm residue symbol.

Class field theory studies field extensions with abelian Galois groups. So we define:

Definition 54. (a) Let K be a field then denote by K^{ab} the *maximal abelian extension* of K.

(b) Let L/K be a field extension then denote by $\text{Gal}(L/K)^{ab} = \text{Gal}((K^{ab} \cap L)/K)$ the Galois group of the maximal abelian subextension of L/K.

For an extension of local fields its maximal abelian subextension is described in the so called local reciprocity law, which is a strong result in local class field theory that can be proved with the modern theory of Galois cohomology.

Theorem 55. *(Local reciprocity law) (cf.* [7, Ch 5 Thm 1.3]*) Let L/K be a finite Galois extension of local fields. Then there is a canonical homomorphism*

$$(\cdot, L/K) : K^* \to Gal(L/K)^{ab}$$

called the norm residue symbol. It is surjective and its kernel is $N_{L/K}L^*$.

For archimedean local fields there is only a single nontrivial norm residue symbol:

Example 56. For the field extension $\mathbb{C}/\mathbb{R}$ of local fields the norm residue symbol is given by

$$(\alpha, \mathbb{C}/\mathbb{R}) = \begin{cases} id & \alpha > 0 \\ \sigma & \alpha < 0 \end{cases}$$

where $id, \sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$ are the identity map and the complex conjugation respectively.

In the non-archimedean case the norm residue symbol is much more difficult to understand. For unramified extensions however the norm residue symbol can be computed explicitly in terms of its Frobenius element.

Proposition 57. *(cf.* [7, Ch 4 Thm 6.5]*) Let L/K be an unramified extension of non-archimedean local fields of degree n and let $\varphi = \varphi_{L/K}$ be the Frobenius element in Gal(L/K). Then for $\alpha \in K^*$ we have that $(\alpha, L/K) = \varphi^{\nu(\alpha)}$.*

In the special case of the totally ramified extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ one can compute the norm residue symbol with transcendental methods.

Theorem 58. *(cf.* [7, Ch 5 Thm 2.4]*) Let $a = up^{\nu_p(a)} \in \mathbb{Q}_p^*$. Then*

$$(a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = \sigma$$

where $\sigma \in$ Gal$(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ is given by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{u^{-1}}$.

Now we want to use the local reciprocity law to find the maximal abelian extension K^{ab} of an arbitrary local field K.

Theorem 59. *(existence theorem) (cf.* [7, Ch 5 Thm 1.4]*) Let K be a local field. Then the map $L \mapsto \mathcal{N}_L = N_{L/K}L^*$ gives a one-one correspondence between finite abelian field extensions of K and the open subgroups of finite index in K^*. Furthermore we have*

$$L_1 \subseteq L_2 \Longleftrightarrow \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2},\ \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2},\ \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}.$$

Hence finding abelian extensions of K is equivalent to finding open subgroups of K^* with finite index. The field corresponding to some subgroup $\mathcal{N} \leq K^*$ is called the *class field* of $\mathcal{N}$. From Prop. 50 we know that

$$K^* \cong \langle \pi \rangle \times U.$$

So every open subgroup with finite index contains a subgroup of the form $\langle \pi^f \rangle \times U^{(n)}$ for some $f, n \in \mathbb{N}$ which is also open and of finite index. Therefore every finite abelian extension L/K is contained in the class field of such a group $\langle \pi^f \rangle \times U^{(n)}$. Hence those class fields are important and to obtain them we will first determine those corresponding to $\langle \pi^f \rangle \times U$. We need the following theorem:

Theorem 60. *(cf.* [7, Ch 5 Thm 1.7]*) Let L/K be an abelian extension of local fields then*

(i) L/K is unramified if and only if $U \subseteq N_{L/K}(L^*)$.

(ii) L/K is tamely ramified if and only if $U^{(1)} \subseteq N_{L/K}(L^*)$.

Hence the unramified extension L/K of order f corresponds to the group $\langle \pi^f \rangle \times U$. The class fields of $\langle \pi \rangle \times U^{(n)}$ can be obtained explicitly by Lubin-Tate modules which are a direct generalization of the case $K = \mathbb{Q}_p$ that we will discuss now.

Example 61. For $K = \mathbb{Q}_p$ the class field to $\langle p \rangle \times U^{(n)}$ is given by $L = \mathbb{Q}_p(\zeta_{p^n})$ and the class field to $\langle p^f \rangle \times U$ is given by the unique unramified extension of degree f (i.e. $L = \mathbb{Q}_p(\zeta_{p^f-1})$). So the maximal abelian extension of $\mathbb{Q}_p$ is given by $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\{\zeta_n : n \in \mathbb{N}\})$. This is the local version of the famous Kronecker-Weber theorem.

Theorem 62. *(Kronecker-Weber) (cf.* [7, Ch 5 Thm 1.10]*) The maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is given by*

$$\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n : n \in \mathbb{N}\}).$$

3.2. **Formal groups and Lubin-Tate modules.** In order to use local class field theory to find the maximal abelian extensions of arbitrary local fields we will introduce the notion of formal groups and Lubin-Tate modules.

Definition 63. (a) A one dimensional commutative *formal group* over a ring R is a formal power series $F(X,Y) \in R[[X,Y]]$ such that

(i) $F(X,Y) \equiv X + Y \mod \deg 2$
(ii) $F(X,Y) = F(Y,X)$
(iii) $F(F(X,Y),Z) = F(X,F(Y,Z))$

(b) Let F and G be formal groups over R. Then a *formal group homomorphism* $f : F \to G$ is a power series $f \in R[[X]]$ such that

$$f(F(X,Y)) = G(f(X), f(Y)).$$

Example 64. Let R be an arbitrary ring. Then

$$G_a(X,Y) = X + Y$$

and

$$G_m = X + Y + XY$$

are formal groups over R called *additive* and *multiplicative formal group* respectively.

The power series

$$f(X) = \log(X+1) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}$$

is a formal group isomorphism

$$f : G_m \tilde{\to} G_a$$

with inverse

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

Theorem 65. *(cf.* [7, Ch 5 Thm 4.3]*) Let F be a formal group over R. The set $End_R(F)$ of all homomorphisms from F into itself form a ring whose addition and multiplication are given by*

$$(f +_F g)(X) = F(f(X), g(X))$$

and

$$f \circ g(X) = f(g(X)).$$

Definition 66. (a) A *formal R-module* is a formal group F over R together with a ring homomorphism

$$[\cdot]_F : R \to End_R(F)$$

such that for $a \in R$ we have $[a]_F(X) \equiv aX \bmod \deg 2$.

(b) Let F and G be formal R-modules. Then a *homomorphism of formal R-modules* is a formal group homomorphism $f : F \to G$ such that for any $a \in R$

$$f([a]_F(X)) = [a]_G(f(X)).$$

Now let R be a valuation ring of a local field K. Then we can define Lubin-Tate modules as follows:

Definition 67. A *Lubin-Tate module* over R w.r.t. the prime element $\pi \in R$ is a formal R-module F such that

$$[\pi]_F \equiv X^q \bmod \pi$$

where q is the number of elements of the residue class field of K.

Example 68. The formal group G_m is a $\mathbb{Z}_p$-module with the multiplication given by

$$[a]_{G_m}(X) = (X+1)^a - 1 = \sum_{k=1}^{\infty} \binom{a}{k} X^k.$$

It is a Lubin-Tate module w.r.t. p because

$$[p]_{G_m}(X) = (X+1)^p - 1 \equiv X^p \bmod p.$$

Concerning existence and uniqueness of Lubin-Tate modules on arbitrary local fields K we have the following theorem.

Theorem 69. *(cf. [7, Ch 5 Thm 4.6]) Let $\pi \in R$ be a prime.*

(a) Let $e \in R[[X]]$ be a formal power series such that

$$e(X) \equiv \pi X \ \mathit{mod} \deg 2$$

and

$$e(X) \equiv X^q \mathit{mod}\ \pi.$$

Then there is a uniquely determined Lubin-Tate module $F = F_e$ such that $[\pi]_F = e$.

(b) Two Lubin-Tate modules w.r.t. π are isomorphic as formal R-modules.

Now we will use Lubin-Tate modules to generalize the Kronecker-Weber theorem. At first we will construct actual R-modules from our Lubin-Tate modules. Therefore denote by $\bar{\mathfrak{p}}$ be the maximal ideal in the algebraic closure $\bar{K}$ of K.

Proposition 70. *(cf. [7, Ch 5 Thm 5.1]) (a) Let F be a formal R-module. Then for $x, y \in \bar{\mathfrak{p}}$ and $a \in R$ the operations*

$$x +_F y = F(x,y) \ \mathit{and}\ a \cdot x = [a]_F(x)$$

make $\bar{\mathfrak{p}}$ into an R-module in the usual sense. We denote this module by $\bar{\mathfrak{p}}_F$.

(b) If $f : F \to G$ is a homomorphism of formal R-modules then $f : \bar{\mathfrak{p}}_F \to \bar{\mathfrak{p}}_G$ is a homomorphism of R-modules.

Definition 71. (a) If F is a Lubin-Tate module over R w.r.t. π then we define by

$$F(n) = \{\lambda \in \bar{\mathfrak{p}}_F : [\pi^n]_F(\lambda) = 0\} = \ker([\pi^n]_F)$$

the *group of π^n division points which is also an R-submodule of $\bar{\mathfrak{p}}_F$.*

(b) Define the *field of π^n division points* (or the *Lubin-Tate extension L_n/K w.r.t. π of degree n*) $L_n = K(F(n))$ as the field obtained by adjoining the π^n division points to K.

One can show that the Lubin-Tate extensions L_n/K only depend on π and not on the Lubin-Tate module F chosen.

Example 72. For $R = \mathbb{Z}_p$ and $F = G_m$ over R we have

$$[p^n]_{G_m}(X) = (X+1)^{p^n} - 1.$$

So $G_m(n) = \{\zeta_{p^n}^k - 1 : 0 \le k \le p^n - 1\}$ and hence $L_n = \mathbb{Q}_p(\zeta_{p^n})$.

To generalize this example to arbitrary local fields we need to find out more about the structure of $F(n)$. Clearly $F(n)$ is an R-module and hence $End_R F(n)$ is also an R module.

Theorem 73. *(cf.* [7, Ch 5 Thm 5.2]*) The group $F(n)$ of π^n division points is a free $R/\pi^n R$ module of rank* 1.

Proof. An isomorphism $f : F \to G$ of Lubin-Tate modules induces isomorphisms $f : \bar{\mathfrak{p}}_F \to \bar{\mathfrak{p}}_G$ and $f : F(n) \to G(n)$ of R-modules. Since all Lubin-Tate modules w.r.t. π are isomorphic we can choose $F = F_e$, where $e(X) = X^q + \pi X$ (cf. Thm.69). Then $F(n)$ are the q^n zeros of the polynomial $e^n = e \circ \cdots \circ e$ which can be shown to be separable. For $\lambda_n \in F(n) \backslash F(n-1)$ the map

$$\Lambda_n : R \to F(n)$$

$$a \mapsto [a]_F(\lambda_n)$$

is a homomorphism of R-modules with kernel $ker(\Lambda_n) = \pi^n R$. It induces an isomorphism $R/\pi^n R \tilde{\to} F(n)$ since both sides have order q^n. □

Corollary 74. *(cf.* [7, Ch 5 Cor 5.3]*) The map $a \mapsto [a]_F$ induces isomorphisms*

$$R/\pi^n R \tilde{\to} End_R(F(n))$$

and

$$U/U^{(n)} \tilde{\to} Aut_R(F(n)).$$

Theorem 75. *(cf.* [7, Ch 5 Thm 5.4]*) Let L_n/K be a Lubin-Tate extension w.r.t. a prime $\pi \in K$ and let F be a corresponding Lubin-Tate module s.t. $e(X) := [\pi]_F(X)$ is a polynomial of degree q (where q is the degree of the residue class field of K). Then L_n/K is totally ramified of degree $q^{n-1}(q-1)$ (where q is the number of elements of κ) with Galois group*

$$Gal(L_n/K) \cong Aut_R(F(n)) \cong U/U^{(n)}.$$

So for any $\sigma \in Gal(L_n/K)$ there is a unique class u mod $U^{(n)}$ such that

$$\forall \lambda \in F(n) : \sigma(\lambda) = [u]_F(\lambda).$$

Let $\lambda_n \in F(n)\backslash F(n-1)$. Then λ_n is prime in L_n and

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)}$$

is its minimal polynomial. In particular we have $L_n = K(\lambda_n)$.

Proof. For

$$e(X) = [\pi]_F(X) = X^q + \pi(a_{q-1}X^{q-1} + \cdots + a_2X^2) + \pi X$$

we see that

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = e^{n-1}(X)^{q-1} + \pi(a^{q-1}e^{n-1}(X)^{q-2} + \cdots + a_2e^{n-1}(X)) + \pi$$

is an Eisenstein polynomial (and hence irreducible) of degree $(q-1)q^{n-1}$. Clearly λ_n is a zero of $e^n(X)$ but not of $e^{n-1}(X)$ and hence $\phi_n(X)$ is the minimal polynomial of λ_n and $L_n = K(\lambda_n)/K$ is totally ramified. Now every $\sigma \in Gal(L_n/K)$ induces an R-module automorphism on $F(n)$. So we get a homomorphism of R-modules

$$\Phi : Gal(L_n/K) \to Aut_R(F(n)).$$

This homomorphism Φ is injective because $L_n = K(F(n))$ and surjective because

$$|Gal(L_n/K)| \geq [K(\lambda_n) : K] = q^{n-1}(q-1) = |U/U^{(n)}| = |Aut_R(F(n))|.$$

□

As a generalization of the explicit description of the norm residue symbol of $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ we get an explicit formula for the norm residue symbol of Lubin-Tate extensions by the following theorem.

Theorem 76. *(cf.* [7, Ch 5 Thm 5.5]*) Let L_n/K be a Lubin-Tate extension w.r.t. π and $a = u\pi^{\nu_K(a)} \in K^*$. Then*

$$(a, L_n/K) = \sigma$$

where $\sigma \in Gal(L_n/K)$ is given by $\sigma(\lambda) = [u^{-1}]_F(\lambda)$.

Corollary 77. *(cf.* [7, Ch 5 Cor 5.6]*) The field L_n/K of the π^n division points is the class field to the group $\langle\pi\rangle \times U^{(n)} \subseteq K^*$.*

For the maximal abelian extension K^{ab}/K we get the following analogue to the local Kronecker-Weber theorem:

Corollary 78. *(cf.* [7, Ch 5 Cor 5.7]*) Let K be a nonarchimedean local field, $\tilde{K}$ its maximal unramified extension and $L_\pi = \bigcup_{n\in\mathbb{N}} L_n$ the union of the Lubin-Tate extensions of K w.r.t. some prime $\pi \in K$. Then*

$$K^{ab} = \tilde{K}L_\pi.$$

4. Elliptic Curves and Complex Multiplication

This chapter contains the basic theory on elliptic curves and complex multiplication. It is based on [10, Ch 3], [11, Ch 6] and [4, Ch 12].

4.1. Basic facts about elliptic curves.

Definition 79. An elliptic curve defined over K is a pair (E, O), where E/K is a nonsingular projective variety over K of dimension one and of genus one and $O \in E(K)$ a K-rational point (called the origin of E).

This definition is very abstract. To work with elliptic curves we will use the following proposition. It says that any elliptic curve can be described by the so called Weierstrass equation.

Proposition 80. *(cf. [10, Ch 3 Prop 3.1]) Let E be an elliptic curve defined over K.*

(a) There exist functions $x, y \in K(E)$ such that the map

$$\varphi : E(\overline{K}) \to \mathbb{P}^2(\overline{K})$$

$$P \mapsto \begin{cases} (x(P) : y(P) : 1) & P \neq O \\ (0 : 1 : 0) & P = O \end{cases}$$

is an isomorphism of E/K onto a smooth curve given by an affine Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \ldots, a_6 \in K$ and satisfying $\varphi(O) = [0 : 1 : 0]$. The functions $x, y \in K(E)$ are called Weierstrass coordinates of E.

(b) Any two Weierstrass equations for E as in (a) are related by a linear change of variables of the form

$$X = u^2X' + r\,Y = u^3Y' + su^2X' + t$$

with $u \in K^*$ and $r, s, t \in K$.

(c) Conversely every smooth cubic curve given by a Weierstrass equation with coefficients in K is an elliptic curve defined over K with base point $O = [0 : 1 : 0]$.

So any elliptic curve is isomorphic to a smooth cubic curve with an inflection point in $O = [0 : 1 : 0]$. Hence if we speak of an elliptic curve over K in the following we will always fix a corresponding Weierstrass equation with coefficients in K to describe the curve.

If $char(K) \neq 2$ then one can simplify the equation by the substitution

$$X = x',\ Y = y' - \frac{a_1 x + a_3}{2},$$

which gives the equation

$$E : (y')^2 = (x')^3 + \frac{b_2}{4}(x')^2 + \frac{b_4}{2}x' + \frac{b_6}{4}$$

with

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1 a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6.$$

If $char(K) \neq 2, 3$ one can simplify the equation even further by setting

$$x' = x'' - \frac{b_2}{12},\ y' = y''.$$

This gives the equation

$$E : (y'')^2 = (x'')^3 - \frac{c_4}{48}x'' - \frac{c_6}{864}$$

with

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Furthermore we define the quantities

$$b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where Δ is called the discriminant of E and for $\Delta \neq 0$ define the so called j-invariant of E by

$$j = \frac{c_4^3}{\Delta}.$$

They satisfy the following relations:

$$4b_8 = b_2b_6 - b_4^2$$

and

$$12^3\Delta = c_4^3 - c_6^2.$$

Note that all the quantities $b_2, b_4, b_6, c_4, c_6, \Delta, j$ can also be defined (and will be used) for $char(K) = 2, 3$.

The next proposition shows the importance of these quantities.

Proposition 81. *(cf.* [10, Ch 3 Prop 1.4]*) (a) A curve E given by a Weierstrass equation is singular if and only if $\Delta = 0$. (I.e. for an elliptic curve we always have $\Delta \neq 0$.)*

(b) Two elliptic curves defined over K are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.

(c) For any $j_0 \in \overline{K}$ there is an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

4.2. Addition on elliptic curves and $E(\mathbb{C})$ as complex Lie group.

Let (E, O) be an elliptic curve defined over K. Then by Bézout's Theorem ([3, Ch 8.7 Thm 10]) any line $L \subset \mathbb{P}^2$ intersects E at exactly three points (with multiplicity) in $\mathbb{P}^2(\overline{K})$. So we can define an addition on $E(\overline{K})$ by the following:

Definition 82. Let $P, Q \in E(\overline{K})$. Then the line through P and Q intersects E in a third point $R \in E(\overline{K})$ and the line through this point R and the origin O intersects in a point $S \in E(\overline{K})$, which we define to be the sum of P and Q. We write $S = P + Q$.

One can now show that $E(K)$ endowed with this addition forms an abelian group (i.e. a $\mathbb{Z}$-module) with neutral element O. In fact, except of associativity all the properties are immediate consequences of the definition. A proof for associativity using the Riemann-Roch theorem is given in [10, Ch 3 Prop 3.4e].

The addition on E can also be described explicitly in coordinates. The coordinates of $P + Q$ are then given by rational functions in the coordinates of P and Q (i.e. addition is a morphism of K-varieties on E). Hence the complex points $E(\mathbb{C})$ of E form a complex Lie group. One can show that this Lie group $E(\mathbb{C})$ is isomorphic to a complex torus $\mathbb{C}/\Lambda$ with the induced addition from $\mathbb{C}$ where $\Lambda = \{n_1\omega_1 + n_2\omega_2 \in \mathbb{C} | n_1, n_2 \in \mathbb{Z}\}$ is a lattice with $\omega_1, \omega_2 \in \mathbb{C}$ linear independent complex numbers over $\mathbb{R}$. We have even more: every rational function on $E(\mathbb{C})$ corresponds bijectively to a meromorphic function $f \in \mathbb{C}(\Lambda)$ on the Riemann surface $\mathbb{C}/\Lambda$. Those meromorphic functions are called elliptic functions.

From the theory of elliptic functions (for example see [10, Ch 6]) one has that $\mathbb{C}(\Lambda) = \mathbb{C}(\mathfrak{p}, \mathfrak{p}')$ where $\mathfrak{p} = \mathfrak{p}(z, \Lambda) \in \mathbb{C}(\Lambda)$ is the so called Weierstrass-$\mathfrak{p}$-function of the lattice Λ. This function $\mathfrak{p}$ satisfies a differential equation

$$(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3.$$

The elliptic curve defined by this equation is then isomorphic (in the sense of isogenies, which is defined below) to the elliptic curve E that we started with.

All in all we have the following theorem:

Theorem 83. *(cf.* [10, Ch 6 Cor 5.1.1]*) Let $E/\mathbb{C}$ be an elliptic curve. Then there exists a lattice*

$$\Lambda \subset \mathbb{C}$$

unique up to homothety (i.e. $\Lambda_1 \sim \Lambda_2 \Leftrightarrow \exists \alpha \in \mathbb{C}^* : \Lambda_1 = \alpha\Lambda_2$) and a complex analytic isomorphism

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$
$$z \mapsto \begin{cases} (\mathfrak{p}(z,\Lambda) : \mathfrak{p}'(z,\Lambda) : 1) & z \neq 0 \\ (0 : 1 : 0) & z = 0 \end{cases}$$

of complex Lie groups.

4.3. **Isogenies and complex multiplication.** Next we define the homomorphisms between elliptic curves.

Definition 84. Let E_1 and E_2 be elliptic curves over K. A morphism $\phi : E_1 \to E_2$ of algebraic K-varieties with $\phi(O) = O$ is called an isogeny from E_1 to E_2. We write $\phi \in Hom(E_1, E_2)$.

Theorem 85. *(cf.* [10, Ch 3 Thm 4.8]*) Let E_1, E_2 be elliptic curves over K, $\phi : E_1 \to E_2$ an isogeny and $P, Q \in E_1$. Then*

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Hence an isogeny is also a homomorphism of abelian groups. Since addition on elliptic curves is a morphism defined over K the sum of two isogenies is again an isogeny. Therefore $Hom(E_1, E_2)$ is a $\mathbb{Z}$-module and $End(E) = Hom(E, E)$ forms a ring called the ring of endomorphisms on E.

Definition 86. For any $m \in \mathbb{Z}$ we can define the multiplication-by-m isogeny, denoted by $[m] : E \to E$, in the natural way ($[m] = m \cdot id$).

Proposition 87. *(cf. [10, Ch 3 Thm 4.2]) (a) Let E be an elliptic curve over K and $m \in \mathbb{Z}\backslash\{0\}$. Then $[m] \neq [0]$.*

(b) Let E_1, E_2 be elliptic curves. Then $Hom(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module.

(c) The ring $End(E)$ is an integral domain and has characteristic 0.

In most cases one has $End(E) \cong \mathbb{Z}$. But for us the other case is important.

Definition 88. Let E be an elliptic curve over K. We say that E has complex multiplication (CM) if $End(E) \ncong \mathbb{Z}$.

Example 89. The elliptic curve $E/\mathbb{C}$ given by the equation $y^2 = x^3 + x$ has complex multiplication. For example the map

$$\phi(x, y) = (-x, iy)$$

is an isogeny with $\phi^2 = [-1]$ and hence $End(E) \ncong \mathbb{Z}$. So E has complex multiplication.

If E is an elliptic curve over $\mathbb{C}$ then $End(E)$ must be an order in an algebraic number field. More precisely we have the following proposition:

Proposition 90. *(cf. [4, Ch 12 Thm 4.7]) Let E be an elliptic curve over $\mathbb{C}$ with $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$ (where $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z} \subset \mathbb{C}$, $\tau \in \mathbb{C}\backslash\mathbb{R}$). Then $End(E)$ is commutative. The curve E has complex multiplication if and only if τ is an imaginary quadratic number. In this case $End(E)$ is an order in the algebraic number field $\mathbb{Q}(\tau)$.*

Corollary 91. *For the elliptic curve $E : y^2 = x^3 + x$ the endomorphism ring is isomorphic to the Gaussian integers $\mathbb{Z}[i]$.*

For arbitrary fields K the situation is slightly more difficult:

Theorem 92. *(cf. [10, Ch 3 Cor 9.4]) Let E be an elliptic curve over a field K. Then $End(E)$ is isomorphic to either $\mathbb{Z}$, an order in an imaginary quadratic field or an order[7] in a quaternion algebra over $\mathbb{Q}$. If $char(K) = 0$ then only the first two are possible (i.e. $End(E)$ is commutative).*

[7] An order $\mathcal{R}$ of a finitely generated $\mathbb{Q}$-algebra $\mathcal{K}$ is a subring $\mathcal{R} \subset \mathcal{K}$ such that $\mathcal{R}$ is finitely generated as a $\mathbb{Z}$-module which satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

4.4. **Division points and Galois actions.**

Definition 93. Let E/K be an elliptic curve and $n \in \mathbb{N}$. We define $E[n] = \{P \in \mathbb{P}^2(\overline{K}) : [n]P = O\}$ to be the n-division points of E.

If E is an elliptic curve over $\mathbb{C}$ then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice Λ. Hence $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.

Obviously the endomorphism ring $End(E)$ acts on the n-division points $E[n]$. By choosing generators of P_1 and P_2 of $E[n]$ we get the following proposition:

Proposition 94. *Let E/K be an elliptic curve and $n \in \mathbb{N}$. Then there is a homomorphism*

$$\tau : End(E) \to M_2(\mathbb{Z}/n\mathbb{Z}).$$

Definition 95. Let E be an elliptic curve over $\mathbb{Q}$. We define the field of definition of $E[n]$ over $\mathbb{Q}$ as $\mathbb{Q}(E[n]) = \mathbb{Q}(x_1, y_1, \dots, x_{n^2-1}, y_{n^2-1})$ where $(x_1 : y_1 : 1), \dots, (x_{n^2-1} : y_{n^2-1} : 1), (0 : 1 : 0)$ are the n-division points of E.

The field $\mathbb{Q}(E[n])$ has some neat properties:

Proposition 96. *(cf.* [11, Ch 6.2 p.189]*) Let E be an elliptic curve over $\mathbb{Q}$.*

(a) Let $P = (x, y) \in E[n]$ be an n-division point. Then x and y are algebraic over $\mathbb{Q}$.

(b) The field of definition $\mathbb{Q}(E[n])$ is a finite Galois extension of $\mathbb{Q}$.

Now we will examine what Galois actions do with points on elliptic curves.

Definition 97. Let $K/\mathbb{Q}$ be a Galois extension and E be an elliptic curve defined over $\mathbb{Q}$. Then for $P \in E(K)$ and $\sigma \in Gal(K/\mathbb{Q})$ define

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & P = (x, y) \neq O \\ O & P = O \end{cases}.$$

Proposition 98. *(cf.* [11, Ch 6.2 p.186]*) Let E be an elliptic curve over $\mathbb{Q}$ and let $K/\mathbb{Q}$ be a Galois extension. Then*

(a) $E(K)$ is a subgroup of $E(\mathbb{C})$.

(b) For $\sigma \in Gal(K/\mathbb{Q})$ and $P \in E(K)$ we have $\sigma(P) \in E(K)$.

(c) For all $P \in E(K)$ and all $\sigma \in Gal(K/\mathbb{Q})$ we have

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

So the Galois group $Gal(K/\mathbb{Q})$ acts on the abelian group $E(K)$ (i.e. $E(K)$ is a $Gal(K/\mathbb{Q})$-module) and for $K \supseteq \mathbb{Q}(E[n])$ we have that $Gal(K/\mathbb{Q})$ acts on $E[n]$. Similarly to Prop.94 we can describe this action explicitly via two generators P_1 and P_2 of $E[n]$. By looking at the kernel of this action one can now show the following theorem.

Theorem 99. *(cf.* [11, Ch 6.3 p.196]*) Let E be an elliptic curve over $\mathbb{Q}$ and $n \geq 2$ an integer. Then there is an injective homomorphism*

$$\rho_n : Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

5. Abelian Extensions of $\mathbb{Q}(i)$ and Ramification of Prime Ideals in these Extensions

In this chapter we will start by showing how abelian extensions of $\mathbb{Q}(i)$ can be obtained by adjoining division points of a certain elliptic curve E. (We mainly follow the treatment in [11, Ch 6]. A more general (but less explicit) approach with arbitrary quadratic field extensions can be found in [9, Ch 2]) . Then we will study the ramification of prime ideals in some of these extensions. Finally we will localize these extensions at their ramified primes and try to find their norm groups via a suitable Lubin-Tate prime element.

5.1. **Abelian extensions of $\mathbb{Q}(i)$.** The elliptic curve E that we will use in the remainder of this paper is given by:

$$E : y^2 = x^3 + x.$$

It has the endomorphism ring $End(E) \cong \mathbb{Z}[\phi] \cong \mathbb{Z}[i]$ (see Cor. 91), where ϕ is given by

$$\phi : E(\mathbb{C}) \to E(\mathbb{C})$$

$$(x, y) \mapsto (-x, iy).$$

Now let $K[n] := \mathbb{Q}(i)(E[n])$ be the field generated by i and the coordinates of the n-division points of E. If we fix generators P_1 and P_2 of $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ then by using Prop. 94 and Thm. 99 we see that both ϕ and the elements of $Gal(K[n]/\mathbb{Q})$ can be represented as elements of $GL_2(\mathbb{Z}/n\mathbb{Z})$ acting on $E[n]$ and we can identify ϕ and the elements of $Gal(K[n]/\mathbb{Q})$ with such matrices.

We then have the following lemma:

Lemma 100. *(cf.* [11, Ch 6 p.206ff]*) The matrix ϕ is not a scalar matrix modulo l for all primes l dividing n. I.e. for $\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ at least one of the following conditions is true:*
(i) $b \not\equiv 0 (mod\ l)$;
(ii) $c \not\equiv 0 (mod\ l)$;
(iii) $a \not\equiv d (mod\ l)$.

Now we can use another lemma for ϕ:

Lemma 101. *(cf. [11, Ch 6 p.208ff]) Let $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$ be a matrix that is not a scalar matrix modulo l for any prime l dividing n. Then the subgroup*

$$G = \{B \in GL_2(\mathbb{Z}/n\mathbb{Z}) : AB = BA\} \leq GL_2(\mathbb{Z}/n\mathbb{Z})$$

is abelian.

This lemma now allows us to prove the following theorem:

Theorem 102. *(cf. [11, Ch 6 p.205ff]) The extension $K[n]/\mathbb{Q}(i)$ is abelian.*

Proof. For $\sigma \in Gal(K_n/\mathbb{Q}(i))$ we have:

$$\sigma(\phi(x,y)) = \sigma(-x, iy) = (-\sigma(x), \sigma(i)\sigma(y)) = (-\sigma(x), i\sigma(y))$$

and

$$\phi(\sigma(x,y)) = \phi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)).$$

Hence σ commutes with ϕ and by Lemma 101 the extension $K_n/\mathbb{Q}(i)$ is abelian. □

Conversely one can show that the maximal abelian extension of $\mathbb{Q}(i)$ is in fact given by $\prod_{n\in\mathbb{N}} K[n]/\mathbb{Q}(i)$ (cf. [9, Ch 2 §5]). Our goal is now to describe these abelian extensions as explicitly as possible with focus on ramifications of prime ideals.

5.2. **Division polynomials.** First we want to find an explicit algebraic description of the n-division points $E[n]$. This can be done via the so called division polynomials (cf. [10, Ch 3 Ex 7] and [4, Ch 13.9]):

Definition 103. Let E/K be an elliptic curve given in short Weierstrass form $E : y^2 = x^3 + Ax + B$. We define the division polynomials $\psi_n \in \mathbb{Z}[A, B, x, y]$ recursively by the following:

$$\begin{aligned}
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^2 - 8B^2)
\end{aligned}$$

and

$$\begin{aligned}\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1} \;\; n \geq 2\\ \psi_{2n} &= \frac{\psi_n}{2y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \;\; n \geq 3.\end{aligned}$$

Proposition 104. *Let E/K be an elliptic curve as in the definition above. Then the set of points $P = (x, y) \in E(\overline{K})$ for which ψ_n vanishes are exactly the set of n-division points $E[n]$ without the point O at infinity.*

Proof. (Sketch) By using the explicit addition formula on E one can show with induction that the multiplication-by-n maps $[n]$ are given by

$$[n](x, y) = \left(\frac{\phi_n(x, y)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\right),$$

where $\phi_n, \omega_n \in K[x, y]$ are polynomials in two variables that are relatively prime to ψ_n. Hence the points $P \in E(\overline{K})$ for which $\psi_n(P) = 0$ are exactly the n-division points of E. □

So the n-division polynomial characterizes the n-division points.

Example 105. For our elliptic curve $E : y^2 = x^3 + x$ we get

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6x^2 - 1$$

$$\psi_4 = 4y(x^6 + 5x^4 - 5x - 1)$$

$$\vdots$$

5.3. **The criterion of Néron-Ogg-Shafarevic.** To gain results about ramification of prime ideals we will need some theory about elliptic curves over local fields.

In the following let K be a local field with valuation ν, valuation ring R and residue class field κ. Let E/K be an elliptic curve with Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then for every $u \in K$ the substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ leads to a new equation where a_i is replaced by u^ia_i. Hence there is always a

Weierstrass equation such that all coefficients lie in R. Then among all those Weierstrass equations there has to be one with minimal discriminant Δ in the following sense:

Definition 106. Let E/K be an elliptic curve. A Weierstrass equation $E: y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ is called a minimal Weierstrass equation for E if $\nu(\Delta)$ is minimized subject to the condition that all its coefficients a_1, a_2, a_3, a_4, a_6 lie in R.

There is a sufficient condition for minimality that is rather easy to check: If $a_i \in R$ and $\nu(\Delta) < 12$ then E is minimal (c.f. [10, Ch 7 Rem 1.1]). Now we define good reduction on elliptic curves that allows us to state the criterion of Néron-Ogg-Shavarevich which tells us that in most cases the m-division points generate a nonramified extension.

Definition 107. Let E be an elliptic curve over a local field K and let $\tilde{E}$ be the reduction modulo the maximal ideal $\mathfrak{p}$ in R of a minimal Weierstrass equation of E. Then we say that E has good reduction if the curve $\tilde{E}/\kappa$ is nonsingular.

Theorem 108. *(Criterion of Néron-Ogg-Shafarevich, cf.* [10, Ch 7 Thm 7.1]*) Let E be an elliptic curve over a local field K and let κ be the residue class field of K. Then the following are equivalent:*

(a) The elliptic curve E/K has good reduction.

(b) The set of m-division points $E[m]$ (i.e. the extension $K(E[m])/K$) is unramified for all integers $m \in \mathbb{N}$ which are relatively prime to $char(\kappa)$.

Example 109. Let $\mathfrak{p}$ be a prime ideal in $K = \mathbb{Q}(i)$, $K_\mathfrak{p}$ the corresponding local field and $\kappa_\mathfrak{p}$ the residue class field. If we look at our elliptic curve

$$E: y^2 = x^3 + x$$

over $K_\mathfrak{p}$ we get that $\Delta = (1+i)^{12} = -64$. Using Prop. 81 we get that for $char(\kappa_\mathfrak{p}) \neq 2$ (i.e $\mathfrak{p} \neq (1+i)$) the curve $\tilde{E}$ is nonsingular and the criterion tells us that the extensions $K[n] = \mathbb{Q}(i)(E[n])/\mathbb{Q}(i)$ are unramified at $\mathfrak{p}$ for all $n \in \mathbb{N}$ which are relatively prime to $char(\kappa_\mathfrak{p})$. For $\mathfrak{p} = (1+i)$ however $\tilde{E}$ is singular and we will see below that $K[3]$ is indeed ramified at $\mathfrak{p}$ although $3 \nmid char(\kappa_\mathfrak{p})$.

5.4. **Ramification of primes in the extension $\mathbb{Q}(i)(E[n])/\mathbb{Q}(i)$.** Using the results above we will now explicitly determine the ramification of primes in the extension $K[n] = \mathbb{Q}(i)(E[n])/\mathbb{Q}(i)$ for $n = 2, 3, 4$, where $E : y^2 = x^3 + x$ is the elliptic curve studied above.

To do so we first recall the structure of the prime ideals in $\mathbb{Z}[i] = O_{\mathbb{Q}(i)}$ first:

Proposition 110. *(cf.* [7, Ch 1 Thm 1.4]*) Let p be a prime in $\mathbb{Z}$ and $R = \mathbb{Z}[i]$. If*

(i) $p = 2$ then $(p)R = (1 + i)^2$ (we say $p = 2$ is ramified) and $R/(1 + i) \cong \mathbb{F}_2$),

(ii) $p \equiv 1 \mod 4$ then there are $a, b \in \mathbb{N}$ with $a^2 + b^2 = p$ and hence $(p)R = (a+bi)(a-bi)$ (we say p splits) and $R/(a+bi) \cong R/(a-bi) \cong \mathbb{F}_p$,

(iii) $p \equiv 3 \mod 4$ then (p) remains prime in R. I.e. $(p)R = (p)$ (we say p remains inert) and $R/(p) \cong \mathbb{F}_{p^2}$.

5.4.1. *The case $n = 2$:* This case is fairly easy: The 2-division points are given by $(0, 0), (i, 0), (-i, 0), O$. All of their coordinates lie in $\mathbb{Q}(i)$ and so the extension $K[2]/\mathbb{Q}(i)$ is trivial and therefore unramified.

5.4.2. *The case $n = 3$:*

Proposition 111. *The 3-division points of*

$$E : y^2 = x^3 + x$$

are given by

$$\begin{aligned} E[3] \quad = \quad & \{O, (\alpha, \pm\beta), (-\alpha, \pm i\beta), \\ & ((2 + \sqrt{3})i\alpha, \pm\beta\frac{1 + \sqrt{3}}{2}(1 - i)), \\ & (-(2 + \sqrt{3})i\alpha, \pm\beta\frac{1 + \sqrt{3}}{2}(1 + i))\} \end{aligned}$$

where $\alpha = \sqrt{\frac{2}{\sqrt{3}} - 1}$ and $\beta = \sqrt{\frac{2}{\sqrt{3}}}\alpha$.[8]

Proof. By Ex.105 the x-coordinates of the 3-division points (except O) are given by the zeros of

$$\psi_3 = 3x^4 + 6x^2 - 1.$$

[8] Here and in the following we stick to the following rule: If we write $\sqrt{a}$ resp. $a^{\frac{1}{n}}$ we always have $a \in \mathbb{R}^+$ and we always mean the unique positive real root of $T^2 - a$ resp. $T^n - a$.

By a simple calculation we get the roots $\alpha, -\alpha, (2+\sqrt{3})i\alpha, -(2+\sqrt{3})i\alpha$. Plugging those into the equation of E one gets the points given in the proposition. □

Since $\sqrt{3} = \frac{3(\alpha^2+1)}{2} \in \mathbb{Q}(i)(\alpha)$ we have $K[3] = \mathbb{Q}(i)(E[3]) = \mathbb{Q}(i)(\alpha, \beta)$. To study $K[3]$ we will study the following tower of field extensions:

$$\begin{array}{c} N = M(\beta) = K[3] \\ | \\ M = L(\alpha) \\ | \\ L = \mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{3}) \\ | \\ \mathbb{Q}(i) \\ \left(\begin{array}{c} | \\ \mathbb{Q} \end{array} \right) \end{array}$$

where $\zeta = \zeta_{12} = e^{\frac{\pi i}{6}} = \frac{\sqrt{3}+i}{2}$.[9] Then $[L : \mathbb{Q}(i)] = [M : L] = [N : M] = 2$ and we can study these extensions individually.

Now we will look at the ramification of prime ideals in the extension $N/\mathbb{Q}(i)$. Doing so we use the following notation: If $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(i)$ and $F/\mathbb{Q}(i)$ is a field extension we denote by $\mathfrak{p}_F$ a prime ideal in O_F lying over $\mathfrak{p}$.

The case $\mathfrak{p} \neq (3), (1+i)$*:*

Proposition 112. *Let* $\mathfrak{p} \neq (3), (1+i)$ *be a prime ideal in* $\mathbb{Q}(i)$ *and* $\mathfrak{p}_N$ *be an ideal in* N *lying over* $\mathfrak{p}$*. Then the extension* $N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{\mathfrak{p}}$ *is unramified.*

Proof. By the theorem of Néron-Ogg-Shavarevich (Thm. 108) the primes $\mathfrak{p}$ that can ramify are only those with bad reduction and those for which $\kappa_{\mathfrak{p}}$ divides $n = 3$. Since E only has bad reduction at $\mathfrak{p} = (1+i)$ (see Ex. 109) and $char(\kappa_{\mathfrak{p}}) = 3$ only if $\mathfrak{p} = (3)$ the extension $N/\mathbb{Q}(i)$ is unramified in all other cases. □

The case $\mathfrak{p} = (3)$*:*

[9] In the following $\zeta = \zeta_{12}$ unless stated otherwise.

Theorem 113. *At $\mathfrak{p} = (3)$ the extension $N/\mathbb{Q}(i)$ is totally ramified. I.e. there is a unique prime ideal $\mathfrak{p}_N \subset O_N$ such that $\mathfrak{p}_N^8 = (3)$, $e(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(3)}) = 8$ and $f(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(3)}) = 1$.*

Proof. Define ν_3 to be an arbitrary extension of the valuation of (3) in $\mathbb{Q}(i)$ onto N (with $\nu_3(3) = 1$). Then

$$\begin{aligned}\nu_3(\beta) &= \nu_3\left(\sqrt{\frac{2}{\sqrt{3}}\alpha}\right)\\ &= \frac{1}{2}\nu_3\left(\frac{2}{\sqrt{3}}\right) + \frac{1}{2}\nu_3(\alpha)\\ &= -\frac{1}{4} + \frac{1}{2}\nu_3\left(\sqrt{\frac{2}{\sqrt{3}} - 1}\right)\\ &= -\frac{1}{4} - \frac{1}{8} = -\frac{3}{8}.\end{aligned}$$

Hence $8 \mid e(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(3)})$ for some prime ideal $\mathfrak{p}_N$. Since $8 = [N : \mathbb{Q}(i)] \geq [N_{\mathfrak{p}_N} : \mathbb{Q}(i)_{(3)}] \geq 8$ we get what is claimed. □

The case $\mathfrak{p} = (1+i)$: We will need the following theorem of Kummer:

Theorem 114. *(Kummer, cf.* [1, Ch 3.App, Kummer's Thm]*) Let L/K be an extension of algebraic number fields. Let $\theta \in O_L$ such that $O_L = O_K[\theta]$ and let $q \in O_K[T]$ be its minimal polynomial over K. Now fix a prime ideal $\mathfrak{p}_K$ in O_K. Denote by $res(q, \mathfrak{p})$ the polynomial obtained by reducing q modulo $\mathfrak{p}_K$ (i.e. q as a polynomial in $\kappa[T]$, where κ is the residue class field of $K_\mathfrak{p}$). If*

$$res(q, \mathfrak{p}_K) = \prod_{j=1}^{t} g_j^{e_j}$$

is the factorization of $res(q, \mathfrak{p})$ into irreducible polynomials g_j which have degree f_j, then there are polynomials $G_j \in O_K[T]$ with $res(G_j, \mathfrak{p}) = g_j$such that

$$\mathfrak{p}_K O_L = \prod_{j=1}^{r} (\mathfrak{p}_K, G_j(\theta))^{e_j}$$

with the f_j to be the respective residue class field degrees.

Now we can determine the ramification at $\mathfrak{p} = (1+i)$:

Theorem 115. *Let $\mathfrak{p}_N$ be a prime ideal in N lying over $(1+i)$. Then the extension $N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(1+i)}$ is ramified with $e(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(1+i)}) = 4$ and $f(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(1+i)}) = 2$.*

To prove this theorem we will determine the ramification of $\mathfrak{p} = (1+i)$ in each extension in the field tower $N/M/L/\mathbb{Q}(i)$ separately. Since all these extensions have degree two we can hope that there is always a generator θ of the ring of integers which we need to use Kummer's theorem. So the main part that remains is to find such a generator for every extension.

For the extension $L/\mathbb{Q}(i)$ this is rather easy because $L = \mathbb{Q}(\zeta_{12})$ is a cyclotomic field and one can use the following lemma:

Lemma 116. *(cf.* [7, Ch 1 Prop 10.2]*) Let n be a natural number and $L = \mathbb{Q}(\zeta_n)$ the corresponding cyclotomic field. (I.e. ζ_n is a primitive n-th root of unity.) Then the ring of integers has a $\mathbb{Z}$-basis given by $1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$. I.e.*

$$O_L = \mathbb{Z} \oplus \zeta_n\mathbb{Z} \oplus \cdots \oplus \zeta_n^{\varphi(n)-1}\mathbb{Z} = \mathbb{Z}[\zeta_n].$$

In our case this means

Lemma 117. *For $L = \mathbb{Q}(\zeta_{12})$ we have*

$$O_L = \mathbb{Z}[\zeta_{12}] \cong \mathbb{Z}[T]/(T^4 - T^2 + 1).$$

Now we can prove the first step of the theorem.

Lemma 118. *The extension $L/\mathbb{Q}(i)$ is inert in $(1+i)$. I.e. $\mathfrak{p}_L = (1+i)O_L$ is the unique prime ideal in L lying over $(1+i)$ and we have*

$$e(L_{(1+i)}/\mathbb{Q}(i)_{(1+i)}) = 1$$

and

$$f(L_{(1+i)}/\mathbb{Q}(i)_{(1+i)}) = 2.$$

Proof. By Lemma 116 we have

$$O_L = \mathbb{Z}[\zeta] = \mathbb{Z}[i][\zeta]$$

and since

$$\begin{aligned}\zeta^2 &= \frac{1}{2}(1+\sqrt{3}i)\\ &= i\frac{1}{2}(\sqrt{3}+i)-1\\ &= i\zeta-1\end{aligned}$$

the minimal polynomial of ζ over $\mathbb{Z}[i]$ is given by

$$mipo(\zeta,\mathbb{Q}(i)) = T^2 - iT - 1.$$

After reducing it modulo $(1+i)$ (i.e. reducing it to the residue class field $\kappa \cong \mathbb{F}_2$ of $\mathbb{Q}(i)_{(1+i)}$ we get

$$res(mipo(\zeta,\mathbb{Q}(i)),(1+i)) = T^2+T+1 \in \kappa[T],$$

which is irreducible. So by Kummer's theorem (Thm 114) the prime $(1+i)$ is purely inert in L and we have $e(L_{(1+i)}/\mathbb{Q}(i)_{(1+i)}) = 1$ and $f(L_{(1+i)}/\mathbb{Q}(i)_{(1+i)}) = 2$. □

Corollary 119. *The residue class field λ of $L_{(1+i)}$ is isomorphic to $\mathbb{F}_4$ and $\zeta^* := res(\zeta)$ is a generator of the multiplicative group λ^* (i.e. $\zeta^* \neq 0, 1$).*

Proof. Let $\kappa \cong \mathbb{F}_2$ be the residue class field of $\mathbb{Q}(i)_{(1+i)}$. By Lemma 118 we have $[\lambda:\kappa]=2$ and by its proof we have

$$res(mipo(\zeta,\mathbb{Q}(i)),(1+i)) = T^2+T+1.$$

Hence $\zeta^* = res(\zeta) \notin \kappa$ and therefore has to be a generator of λ^*. □

Next we are looking at the extension M/L. To find an O_L-basis of O_M we multiply α by an element of L such that the result w becomes integral:

By Prop. 111 we have

$$\alpha = \sqrt{\frac{2}{\sqrt{3}}-1} = (2-\sqrt{3})^{\frac{1}{2}}3^{-\frac{1}{4}}.$$

Since $2-\sqrt{3} = \frac{1}{2}(4-2\sqrt{3}) = \frac{1}{2}(\sqrt{3}-1)^2$ we get

$$\alpha = (2-\sqrt{3})^{\frac{1}{2}}3^{-\frac{1}{4}} = (\sqrt{3}-1)2^{-\frac{1}{2}}3^{-\frac{1}{4}} = \frac{(\sqrt{3}-1)}{2\sqrt{3}}2^{\frac{1}{2}}3^{\frac{1}{4}}.$$

We know that $\zeta_8 = e^{\frac{i\pi}{4}} = 2^{-\frac{1}{2}}(1+i)$. Hence $2^{\frac{1}{2}} = \frac{1+i}{\zeta_8} = (1+i)\zeta_8^7 = -(1+i)\zeta_8^3$. We get

$$\alpha = \frac{(\sqrt{3}-1)}{2\sqrt{3}} 2^{\frac{1}{2}} 3^{\frac{1}{4}} = -\frac{(\sqrt{3}-1)(1+i)}{2\sqrt{3}} \zeta_8^3 3^{\frac{1}{4}} = -\frac{(\sqrt{3}-1)(1+i)}{2\sqrt{3}} w$$

with $w = \zeta_8^3 3^{\frac{1}{4}} \in M$.

Lemma 120. *The element $w = \zeta_8^3 3^{\frac{1}{4}} \in M$ has the following properties:*

(i) $M = L(w) = L \oplus Lw$.

(ii) $w^2 = 1 - 2\zeta^2 (\zeta = \zeta_{12})$.

(iii) $mipo(w, L) = T^2 - (1 - 2\zeta^2)$.

(iv) For $id \neq \sigma \in Gal(M/L)$ we have $\sigma(w) = -w$.

(v) $mipo(w, \mathbb{Q}) = T^4 + 3$.

(vi) $w \in O_M$.

Proof. (i) Since $M = L(\alpha)$ and $\frac{\alpha}{w} = -\frac{(\sqrt{3}-1)(1+i)}{2\sqrt{3}} \in L$ we get $M = L(w)$.

(ii) $w^2 = \zeta_8^6 3^{\frac{1}{2}} = -i\sqrt{3} = 1 - 2\zeta^2$.

(iii) Since $w \notin L$ the claim is a direct consequence of (ii).

(iv) Follows directly from (iii) and $0 = Tr_{M/L}(w) = w + \sigma(w)$.

(v) $T^4 + 3$ is irreducible over $\mathbb{Q}$ and $w^4 + 3 = 0$.

(vi) $w \in O_M$ is an immediate consequence of (v). □

So we have

$$M = L \oplus Lw = (\mathbb{Q} + \zeta\mathbb{Q} + \zeta^2\mathbb{Q} + \zeta^3\mathbb{Q}) \oplus (\mathbb{Q} + \zeta\mathbb{Q} + \zeta^2\mathbb{Q} + \zeta^3\mathbb{Q})w$$

and we can represent the elements of M as 8-tupels of rational numbers. To find out which of them are integral over O_L we will compute their minimal polynomials over L. By doing that we get the following lemma:

Lemma 121. *As an additive group the quotient $O_M/O_L[w]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The residue classes are represented by the elements $0, \theta_M, \theta_M^{'}, \theta_M^{''}$ given by*

$$\theta_M = \frac{1}{2}(1 + \zeta + \zeta^2)(1 + w),$$

$$\theta_M^{'} = \frac{1}{2}(\zeta + \zeta^2 + \zeta^3)(1 + w)$$

and

$$\theta_M^{''} = \frac{1}{2}(1 + \zeta^3)(1 + w).$$

Proof. Let $x = A + Bw$ be an arbitrary element in M where

$$A = a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3$$

and

$$B = a_5 + a_6\zeta + a_7\zeta^2 + a_8\zeta^3$$

lie in L. Since $\sigma(x) = \sigma(A + Bw) = A - Bw$ the minimal polynomial of x over L is given by

$$mipo(x, L) = T^2 - 2AT + (A^2 - B^2w^2).$$

Because x is integral in M if and only if x is integral over O_L[10], we have that $x \in O_M$ if and only if $2A, A^2 - B^2w^2 \in O_L$. So assuming $x \in O_M$ we get $A \in \frac{1}{2}O_L$ as a necessary condition. Additionally $A^2 - B^2w^2 \in O_L$ or equivalently: for every prime ideal $\mathfrak{p}_L$ in O_L the valuation $\nu_{\mathfrak{p}_L}(A^2 - B^2w^2)$ is nonnegative.[11]

Since $2A \in O_L$ we have

$$\nu_{\mathfrak{p}_L}(A) \geq \begin{cases} -2 & \mathfrak{p}_L = (1+i) \\ 0 & \mathfrak{p}_L \neq (1+i) \end{cases}.$$

By Thm. 113 there is a unique prime ideal $\mathfrak{p}_{L,3}$ in L lying over $\mathfrak{p} = (3)$. Since $mipo(w, \mathbb{Q}) = T^4 + 3$ we have

$$\nu_{\mathfrak{p}_L}(w^2) = \begin{cases} 1 & \mathfrak{p}_L = \mathfrak{p}_{L,3} \\ 0 & \mathfrak{p}_L \neq \mathfrak{p}_{L,3} \end{cases}.$$

Hence we obtain

$$\nu_{\mathfrak{p}_L}(B) \geq \begin{cases} -2 & \mathfrak{p}_L = (1+i) \\ -\frac{1}{2} & \mathfrak{p}_L = \mathfrak{p}_{L,3} \\ 0 & \mathfrak{p}_L \neq (1+i), \mathfrak{p}_{L,3} \end{cases}$$

and since $B \in L$ and $\nu_{\mathfrak{p}_{L,3}}(L^*) = \mathbb{Z}$ we can conclude that $\nu_{\mathfrak{p}_{L,3}}(B) \geq 0$ and hence $B \in \frac{1}{2}O_L$. Therefore $a_1, \ldots, a_8 \in \frac{1}{2}\mathbb{Z}$.

Since for $a_1, \ldots, a_8 \in \mathbb{Z}$ we have that $x \in O_L[w] \subset O_M$ all we have to do is check whether $x \in O_M$ (i.e. whether $A^2 - B^2w^2 \in O_L$) for

[10] Cf. [7, Thm 2.4 Ch 1]

[11] Here and in the following for a prime ideal $\mathfrak{p}$ in a ring R the symbol $\nu_{\mathfrak{p}}$ denotes the normalized valuation on $R_{\mathfrak{p}}$.

$(a_1, \ldots, a_8) \in \{0, \frac{1}{2}\}^8$. Checking these $2^8 = 256$ cases[12] we get that $x \in O_M$ if and only if

$$x \equiv 0, \theta_M, \theta_M^{'}, \theta_M^{''} \mod O_L + wO_L,$$

where

$$\theta_M = \frac{1}{2}(1+\zeta+\zeta^2)(1+w),$$
$$\theta_M^{'} = \frac{1}{2}(\zeta+\zeta^2+\zeta^3)(1+w)$$

and

$$\theta_M^{''} = \frac{1}{2}(1+\zeta^3)(1+w).$$

□

We will now compute the minimal polynomial of θ_M over L directly. So we will immediately see that in fact $\theta_M \in O_M$. (Analogously one could compute the minimal polynomials of $\theta_M^{'}$ and $\theta_M^{''}$ to see that they are also integral.)

Lemma 122. *The minimal polynomial of $\theta_M = \frac{1}{2}(1+\zeta+\zeta^2)(1+w)$ over L is given by*

$$mipo(\theta_M, L) = T^2 - (1+\zeta+\zeta^2)T + (-2-\zeta+2\zeta^2+2\zeta^3).$$

Proof. Let $\sigma \in Gal(M/L)$ be the nontrivial Galois automorphism of M/L. Since $mipo(w, L) = T^2 - (1-2\zeta^2)$ we have $\sigma(w) = -w$. So

$$\sigma(\theta_M) = \sigma(\frac{1}{2}(1+\zeta+\zeta^2)(1+w)) = \frac{1}{2}(1+\zeta+\zeta^2)(1-w).$$

Hence

$$Tr_{M/L}(\theta_M) = \theta_M + \sigma(\theta_M) = 1+\zeta+\zeta^2.$$

Furthermore we have[13]

$$\begin{aligned} N_{M/L}(\theta_M) &= \theta_M\sigma(\theta_M) \\ &= \frac{1}{4}(1+\zeta+\zeta^2)^2(1-w^2) \\ &= \frac{1}{4}(1+\zeta+\zeta^2)^2 2\zeta^2 \\ &= -2-\zeta+2\zeta^2+2\zeta^3. \end{aligned}$$

[12] The function FindInteger, which I wrote in Mathematica (see the Appendix), gives the solutions listed here.

[13] Here we use $w^2 = 1-2\zeta^2$ (Lemma 120(ii)). In the last computation we use the function NormalPoly, which I wrote in Mathematica (see the Appendix).

So

$$mipo(\theta_M, L) = T^2 - (1+\zeta+\zeta^2)T + (-2-\zeta+2\zeta^2+2\zeta^3).$$

□

Lemma 123. *The ring of integers O_M of M is given by*

$$O_M = O_L[\theta_M].$$

Proof. By construction of θ_M we have that $\theta_M \in O_M$. So we have to show that $O_M \subseteq O_L[\theta_M]$. By the calculation above we know that $O_M = O_L[w, \theta_M, \theta_M^{'}, \theta_M^{''}]$. So we have to show that $w, \theta_M^{'}, \theta_M^{''} \in O_L[\theta_M]$. Since

$$\theta_M = \frac{1}{2}(1+\zeta+\zeta^2)(1+w)$$

we have that

$$w = \frac{2\theta_M}{1+\zeta+\zeta^2} - 1.$$

By inverting[14] the term $1+\zeta+\zeta^2$, we get that

$$w = (2-\zeta-\zeta^2+\zeta^3)\theta_M - 1 \in O_L[\theta_M].$$

We have that

$$\begin{aligned} \theta_M^{'} &= \frac{1}{2}(\zeta+\zeta^2+\zeta^3)(1+w) \\ &= \frac{1}{2}\zeta(1+\zeta+\zeta^2)(1+w) \\ &= \zeta\theta_M \in O_L[\theta_M]. \end{aligned}$$

And since

$$\theta_M^{''} \equiv \theta_M^{'} + \theta_M \mod O_L[w]$$

we have

$$\theta_M^{''} \in O_L[\theta_M].$$

Hence $O_M = O_L[\theta_M]$. □

To determine the decomposition of $\mathfrak{p}_L$ in O_M by Kummer's Theorem all we have to do now is to reduce the minimal polynomial of θ_M over L modulo $(1+i)$. Since ζ reduces to ζ^*, a generator of the residue class

[14] I used the function InvertPoly (see the Appendix), which inverts elements of L polynomial in ζ.

field that has order 4 (see Lemma 118) we get

$$res(1+\zeta+\zeta^2,(1+i)) = 1+\zeta^*+(\zeta^*)^2 = 0$$

and since $res(2,(1+i)) = 0$ we have

$$res(-2-\zeta+2\zeta^2+2\zeta^3,(1+i)) = \zeta^*.$$

So we get

$$res(mipo(\theta_M,L),(1+i)) = T^2-\zeta^* = (T-(\zeta^*)^2)^2.$$

So by Kummer's theorem (Thm. 114) we get the following lemma:

Lemma 124. *The extension M/L is totally ramified in $(1+i)$:*

$$e(M_{\mathfrak{p}_M}/L_{(1+i)}) = 2$$

and

$$f(M_{\mathfrak{p}_M}/L_{(1+i)}) = 1.$$

where $\mathfrak{p}_M = (1+i,\theta_M-\zeta^2)$ is the unique prime ideal in O_M lying over $(1+i)$.

In a very similar manner one can now repeat this calculation for N/M:

By Prop. 111 we have

$$\begin{aligned}\beta &= \sqrt{\frac{2}{\sqrt{3}}\alpha} = (\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{-\frac{3}{8}} \\ &= \frac{1}{\sqrt{3}}(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}.\end{aligned}$$

We calculate:[15]

$$\begin{aligned}
((\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}})^2 &= (\sqrt{3}-1)\sqrt{2}\cdot 3^{\frac{1}{4}}\\
&= (\sqrt{3}-1)\sqrt{2}\zeta_8^{-3}w\\
&= (\sqrt{3}-1)\sqrt{2}\zeta_8^{5}w\\
&= (\sqrt{3}-1)2^{\frac{1}{2}-\frac{5}{2}}(1+i)^5 w\\
&= \frac{1}{4}(-1+2\zeta-\zeta^3)(1+\zeta^3)^5((2-\zeta-\zeta^2+\zeta^3)\theta_M-1)\\
&= (-2+2\zeta+2\zeta^2-2\zeta^3)+(4-2\zeta-6\zeta^2+6\zeta^3)\theta_M.
\end{aligned}$$

Since all the coefficients are divisible by 2 we can divide $(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}$ by $(1+i)$ and still get an integer. We write

$$\begin{aligned}
\beta &= \frac{1}{\sqrt{3}}(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}\\
&= \frac{(1+i)}{\sqrt{3}}\frac{(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}}{(1+i)}\\
&= \frac{(1+i)}{\sqrt{3}}v
\end{aligned}$$

with $v = \frac{(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}}{(1+i)}$.

Lemma 125. *The element* $v = \frac{(\sqrt{3}-1)^{\frac{1}{2}}2^{\frac{1}{4}}3^{\frac{1}{8}}}{(1+i)} \in N$ *has the following properties:*

(i) $N = M(v) = M \oplus Mv$.

(ii) $v^2 = (\zeta-\zeta^2)+(2-3\zeta+\zeta^2+\zeta^3)\theta_M$.

(iii) $mipo(v, M) = T^2 - ((\zeta-\zeta^2)+(2-3\zeta+\zeta^2+\zeta^3)\theta_M)$.

(iv) For $id \neq \sigma \in Gal(N/M)$ *we have* $\sigma(v) = -v$.

(v) $mipo(v,\mathbb{Q}) = T^8 - 6T^4 - 3$.

(vi) $v \in O_N$.

Proof. (i) Since $N = M(\beta)$ and $\frac{\beta}{v} = \frac{1+i}{\sqrt{3}} \in M$ we get $N = M(w)$.

[15] Here we use the following identities: $\zeta_8 = 2^{-\frac{1}{2}}(1+i)$; $i = \zeta^3$; $\sqrt{3} = 2\zeta - \zeta^3$ (all of those can be verified easily on the unit circle); $w = \zeta_8^3 3^{\frac{1}{4}}$ (as in Lemma 120);and $w = (2-\zeta-\zeta^2+\zeta^3)\theta_M - 1$ (by the proof of Lemma 123). The last step in the calculation is a bit tedious and can be done via the function TNormalPoly (see the Appendix).

(ii) By the calculation above we have[16]

$$\begin{aligned} v^2 &= \frac{(\sqrt{3}-1)\sqrt{2}\cdot 3^{\frac{1}{4}}}{(1+i)^2} \\ &= \frac{1}{2i}(\sqrt{3}-1)\sqrt{2}\cdot 3^{\frac{1}{4}} \\ &= -\frac{\zeta^3}{2}((-2+2\zeta+2\zeta^2-2\zeta^3)+(4-2\zeta-6\zeta^2+6\zeta^3)\theta_M) \\ &= (\zeta-\zeta^2)+(2-3\zeta+\zeta^2+\zeta^3)\theta_M \end{aligned}$$

(iii) Since $v \notin M$ the claim is a direct consequence of (ii).

(iv) Follows directly from (iii) and $0 = Tr_{N/M}(v) = v + \sigma(v)$.

(v) Since

$$\begin{aligned} v^4 &= \frac{(\sqrt{3}-1)^2 2\sqrt{3}}{(1+i)^4} \\ &= \frac{(4-2\sqrt{3})2\sqrt{3}}{-4} \\ &= 3-2\sqrt{3} \end{aligned}$$

and

$$\begin{aligned} v^8 &= (3-2\sqrt{3})^2 \\ &= 21-12\sqrt{3} \end{aligned}$$

we get

$$v^8 - 6v^4 - 3 = 0.$$

Now the polynomial $T^8 - 6T^4 - 3$ is irreducible over $\mathbb{Q}$ and hence it is the minimal polynomial of v.

(vi) $v \in O_N$ is an immediate consequence of (v). □

Again $O_M[v] \subset O_N$ and $N = M \oplus Mv$. To find O_N we will again compute the minimal polynomial of an element in N over M.

Lemma 126. *As an additive group the quotient $O_N/O_M[v]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The residue classes are represented by the elements $0, \theta_N, \theta_N^{'}, \theta_N^{''}$ given by*

$$\theta_N = \frac{1}{2}((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))(1+v),$$

[16] Again the last computation can be done using TNormalPoly (see the Appendix).

$$\theta_N^{'} = \frac{1}{2}((\zeta + \zeta^2 + \zeta^3) + \theta_M(1 + \zeta^3))(1 + v)$$

and

$$\theta_N^{''} = \frac{1}{2}((1 + \zeta^3) + \theta_M(1 + \zeta + \zeta^2))(1 + v)$$

Proof. Let $y = A + Bv$ be an arbitrary element in N where

$$A = (a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3) + (a_5 + a_6\zeta + a_7\zeta^2 + a_8\zeta^3)\theta_M$$

and

$$B = (a_9 + a_{10}\zeta + a_{11}\zeta^2 + a_{12}\zeta^3) + (a_{13} + a_{14}\zeta + a_{15}\zeta^2 + a_{16}\zeta^3)\theta_M$$

are elements of M. Then its minimal polynomial $mipo(y, M)$ is given by

$$mipo(y, M) = T^2 - 2AT + (A^2 - B^2v^2).$$

So $y \in O_N$ if and only if $2A, A^2 - B^2v^2 \in O_M$. Looking at the valuations over prime ideals $\mathfrak{p}_M$ in O_M we get

$$\nu_{\mathfrak{p}_M}(A^2 - B^2v^2) \geq 0.$$

Since $2A \in O_M$ and $(2) = \mathfrak{p}_{M,2}^4$ (see Lemma 124) we have

$$\nu_{\mathfrak{p}_M}(A) \geq \begin{cases} -4 & \mathfrak{p}_M = \mathfrak{p}_{M,2} \\ 0 & \mathfrak{p}_M \neq \mathfrak{p}_{M,2} \end{cases}$$

and we know that since $mipo(v, \mathbb{Q}) = T^8 - 6T^4 - 3$ and $(3) = \mathfrak{p}_{M,3}^4$ (see Thm. 113) we get

$$\nu_{\mathfrak{p}_M}(v^2) = \begin{cases} 1 & \mathfrak{p}_M = \mathfrak{p}_{M,3} \\ 0 & \mathfrak{p}_M \neq \mathfrak{p}_{M,3} \end{cases}.$$

Hence

$$\nu_{\mathfrak{p}_M}(B) \geq \begin{cases} -4 & \mathfrak{p}_M = \mathfrak{p}_{M,2} \\ -\frac{1}{2} & \mathfrak{p}_M = \mathfrak{p}_{M,3} \\ 0 & \mathfrak{p}_M \neq \mathfrak{p}_{M,2}, \mathfrak{p}_{M,3} \end{cases}$$

and since $\nu_{\mathfrak{p}_{M,3}}(M^*) = \mathbb{Z}$ and therefor $\nu_{\mathfrak{p}_{M,3}}(B) \geq 0$ we get $B \in \frac{1}{2}O_M$. Hence $a_1, \ldots, a_{16} \in \frac{1}{2}\mathbb{Z}$.

Again by checking[17] whether $y \in O_N$ for $(a_1, \ldots, a_{16}) \in \{0, \frac{1}{2}\}^{16}$ we get that $y \in O_N$ if and only if

$$y \equiv 0, \theta_N, \theta_N^{'}, \theta_N^{''} \mod O_M + vO_M,$$

where

$$\theta_N = \frac{1}{2}((1+\zeta+\zeta^2) + \theta_M(\zeta+\zeta^2+\zeta^3))(1+v),$$

$$\theta_N^{'} = \frac{1}{2}((\zeta+\zeta^2+\zeta^3) + \theta_M(1+\zeta^3))(1+v)$$

and

$$\theta_N^{''} = \frac{1}{2}((1+\zeta^3) + \theta_M(1+\zeta+\zeta^2))(1+v).$$

□

Lemma 127. *The minimal polynomial of θ_N over M is given by*

$$\begin{aligned} mipo(\theta_N, M) &= T^2 - ((1+\zeta+\zeta^2) + \theta_M(\zeta+\zeta^2+\zeta^3))T + \\ &\quad ((4+6\zeta+3\zeta^2-\zeta^3) + \theta_M(-3+5\zeta^2+5\zeta^3)). \end{aligned}$$

Proof. Let $\sigma \in Gal(N/M)$ be the nontrivial Galois homomorphism of N/M. Since $mipo(v, M) = T^2 - ((\zeta - \zeta^2) + (2+3\zeta+\zeta^2+\zeta^3)\theta_M)$ we have $\sigma(v) = -v$. So

$$\begin{aligned} \sigma(\theta_N) &= \sigma(\frac{1}{2}((1+\zeta+\zeta^2) + \theta_M(\zeta+\zeta^2+\zeta^3))(1+v)) \\ &= \frac{1}{2}((1+\zeta+\zeta^2) + \theta_M(\zeta+\zeta^2+\zeta^3))(1-v). \end{aligned}$$

Hence

$$\begin{aligned} Tr_{N/M}(\theta_N) &= \theta_N + \sigma(\theta_N) \\ &= (1+\zeta+\zeta^2) + \theta_M(\zeta+\zeta^2+\zeta^3) \end{aligned}$$

[17] Similar to Lemma 121 I used the function TFindInteger (see the Appendix) to get these solutions.

and[18]

$$\begin{aligned}
N_{N/M}(\theta_N) &= \theta_N\sigma(\theta_N) \\
&= \frac{1}{4}((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))^2(1-v^2) \\
&= \frac{1}{4}((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))^2((1-\zeta+\zeta^2)+ \\
&\quad \theta_M(-2+3\zeta-\zeta^2-\zeta^3) \\
&= (4+6\zeta+3\zeta^2-\zeta^3)+\theta_M(-3+5\zeta^2+5\zeta^3)
\end{aligned}$$

So

$$\begin{aligned}
mipo(\theta_N, M) &= T^2-((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))T+ \\
&\quad ((4+6\zeta+3\zeta^2-\zeta^3)+\theta_M(-3+5\zeta^2+5\zeta^3)).
\end{aligned}$$

□

Lemma 128. *The ring of integers O_N of N is given by*

$$O_N = O_M[\theta_N].$$

Proof. By construction $\theta_N \in O_N$. So we have to show that $O_N \subseteq O_M[\theta_N]$. By the calculation above we know that $O_N = O_M[v, \theta_N, \theta_N', \theta_N'']$. So we have to show that $v, \theta_N', \theta_N'' \in O_M[\theta_N]$.
Since

$$\theta_N = \frac{1}{2}((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))(1+v)$$

we have that

$$v = \frac{2\theta_N}{(1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3)} - 1.$$

By inverting[19] the term $(1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3)$ we get

$$v = ((2-2\zeta-\zeta^2+\zeta^3)+\theta_M(-\zeta+2\zeta^2-\zeta^3))\theta_N - 1 \in O_M[\theta_N].$$

We have that

[18] Here we use $v^2 = (\zeta-\zeta^2)+\theta_M(2-3\zeta+\zeta^2+\zeta^3)$ (see Lemma 125(ii). In the last computation we use the function TNormalPoly (see the Appendix).

[19] Here I used the function TInvertPoly (see the Appendix).

$$\begin{aligned}\theta_N' &= \frac{1}{2}((\zeta+\zeta^2+\zeta^3)+\theta_M(1+\zeta^3))(1+v)\\ &= \zeta\cdot\frac{1}{2}((1+\zeta+\zeta^2)+\theta_M(\zeta+\zeta^2+\zeta^3))(1+v)+\theta_M(1-\zeta^2)(1+v)\\ &= \zeta\theta_N+\theta_M(1-\zeta^2)(1+v)\in O_M[\theta_N]\end{aligned}$$

and since

$$\theta_N'' \equiv \theta_N' + \theta_N \mod O_M[v]$$

we have

$$\theta_N'' \in O_M[\theta_N].$$

Hence $O_N = O_M[\theta_N]$. □

Now we will reduce the minimal polynomial of θ_N over M modulo $\mathfrak{p}_M$ to use Kummer's theorem. Using $res(\zeta,\mathfrak{p}_M)=\zeta^*$ and $res(\theta_M,\mathfrak{p}_M)=(\zeta^*)^2$ we get

$$\begin{aligned}& res(1+\zeta+\zeta^2+\theta_M(\zeta+\zeta^2+\zeta^3),\mathfrak{p}_M\\ =\;& res((1+\zeta+\zeta^2)(1+\theta_M\zeta),\mathfrak{p}_M\\ =\;& (1+\zeta^*+(\zeta^*)^2)(1+(\zeta^*)^3)\\ =\;& 0\end{aligned}$$

and

$$\begin{aligned}& res((4+6\zeta+3\zeta^2-\zeta^3)+\theta_M(-3+5\zeta^2+5\zeta^3),\mathfrak{p}_{M,2})\\ =\;& ((\zeta^*)^2+(\zeta^*)^3)+(\zeta^*)^2(1+(\zeta^*)^2+(\zeta^*)^3\\ =\;& 1+\zeta^*+(\zeta^*)^2\\ =\;& 0.\end{aligned}$$

So we get

$$res(mipo(\theta_N,M),\mathfrak{p}_M)=T^2.$$

So by Kummer's theorem (Thm. 114) we get the following lemma:

Lemma 129. *The extension N/M is totally ramified in $\mathfrak{p}_M$:*

$$e(N_{\mathfrak{p}_N}/M_{\mathfrak{p}_M})=2$$

and

$$f(N_{\mathfrak{p}_N}/M_{\mathfrak{p}_M})=1.$$

where $\mathfrak{p}_N = (1+i, \theta_M - \zeta^2, \theta_N)$ *is the unique prime ideal in* O_N *lying over* $\mathfrak{p}_M$*.*

Combining Lemma 118, Lemma 124 and Lemma 129 we have proved Thm 115. I.e. we have that $e(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(1+i)}) = 4$ and $f(N_{\mathfrak{p}_N}/\mathbb{Q}(i)_{(1+i)}) = 2$.

5.4.3. *The case $n = 4$:*

Proposition 130. *The* 4*-division points of*

$$E : y^2 = x^3 + x$$

are given by

$$\begin{aligned} E[4] &= \{O, (0,0), (\pm i, 0), (1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}), \\ &\quad (i(\sqrt{2}+1), \pm(1-i)(\sqrt{2}+1)), \\ &\quad (i(\sqrt{2}-1), \pm(1+i)(\sqrt{2}-1)), \\ &\quad (-i(\sqrt{2}-1), \pm(1-i)(\sqrt{2}-1)), \\ &\quad (-i(\sqrt{2}+1), \pm(1+i)(\sqrt{2}+1))\}. \end{aligned}$$

Proof. By Ex.105 the 4-division points (except O) are given by the zeros of

$$\psi_4 = 4y(x^6 + 5x^4 - 5x^2 - 1).$$

The points where $y = 0$ are the 2-division points $(0,0), (i,0), (-i,0)$. The zeros of $x^6 + 5x^4 - 5x^2 - 1$ can be computed by the substitution $x' = x^2$. We have

$$\begin{aligned} (x')^3 + 5(x')^2 - 5x' - 1 &= (x'-1)((x')^2 + 6x' + 1) \\ &= (x'-1)(x' + 3 + 2\sqrt{2})(x' + 3 - 2\sqrt{2}). \end{aligned}$$

So $x' \in \{1, -3+2\sqrt{2}, -3-2\sqrt{2}\}$ and hence $x \in \{\pm 1, \pm i(\sqrt{2}-1), \pm i(\sqrt{2}+1)\}$. Plugging those into the equation of E one gets the remaining points given in the proposition. □

Hence the field $K[4]$ is given by

$$K[4] = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8),$$

where $\zeta_8 = e^{\frac{\pi i}{4}}$.

Similar to Prop 112 we have the following proposition:

Proposition 131. *Let $\mathfrak{p} \neq (1+i)$ be a prime ideal in $\mathbb{Q}(i)$ and $\mathfrak{P}$ be an ideal in $K[4]$ lying over $\mathfrak{p}$. Then the extension $K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{\mathfrak{p}}$ is unramified.*

Proof. By the theorem of Néron-Ogg-Shavarevich (Thm. 108) the primes $\mathfrak{p}$ that can ramify are only those with bad reduction and those for which $\kappa_{\mathfrak{p}}$ divides $n = 4$. Since E only has bad reduction at $\mathfrak{p} = (1+i)$ (see Ex. 109) and $char(\kappa_{\mathfrak{p}}) = 2$ only if $\mathfrak{p} = (1+i)$ the extension is unramified in all other cases. □

Theorem 132. *The extension $K[4]/\mathbb{Q}(i)$ is ramified at $(1+i)$:*

$$e(K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{(1+i)}) = 2$$

and

$$f(K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{(1+i)}) = 1$$

for the prime ideal $\mathfrak{P} = (1+i, \zeta_8 - 1)$ in $K[4]$.

Proof. By Lemma 116 we have

$$O_{K[4]} = \mathbb{Z}[\zeta_8] = \mathbb{Z}[i][\zeta_8]$$

and the minimal polynomial of ζ_8 in $\mathbb{Z}[i]$ is given by

$$mipo(\zeta_8, \mathbb{Q}(i)) = T^2 - i.$$

After reducing it modulo $(1+i)$ we get

$$res(mipo(\zeta_8, \mathbb{Q}(i)), (1+i)) = T^2 - 1 = (T-1)^2.$$

So by Kummer's theorem (Thm. 114) there is a prime $\mathfrak{P} = (1+i, \zeta_8 - 1)$ such that $\mathfrak{P}^2 = (1+i)$ i.e. $(1+i)$ is ramified in $K[4]$ and we have $e(K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{(1+i)}) = 2$ and $f(K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{(1+i)}) = 1$. □

So $\mathfrak{p} = (1+i)$ is totally ramified in $K[4]$ and all other primes are unramified.

5.5. **Lubin-Tate prime elements.** Now that we have computed the ramifications of $K[n]$ for $n = 3, 4$ we can localize at their ramified prime ideals. We will then compute corresponding Lubin-Tate prime elements or prove that they do not exist.

5.5.1. *The case $n = 3$ and $\mathfrak{p} = (1+i)$.*

Theorem 133. *Let $\tilde{N}/\tilde{K}$ be the field extension $K[3]_{\mathfrak{p}_{K[3]}}/\mathbb{Q}(i)_{(1+i)}$. Then there is no prime π in $O_{\tilde{K}}$ such that*

$$N_{\tilde{N}/\tilde{K}}(\tilde{N}) = \langle \pi^f \rangle \times U^{(n)}$$

for any $f, n \in \mathbb{N}$.

Proof. The field $\tilde{L} = L_{(1+i)}$ (where $L = \mathbb{Q}(\zeta)$ as in Lemma 117) is unramified of degree 2 over $\tilde{K}$ (see Lemma 118) and hence (cf. Thm. 60)

$$N_{\tilde{L}/\tilde{K}}(\tilde{L}^*) = \langle \pi^2 \rangle \times U$$

for an arbitrary prime $\pi \in O_{\tilde{K}}$. By Thm. 59 and since $\tilde{N}/\tilde{L}$ is totally ramified of degree 4 (see Thm. 115) we know that $N_{\tilde{N}/\tilde{K}}(\tilde{N}^*)$ is a subgroup of $\langle \pi^2 \rangle \times U$ of index 4. So if $N_{\tilde{N}/\tilde{K}}(\tilde{N}^*)$ is of the form

$$N_{\tilde{N}/\tilde{K}}(\tilde{N}^*) = \langle \pi^2 \rangle \times U^{(n)}$$

for some prime $\pi \in O_{\tilde{K}}$ and $n \in \mathbb{N}$ we would have $n = 3$, since $[U^{(k)} : U^{(k+1)}] = 2$ (cf. Prop. 50).

Now let ν be the normalized valuation on $\tilde{N}$. The prime ideals $\mathfrak{p}_{\tilde{K}} = \mathfrak{p}_{\tilde{L}} = (1+i)$, $\mathfrak{p}_{\tilde{M}} = (1+i, \theta_M - \zeta^2)$and $\mathfrak{p}_{\tilde{N}} = (1+i, \theta_M - \zeta^2, \theta_N)$ (cf. Lemma 118, 124 and 129) are related by

$$\mathfrak{p}_{\tilde{K}} = \mathfrak{p}_{\tilde{L}} = \mathfrak{p}_{\tilde{M}}^2 = \mathfrak{p}_{\tilde{N}}^4.$$

Hence $\nu(1+i) = 4$, $\nu(\theta_M - \zeta^2) = 2$ and $\nu(\theta_N) = 1$. So θ_N is a prime element in $\tilde{N}$ and we compute the norm of this element $\theta_N \in \tilde{N}$:[20]

$$\begin{aligned}
N_{\tilde{N}/\tilde{K}}(\theta_N) &= N_{N/K}(\theta_N) \\
&= N_{M/K}((4+6\zeta+3\zeta^2-\zeta^3)+\theta_M(-3+5\zeta^2+5\zeta^3)) \\
&= N_{L/K}((4+6\zeta+3\zeta^2-\zeta^3)^2 + \\
&\quad (4+6\zeta+3\zeta^2-\zeta^3)(-3+5\zeta^2+5\zeta^3)Tr_{M/L}(\theta_M) + \\
&\quad (-3+5\zeta^2+5\zeta^3)^2 N_{M/L}(\theta_M)) \\
&= N_{L/K}((4+6\zeta+3\zeta^2-\zeta^3)^2 + \\
&\quad (4+6\zeta+3\zeta^2-\zeta^3)(-3+5\zeta^2+5\zeta^3)(1+\zeta+\zeta^2) + \\
&\quad (-3+5\zeta^2+5\zeta^3)^2(-2-\zeta+2\zeta^2+2\zeta^3))
\end{aligned}$$

[20] Here we use Lemma 127, Lemma 122 and the function NormalPoly (see the Appendix).

$$\begin{aligned} &= N_{L/K}(19+22\zeta-11\zeta^3) \\ &= (19+22\zeta-11\zeta^3)(19+22\zeta^5-11\zeta^3) \\ &= -2. \end{aligned}$$

Now suppose $N_{\tilde{N}/\tilde{K}}(\tilde{N}^*) = \langle \pi^2 \rangle \times U^{(3)}$. Then $-2 \in \langle \pi^2 \rangle \times U^{(3)}$, hence, $-2 = \pi^2 u$ for some $u \in U^{(3)}$ and so $-\frac{\pi^2}{2} = u^{-1} \in U^{(3)}$. Since $\pi \in (1+i)\backslash(1+i)^2$ we have $\pi = a+bi$ with $a, b \in \mathbb{Z}_2$ and $a \equiv b \equiv 1 \mod 2$. Since $u^{-1} \equiv 1 \mod (1+i)^3$ we obtain

$$\begin{aligned} -\frac{\pi^2}{2} &= -\frac{a^2-b^2+2abi}{2} \\ &= -\frac{a^2-b^2}{2} - abi \equiv 1 \mod (1+i)^3. \end{aligned}$$

On the other hand

$$-\frac{a^2-b^2}{2} - abi \equiv -i \mod (2)$$

and since $-i \equiv 1 \mod (2)$ would imply that $1+i \equiv 0 \mod (2)$ we get

$$-\frac{\pi^2}{2} \not\equiv 1 \mod (2)$$

and so

$$-\frac{\pi^2}{2} \not\equiv 1 \mod (1+i)^3$$

which is a contradiction.[21] □

The theorem above suggests that there is no real connection between division points of elliptic curves and division points of Lubin-Tate modules apart from the fact that both generate abelian extensions.

5.5.2. *The case $n = 3$ and $\mathfrak{p} = (3)$.*

Theorem 134. *The field extension $\hat{N}/\hat{K} := K[3]_{\mathfrak{p}_{K[3]}}/\mathbb{Q}(i)_{(3)}$ is totally and tamely ramified with degree 8. Its norm group is given by*

$$N_{\hat{N}/\hat{K}}(\hat{N}^*) = \langle \pi \rangle \times U^{(1)},$$

where $\pi = -3$ is prime in $O_{\hat{K}}$.

Proof. Because of Thm. 113 the field extension $\hat{N}/\hat{K}$ is totally ramified and has degree 8. Therefore it is also tamely ramified.

[21] Note that this proof did not show that there is no prime π such that $N_{\tilde{N}/\tilde{K}}(\tilde{N})\langle \pi^f \rangle \times U^{'}$ for some $f \in \mathbb{N}$ and some subgroup $U^{'}$ of U. The question whether this is the case remains open in this proof.

Let $v \in N$ be as in Lemma 125. Then by Lemma 125(v) the minimal polynomial of v over $\mathbb{Q}$ is given by

$$mipo(v, \mathbb{Q}) = T^8 - 6T^4 - 3.$$

Since 3 is prime in $\hat{K}$ this is also an Eisenstein polynomial over $\hat{K}$ and therefor irreducible. Hence

$$8 \leq [\hat{K}(v) : \hat{K}] \leq [\hat{N} : \hat{K}] = 8$$

and so

$$\hat{N} = \hat{K}(v).$$

Now let $\pi = -3$, which is a prime in $\hat{K}$, and F be the uniquely determined Lubin-Tate module such that $[\pi]_F = T \cdot mipo(v, \hat{K}) = T^9 - 6T^5 - 3T$ (which exists by Thm. 69). Then for the corresponding Lubin-Tate extension L_1 of degree 1 we get

$$\begin{aligned} L_1 &= \hat{K}(F(1)) \\ &= \hat{K}(ker([\pi]_F)) \\ &\supseteq \hat{K}(v) = \hat{N}. \end{aligned}$$

Since $[L_1 : \hat{K}] = |U : U^{(1)}| = 8$ we get

$$L_1 = \hat{N}.$$

□

Hence the field $K[3]_{(3)}$ generated by the 3-division points is a Lubin-Tate extension of $\mathbb{Q}(i)_{(3)}$.

5.5.3. *The case $n = 4$ and $\mathfrak{p} = (1 + i)$.*

Theorem 135. *The field extension $\tilde{E}/\tilde{K} := K[4]_{\mathfrak{P}}/\mathbb{Q}(i)_{(1+i)}$ is wildly ramified with degree 2. Additionally there is no prime π in $O_{\tilde{K}}$ such that*

$$N_{\tilde{E}/\tilde{K}}(\tilde{E}^*) = \langle \pi^f \rangle \times U^{(n)}$$

for any $f, n \in \mathbb{N}$.

Proof. By Thm. 132 the field extension $\tilde{E}/\tilde{K}$ is totally ramified with degree 2 and therefore is wildly ramified.

If now $N_{\tilde{E}/\tilde{K}}(\tilde{E}^*)$ was of the form

$$\langle \pi^f \rangle \times U^{(n)}$$

for some $f, n \in \mathbb{N}$ then $f = 1$ and $n = 2$ (cf. Thm. 60).

But we have

$$N_{\tilde{E}/\tilde{K}}(\zeta_8) = \zeta_8 \zeta_8^5 = -i \notin U^{(2)}$$

which contradicts the above.[22] □

[22] As in the proof of Thm. 133 we did not show that there is no prime π such that $N_{\tilde{N}/\tilde{K}}(\tilde{N})\langle \pi^f \rangle \times U^{'}$ for some $f \in \mathbb{N}$ and some subgroup $U^{'}$ of U.

6. Summary and conclusion

This chapter should give a short summary and an interpretation of the results of chapter 5.

6.1. **Summary of the results.**

We adjoined 3- and 4-division points of the elliptic curve

$$y^2 = x^3 + x$$

to the field $\mathbb{Q}(i)$ to get abelian extensions of $\mathbb{Q}(i)$ given by

$$K[3] = \mathbb{Q}(i)(\alpha, \beta)$$

with

$$\alpha = \sqrt{\frac{2}{\sqrt{3}} - 1}, \beta = \sqrt{\frac{2}{\sqrt{3}}\alpha}$$

and

$$K[4] = \mathbb{Q}(i)(\sqrt{2}) = \mathbb{Q}(\zeta_8).$$

6.1.1. *The case* $n = 3$*:*

We described the field $K[3]$ with the following tower of field extensions and their corresponding rings of integers:

$$\begin{array}{cc}
K[3] = N = M(\beta) & O_N = O_M[\theta_N] \\
| & | \\
M = L(\alpha) & O_M = O_L[\theta_M] \\
| & | \\
L = \mathbb{Q}(\zeta) & O_L = \mathbb{Z}[\zeta] \\
| & | \\
\mathbb{Q}(i) & \mathbb{Z}[i] \\
\begin{pmatrix} | \\ \mathbb{Q} \end{pmatrix} & \begin{pmatrix} | \\ \mathbb{Z} \end{pmatrix}
\end{array}$$

Then we determined the ramification of the extension $K[3]/\mathbb{Q}(i)$.

The case $n = 3$*,* $\mathfrak{p} = (1 + i)$. Here we got the following picture:

$$\begin{array}{ccc}
N = M(\beta) & \mathfrak{p}_{N,2} = (1+i, \theta_M - \zeta^2, \theta_N) & \\
| & | & e(N_{\mathfrak{p}_{N,2}}/M_{\mathfrak{p}_{M,2}}) = 2 \\
M = L(\alpha) & \mathfrak{p}_{M,2} = (1+i, \theta_M - \zeta^2) & \\
| & | & e(M_{\mathfrak{p}_{M,2}}/L_{(1+i)}) = 2 \\
L = \mathbb{Q}(\zeta) & (1+i) & \\
| & | & f(L_{(1+i)}/\mathbb{Q}(i)_{(1+i)}) = 2 \\
\mathbb{Q}(i) & (1+i) & \\
\left(\begin{array}{c} | \\ \mathbb{Q} \end{array}\right) & \begin{array}{c} | \\ 2 \end{array} & e(\mathbb{Q}(i)_{(1+i)}/\mathbb{Q}_2) = 2
\end{array}$$

and we determined that for the localized extension $\tilde{N}/\tilde{K} = K[3]_{\mathfrak{p}_{K[3],2}}/\mathbb{Q}(i)_{(1+i)}$ there is no prime $\pi \in O_{\tilde{K}}$ such that

$$N_{\tilde{N}/\tilde{K}}(\tilde{N}) = \langle \pi^f \rangle \times U^{(n)}$$

for any $f, n \in \mathbb{N}$ and $U^{(n)} = \{x \in O_{\tilde{K}} : x \equiv 1 \mod (1+i)^n\}$.

The case $n = 3$, $\mathfrak{p} = (3)$. Here we got:

$$\begin{array}{ccc}
N = M(\beta) & \mathfrak{p}_{N,3} & \\
| & | & e(N_{\mathfrak{p}_{N,3}}/M_{\mathfrak{p}_{M,3}}) = 2 \\
M = L(\alpha) & \mathfrak{p}_{M,3} & \\
| & | & e(M_{\mathfrak{p}_{M,3}}/L_{\mathfrak{p}_{L,3}}) = 2 \\
L = \mathbb{Q}(\zeta) & \mathfrak{p}_{L,3} & \\
| & | & e(L_{\mathfrak{p}_{L,3}}/\mathbb{Q}(i)_{(3)}) = 2 \\
\mathbb{Q}(i) & (3) & \\
\left(\begin{array}{c} | \\ \mathbb{Q} \end{array}\right) & \begin{array}{c} | \\ 3 \end{array} & f(\mathbb{Q}(i)_{(3)}/\mathbb{Q}_3) = 2
\end{array}$$

Additionally we had that $N_{\mathfrak{p}_{N,3}}$ is the Lubin-Tate extension L_1 of $\mathbb{Q}(i)_{(3)}$ w.r.t. $\pi = -3 \in \mathbb{Q}(i)_{(3)}$.

The case $n = 3$, $\mathfrak{p} \neq (1+i), (3)$. Here the criterion of Néron-Ogg-Shafarevic told us that the extension $K[3]/\mathbb{Q}(i)$ is always unramified at $\mathfrak{p}$.

6.1.2. *The case* $n = 4$. This case was much easier because the rings of integer were easy to determine and there is only one ramified prime ideal:

$$\begin{array}{cc} K[4]=\mathbb{Q}(\zeta_8) & O_{K[4]}=\mathbb{Z}[\zeta_8] \\ | & | \\ \mathbb{Q}(i) & \mathbb{Z}[i] \\ \left(\begin{array}{c} | \\ \mathbb{Q} \end{array}\right) & \left(\begin{array}{c} | \\ \mathbb{Z} \end{array}\right) \end{array}$$

The case $n = 4$, $\mathfrak{p} = (1 + i)$. At $\mathfrak{p} = (1 + i)$ we got:

$$\begin{array}{ccc} K[4]=\mathbb{Q}(\zeta_8) & \mathfrak{p}_{K[4],2}=(1+i,\zeta_8-1) & \\ | & | & e(K[4]_{\mathfrak{p}_{K[4],2}}/\mathbb{Q}_2)=2 \\ \mathbb{Q}(i) & (1+i) & \\ \left(\begin{array}{c} | \\ \mathbb{Q} \end{array}\right) & \begin{array}{c} | \\ 2 \end{array} & e(\mathbb{Q}(i)_{(1+i)}/\mathbb{Q}_2)=2 \end{array}$$

Furthermore we found that for the localized extension $\tilde{E}/\tilde{K} = K[4]_{\mathfrak{p}}/\mathbb{Q}(i)_{(1+i)}$ there is no prime $\pi \in O_{\tilde{K}}$ such that

$$N_{\tilde{E}/\tilde{K}}(\tilde{E}^*) = \langle \pi \rangle \times U^{(n)}$$

for any $f, n \in \mathbb{N}$.

The case $n = 4$, $\mathfrak{p} \neq (1 + i)$. Again the criterion of Néron-Ogg-Shafarevic guaranteed that any other prime ideal $\mathfrak{p} \neq (1 + i)$ is unramified.

6.2. **Conclusion.** In summary these few examples do not indicate that there is an easy connection between division points of elliptic curves with complex multiplication and the division points of Lubin-Tate modules, apart from the fact that they both generate abelian extensions.

It would be nice to have a much larger "database" of results about the ramifications of primes in extensions obtained by elliptic curves with complex multiplication but it is not possible (at least not easily) to generalize the methods used here to obtain the necessary ramification data for n-division points with $n \geq 5$.

Appendix: Mathematica Listing

This appendix contains the Mathematica code I used to determine the generators of the abelian extensions computed in Chapter 5.4.2. It mostly contains functions that simplify calculations in the fields L and M defined in that chapter.

In fact most (simple) calculations in that chapter were made using these functions.

The only calculation that could not be done easily by hand however is the determination of the generators $\theta_M, \theta'_M, \theta''_M$ resp. $\theta_N, \theta'_N, \theta''_N$ of the rings of integers O_M resp. O_N used in Lemma 123 resp. Lemma 128.

Integralbasis.nb

written by Jakob Preininger

This notebook provides functions to work in the fields L and M and calculates integral bases for both O_M and O_N which are used in section 5.4.2

Functions to work in L

The following functions are written to work with the field L = Q(z), where z = zeta = e^(2 Pi*I/12) is the primitive 12 th root of unity, as Q - vectorspace in the basis B = {1, z, z^2, z^3}, which is also a Z - basis of the ring of integers of L.

PolyToList

In : a rational polynomial f in the variable z

Out : the list of coefficients of f

```
PolyToList[f_] := CoefficientList[f, z];
```

ListToPoly

In : a list l of rationals

Out : the polynomial with variable z with coefficients given in l

```
ListToPoly[l_] := Module[{erg = 0, i},
   For[i = 0, i < Length[l], i++,
    erg += l[[i + 1]] z^i;];
   erg
  ];
```

PowerList

In : a natural number n

Out : the list of powers of z = e^(2 Pi*I/12) in the basis B with size n

```
PowerList[n_] :=
  Module[{erg = {}, i},
   For[i = 0, i < n, i++,
    Switch[Mod[i, 12],
      0, AppendTo[erg, 1],
      1, AppendTo[erg, z],
      2, AppendTo[erg, z^2],
      3, AppendTo[erg, z^3],
      4, AppendTo[erg, z^2 - 1],
      5, AppendTo[erg, z^3 - z],
      6, AppendTo[erg, -1],
      7, AppendTo[erg, -z],
      8, AppendTo[erg, -z^2],
      9, AppendTo[erg, -z^3],
      10, AppendTo[erg, 1 - z^2],
      11, AppendTo[erg, z - z^3]];
   ];
   erg
  ];
```

NormalListToPoly

In : a list l of rationals

Out : the evaluation of the polynomial with coefficients l in z written in the basis B

```
NormalListToPoly[l_] :=
  l.PowerList[Length[l]];
```

NormalList

In : a list l of rationals

Out : the evaluation of the polynomial with coefficients l in z written as a coefficient list in the basis B

```
NormalList[l_] :=
  Module[{i, erg = PolyToList[NormalListToPoly[l]]},
   For[i = Length[erg], i < 4, i++, AppendTo[erg, 0];];
   erg
  ];
```

NormalPoly

In : a rational polynomial f in the variable z

Out : the evaluation of the polynomial f in z written in the basis B

```
NormalPoly[f_] :=
  NormalListToPoly[PolyToList[f]];
```

NormalPolyToList

In : a rational polynomial f in the variable z

Out : the evaluation of the polynomial f in z written as coefficient list in the basis B

```
NormalPolyToList[f_] :=
  NormalList[PolyToList[f]];
```

InvertPoly

In: A rational polynomial poly in z.

Out: The inverse of poly in L

```
InvertPoly[poly_] :=
  Module[{sol},
   sol = Solve[
     NormalPolyToList[poly (a + b z + c z^2 + d z^3)] == NormalPolyToList[1], {a, b, c, d}];
   First[a + b z + c z^2 + d z^3 /. sol]
  ];
```

A

In: rational numbers a, b, c, d

Out: the polynomial a+bz+cz^2+dz^3 in z.

```
A[a_, b_, c_, d_] := a + b z + c z^2 + d z^3;
```

B

In : rational numbers e, f, g, h

Out : the polynomial e + fz + gz^2 + hz^3 in z.

```
B[e_, f_, g_, h_] := e + f z + g z^2 + h z^3;
```

Q

In : rational numbers a, b, c, d, e, f, g, h and a rational polynomial qw in z (an element in L)

Out : the constant coefficient in the minimal polynomial of an element (a + bz + cz^2 + dz^3) + q (e + fz + gz^2 + hz^3) in M = L(q), where q^2 = qw

```
Q[a_, b_, c_, d_, e_, f_, g_, h_, qw_] :=
  NormalPolyToList[A[a, b, c, d]^2 - qw B[e, f, g, h]^2];
```

FindInteger

In : a rational polynomial qw in z (an element in L)

Out : the list of all integral elements in M = L(w) mod Z[z, w], where w^2 = qw written as 8 - tupels {a, b, c, d, e, f, g, h} that one has to read as: a + bz + cz^2 + dz^3 + w(e + fz + gz^2 + hz^3)

```
FindInteger[qw_] :=
  Module[{a, b, c, d, e, f, g, h, z, erg = {}},
   For[a = 0, a < 1, a += 1 / 2,
    For[b = 0, b < 1, b += 1 / 2,
      For[c = 0, c < 1, c += 1 / 2,
        For[d = 0, d < 1, d += 1 / 2,
          For[e = 0, e < 1, e += 1 / 2,
            For[f = 0, f < 1, f += 1 / 2,
              For[g = 0, g < 1, g += 1 / 2,
                For[h = 0, h < 1, h += 1 / 2,
                  If[Mod[Q[a, b, c, d, e, f, g, h, qw], 1] == {0, 0, 0, 0},
                    AppendTo[erg, {a, b, c, d, e, f, g, h}]];
                ];
              ];
            ];
          ];
        ];
      ];
    ];
   ];
   erg
  ];
```

Functions in M

The following functions are written to work with the field M = Q(z,t), where z = e^(2 Pi*I/12) is the primitive 12 th root of unity and t = theta_M, as Q-vectorspace in the basis C = {1, z, z^2, z^3, t, tz, tz^2, tz^3}, which is also a Z - basis of the ring of integers of M (see section 5.4.2)

TPolyToList

In : a polynomial f in the variables t, z

Out : the list of coefficients of f

```
TPolyToList[f_] := CoefficientList[f, {t, z}];
```

TListToPoly

In : a list l of lists of rationals

Out : the polynomial with variables t, z with coefficients given in l

```
TListToPoly[l_] := Module[{erg = 0, i, j},
   For[i = 0, i < Length[l], i++,
    For[j = 0, j < Length[l[[i + 1]]], j++,
      erg += l[[i + 1]][[j + 1]] t^i z^j;
     ];
   ];
   erg
  ];
```

TPowerList

In : a natural number n

Out : the list of powers of t of length n written in the basis C

```
TPowerList[n_] :=
  Module[{erg = {}, i},
   For[i = 0, i < n, i++,
    If[i ≥ 2, AppendTo[erg, ((2 + z - 2 z^2 - 2 z^3) + t (1 + z + z^2)) t^(i - 2)],
      If [i == 1, AppendTo[erg, t], AppendTo[erg, 1];];];
   ];
   erg
  ];
```

TReduce

In : a rational polynomial f in the variables t, z

Out : the polynomial f evaluated in t and z written as a polynomial that is linear in t (but not yet normalized in z)

```
TReduce[f_] :=
  Module[{erg = f, l},
   For[l = Length[CoefficientList[f, t]], l > 2, l--,
    erg = TPowerList[l].CoefficientList[erg, t];
   ];
   erg
  ];
```

TNormalPolyToList

In : a rational polynomial f in the variables t, z

Out : the polynomial f evaluated in t and z written as a list in the form {{a, b, c, d}, {e, f, g, h}} = (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3)

```
TNormalPolyToList[f_] :=
  Module[{erg = {}, zw = TPolyToList[TReduce[f]], i},
   For[i = 0, i < 2, i++,
    If[Length[zw] ≤ i, AppendTo[zw, {}]];
    AppendTo[erg, NormalList[zw[[i + 1]]]];
   ];
   erg
  ];
```

TNormalList

In : a list l of lists of rationals

Out : the polynomial with coefficients in l evaluated in t and z written as a list in the form {{a, b, c, d}, {e, f, g, h}} = (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3)

```
TNormalList[l_] :=
  TNormalPolyToList[TListToPoly[l]];
```

TNormalPoly

In : a rational polynomial f in the variables t, z

Out : the polynomial f evaluated in t and z in the form (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3)

```
TNormalPoly[f_] :=
  TListToPoly[TNormalPolyToList[f]];
```

TNormalListToPoly

In : a list l of lists of rationals

Out : the polynomial with coefficients in l evaluated in t and z written as a list in the form {{a, b, c, d}, {e, f, g, h}} = (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3)

```
TNormalListToPoly[l_] :=
  TListToPoly[TNormalList[l]];
```

TInvertPoly

In : A rational polynomial poly in z and t.

Out : The inverse of poly in M

```
TInvertPoly[poly_] :=
 Module[{sol},
  sol = Solve[TNormalPolyToList[poly ((a + b z + c z^2 + d z^3) + t (e + f z + g z^2 + h z^3))] ==
     TNormalPolyToList[1], {a, b, c, d, e, f, g, h}];
  First[(a + b z + c z^2 + d z^3) + t (e + f z + g z^2 + h z^3) /. sol]
 ]
```

TA

In: rational numbers a, b, c, ..., h

Out: The polynomial (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3) in z and t.

```
TA[a_, b_, c_, d_, e_, f_, g_, h_] := a + b z + c z^2 + d z^3 + t (e + f z + g z^2 + h z^3);
```

TB

In: rational numbers i, j, k, ..., p

Out: The polynomial (i + jz + kz^2 + lz^3) + t(m + nz + oz^2 + pz^3) in z and t.

```
TB[i_, j_, k_, l_, m_, n_, o_, p_] := i + j z + k z^2 + l z^3 + t (m + n z + o z^2 + p z^3);
```

TQ

In : rational numbers a, b, c, ..., p and a rational polynomial qv in t and z (an element in M)

Out : the constant coefficient in the minimal polynomial of an element (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3) + v((i + jz + kz^2 + lz^3) + t(m + nz + oz^2 + pz^3)) in N = M(v), where v^2 = qv

```
TQ[a_, b_, c_, d_, e_, f_, g_, h_, i_, j_, k_, l_, m_, n_, o_, p_, qv_] :=
  TNormalPolyToList[TA[a, b, c, d, e, f, g, h]^2 - qv TB[i, j, k, l, m, n, o, p]^2];
```

FindInteger

In : a rational polynomial qv in t and z (an element in M)

Out : the list of all integral elements in N = M (v) mod Z[z, t, v], where v^2 = qv written as 16 - tupels {a, b, c, ..., p} = (a + bz + cz^2 + dz^3) + t(e + fz + gz^2 + hz^3) + v((i + jz + kz^2 + lz^3) + t (m + nz + oz^2 + pz^3))

```
TFindInteger[qv_] :=
  Module[{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, erg = {}},
   For[a = 0, a < 1, a += 1 / 2,
    For[b = 0, b < 1, b += 1 / 2,
      For[c = 0, c < 1, c += 1 / 2,
        For[d = 0, d < 1, d += 1 / 2,
          For[e = 0, e < 1, e += 1 / 2,
            For[f = 0, f < 1, f += 1 / 2,
              For[g = 0, g < 1, g += 1 / 2,
                For[h = 0, h < 1, h += 1 / 2,
                  For[i = 0, i < 1, i += 1 / 2,
                    For[j = 0, j < 1, j += 1 / 2,
                      For[k = 0, k < 1, k += 1 / 2,
                        For[l = 0, l < 1, l += 1 / 2,
                          For[m = 0, m < 1, m += 1 / 2,
                            For[n = 0, n < 1, n += 1 / 2,
                              For[o = 0, o < 1, o += 1 / 2,
                                For[p = 0, p < 1, p += 1 / 2,
                                  If[Mod[TQ[a, b, c, d, e, f, g, h, i, j, k, l, m, n, o,
                                        p, qv], 1] == {{0, 0, 0, 0}, {0, 0, 0, 0}},
                                    AppendTo[erg, {a, b, c, d, e, f, g,
                                      h, i, j, k, l, m, n, o, p}]];
                                 ];
                               ];
                             ];
                           ];
                         ];
                       ];
                     ];
                   ];
                 ];
               ];
             ];
           ];
         ];
       ];
     ];
   ];
   erg
  ];
```

The results

In Lemma 121 we need to find integral elements of M mod O_L[w]. Since w^2=1-2z^2 the following function gives the solutions:

```
FindInteger[1 - 2 z^2]
```

```
                                           1  1  1     1  1  1
{{0, 0, 0, 0, 0, 0, 0, 0}, {0, -, -, -, 0, -, -, -},
                                           2  2  2     2  2  2
   1           1  1           1     1  1  1     1  1  1
 {-, 0, 0, -, -, 0, 0, -}, {-, -, -, 0, -, -, -, 0}}
   2           2  2           2     2  2  2     2  2  2
```

So theta_M = 1/2(1 + z + z^2)(1+w), theta_M' =1/2(z+z^2+z^3)(1+w) and theta_M"=1/2(1+z^3)(1+w).

In Lemma 122 we compute the norm of theta_M in L:

```
Expand[NormalPoly[1 / 4 (1 + z + z^2) ^2 2 z^2]]
```

$$-2-z+2\,z^2+2\,z^3$$

So N_M/L(theta_M) = -2-z+2z^2+2z^3.

In Lemma 123 we need to invert 1+z+z^2:

```
InvertPoly[1 + z + z^2]
```

$$1-\frac{z}{2}-\frac{z^2}{2}+\frac{z^3}{2}$$

So 2/(1+z+z^2)=2-z-z^2+z^3.

In Lemma 124 we compute 1/4(-1+2z-z^3)(1+z^3)^5((2-z-z^2+z^3)t-1):

```
TNormalPoly[1 / 4 (-1 + 2 z - z^3) (1 + z^3) ^5 ((2 - z - z^2 + z^3) t - 1)]
```

$$-2+4\,t+2\,z-2\,t\,z+2\,z^2-6\,t\,z^2-2\,z^3+6\,t\,z^3$$

So 1/4(-1+2z-z^3)(1+z^3)^5((2-z-z^2+z^3)t-1) = (-2+2z+2z^2-2z^3)+t(4-2z-6z^2+6z^3).

In Lemma 125 we need to simplify -z^3/2((-2+2z+2z^2-2z^3)+t(4-2z-6z^2+6z^3):

```
TNormalPoly[-z^3 / 2 ((-2 + 2 z + 2 z^2 - 2 z^3) + t (4 - 2 z - 6 z^2 + 6 z^3))]
```

$$2\,t+z-3\,t\,z-z^2+t\,z^2+t\,z^3$$

So -z^3/2((-2+2z+2z^2-2z^3)+t(4-2z-6z^2+6z^3) = (z-z^2)+t(2-3z+z^2+z^3).

In Lemma 126 we need to find integral elements of N mod O_M[v]. Since v^2=(z-z^2)+t(2-3z+z^2+z^3) the following function gives the solutions:

```
TFindInteger[z - z^2 + t (2 - 3 z + z^2 + z^3)]
```

$$\Big\{\{0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0\},$$
$$\Big\{0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0,0,\tfrac{1}{2},0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0,0,\tfrac{1}{2}\Big\},$$
$$\Big\{\tfrac{1}{2},0,0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0,\tfrac{1}{2},0,0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0\Big\},$$
$$\Big\{\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0,0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0,0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2}\Big\}\Big\}$$

So theta_N = 1/2((1 + z + z^2)+t(z+z^2+z^3))(1+v), theta_N' =1/2((z+z^2+z^3)+t(1+z^3))(1+v) and theta_N''=1/2((1+z^3)+t(1+z+z^2))(1+v).

In Lemma 127 we need to compute the norm of theta_N in M:

```
TNormalPoly[1 / 4 ((1 + z + z^2) + t (z + z^2 + z^3)) ^2 ((1 - z + z^2) + t (-2 + 3 z - z^2 - z^3))]
```

$$4-3\,t+6\,z+3\,z^2+5\,t\,z^2-z^3+5\,t\,z^3$$

So N_N/M(theta_N) = (4+6z+3z^2-z^3)+t(-3+5z^2+5z^3)

In Lemma 128 we need to invert (1+z+z^2)+t(z+z^2+z^3):

```
TInvertPoly[(1 + z + z^2) + t (z + z^2 + z^3)]
```

$$1-z-\frac{z^2}{2}+\frac{z^3}{2}+t\left(-\frac{z}{2}+z^2-\frac{z^3}{2}\right)$$

So 2/((1+z+z^2)+t(z+z^2+z^3)) = (2-2z-z^2+z^3)+t(-z+2z^2-z^3).

In Theorem 133 we need to compute the Norm of theta_N in the extension N/K:

```
Simplify[
 NormalPoly[(4 + 6 z + 3 z^2 - z^3) ^2 + (4 + 6 z + 3 z^2 - z^3) (-3 + 5 z^2 + 5 z^3) (1 + z + z^2) +
   (-3 + 5 z^2 + 5 z^3) ^2 (-2 - z + 2 z^2 + 2 z^3)]]
```

$19 + 22\,z - 11\,z^3$

```
Simplify[NormalPoly[(19 + 22 z - 11 z^3) (19 + 22 z^5 - 11 z^3)]]
```

```
-2
```

So N_N/K(theta_N) = -2.

References

[1] CASSELS J.W.S., FRÖHLICH A.: Algebraic Number Theory. Academic Press, London 1967

[2] CHILDRESS N.: Class Field Theory. Springer, New York 2009

[3] COX D., LITTLE J., O'SHEA D.: Ideals Varieties and Algorithms. Springer, New York, 2nd Ed. 1997

[4] HUSEMÖLLER D.: Elliptic Curves. Springer, New York, 2nd Ed. 2004

[5] LORENZ F.: Einführung in die Algebra II, Spektrum Akad. Verlag, Heidelberg-Berlin-Oxford, 2te Aufl. 1997

[6] MILNE J.: Algebraic Number Theory. http://www.jmilne.org/math/CourseNotes/ANT.pdf, v.3.05 2013

[7] NEUKIRCH J.: Algebraische Zahlentheorie. Springer, Berlin-Heidelberg-New York 1992

[8] SERRE J.P.: Local Fields. Springer, New York 1979

[9] SILVERMAN J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer, New York 1994

[10] SILVERMAN J.H.: The Arithmetic of Elliptic Curves. Springer, New York, 2nd Ed. 2009

[11] SILVERMAN J.H., TATE J.: Rational Points on Elliptic Curves. Springer, New York 1992

Abstract

The aim of this thesis is to compare the theory of Lubin-Tate modules, which describe ramified abelian extensions of local fields, to the theory of elliptic curves with complex multiplication, which also can be used to generate abelian extensions of imaginary quadratic fields, and thereby establish a more explicit understanding of class field theory.

After a short introduction in Chapter one we start with a brief review of the theory of local fields in Chapter two. We define the notion of an absolute value on a field and of a completion of a field with respect to such an absolute value. Additionally we introduce residue class degree and ramification index on such fields and state some of their basic properties. Then we define local fields and present some some results about the solvabilty of Galois extensions of local fields and the structure of the multiplicative group of such fields.

In Chapter three we give a short summary of local class field theory. In particular we deal with the local reciprocity law and the existence theorem, which give a one-to-one correspondence between finite abelian extensions of a local field K and the open subgroups of finite index in the group K^*. Furthermore we introduce formal groups and the theory of Lubin-Tate modules.

Chapter four is dedicated to the theory of elliptic curves and its structure as abelian groups which leads to the notion of complex multiplication.

In Chapter five, the main part of this thesis, we pick the elliptic curve $y^2 = x^3+x$, which has complex multiplication, and compute its division points. Then we use these division points to generate abelian extensions of $\mathbb{Q}(i)$ and the criterion of Néron-Ogg-Shafarevic to determine which primes of $\mathbb{Q}(i)$ possibly ramify in these extensions and compute the corresponding ramification indices and residue class degrees, which we use to determine whether the localized extensions are Lubin-Tate extensions.

Finally Chapter six summarizes the results from Chapter five. The Appendix contains the Mathematica code used to do some computations in Chapter five.

Zusammenfassung

Ziel dieser Arbeit ist es die Theorie der Lubin-Tate Moduln, die verzweigte abelsche Erweiterungen lokaler Körper untersucht, mit der Theorie der elliptischen Kurven mit komplexer Multiplikation, die ebenfalls zur Erzeugung abelscher Erweiterungen von imaginär-quadratischen Zahlkörpern verwendet werden kann, zu vergleichen und dabei ein explizitäres Verständnis für Klassenkörpertheorie zu erhalten.

Nach einer kurzen Einleitung in Kapitel eins beginnen wir in Kapitel zwei mit einer kurzen Wiederholung der Theorie lokaler Körper. Wir definieren den Begriff eines Absolutbetrages auf einem Körper und einer Vervollständigung eines Körpers bezüglich eines solchen Betrages. Weiters führen wir Restklassengrad und Verzweigungsindex auf derartigen Körpern ein und stellen einige ihrer wichtigen Eigenschaften fest. Danach definieren wir lokale Körper und präsentieren einige Resultate über die Auflösbarkeit von Galoiserweiterungen lokaler Körper und die Struktur der multiplikativen Gruppe solcher Körper.

In Kapitel drei geben wir eine Zusammenfassung lokaler Klassenkörpertheorie. Im speziellen beschäftigen wir uns mit dem lokalen Reziprozitätsgesetz und dem Existenzsatz, der uns eine bijektive Korrespondenz zwischen endlichen abelschen Erweiterungen eines lokalen Körpers K und den offenen Untergruppen endlichen Indexes der Gruppe K^*herstellt. Desweiteren führen wir den Begriff der formalen Gruppe und der daraus entstehenden Theorie der Lubin-Tate Moduln ein.

Kapitel vier beschäftigt sich mit der Theorie elliptischer Kurven, speziell mit der abelschen Gruppenstruktur auf diesen die uns zum Begriff der komplexen Multiplikation führt.

In Kapitel fünf, dem Hauptteil der Arbeit, wählen wir die elliptische Kurve $y^2 = x^3 + x$, die komplexe Multiplikation hat, und berechnen ihre Teilungspunkte. Dann nutzen wir diese Teilungspunkte um abelsche Erweiterungen von $\mathbb{Q}(i)$ zu konstruieren und das Kriterium von Néron-Ogg-Shafarevic um zu bestimmen welche Primideale von $\mathbb{Q}(i)$ in diesen Erweiterung verzweigt sein können. Danach berechnen wir Verzweigungsindizes und Restklassengrade dieser Primideale und bestimmen damit ob die bezüglich dieser Primideale lokalisierten Erweiterungen Lubin-Tate Erweiterungen.

Schließlich fassen wir in Kapitel sechs die Resultate aus Kapitel fünf zusammen. Desweiteren findet man im Anhang den Mathematica-Code der für einige Berechnungen in Kapitel fünf verwendet wurde.

Curriculum Vitae

Personal data:

Name:	Jakob Preininger BSc
Date of birth:	June 20, 1988
Place of birth:	Ried im Innkreis, Austria
Address:	Linzer Straße 460/1 A-1140 Wien
Citizenship:	Austria
E-mail:	preininger.jakob@gmx.at

Education:

2011 - 2013: MSc student at the Faculty of Mathematics at the University of Vienna
Master thesis: “Lubin-Tate extensions and divisions points on the elliptic curve $y^2 = x^3 + x$“ supervised by Joachim Mahnkopf

2011: BSc in mathematics with distinction
Bacherlor theses: “The ring of number-theoretic functions” and “Infinite Galois Theory” supervised by Leonhard Summerer

2007 - 2011: BSc student at the Faculty of Mathematics at the University of Vienna

2006 - 2007: Civil service

2006: Matura (school leaving exam)

1998 - 2006: BG/BRG Dr. Schauerstraße Wels, Austria

1994 - 1998: VS2 Grieskirchen, Austria

Scholarships:

Performance scholarships awarded by the University of Vienna for the academic years 2007-2008, 2008-2009 and 2010-2011

Extracurricular activities:

2012: Participation at the seminar: “Algorithms for Complex Multiplication over Finite Fields” in Oberwolfach (Germany)

2008 - 2011: Annual participation at the Vojtěch Jarník International Mathematical Competition (VJIMC) in Ostrava (Czech Republic)

2008 - 2010: Participation at the International Mathematics Competition (IMC)
in Blagoevgrad (Bulgaria, 2008 and 2010) and Budapest (Hungary, 2009)

2004 - 2006: Participation at the International Mathematical Olympiad (IMO)
in Athens (Greece, 2004), Mérida (Mexico, 2005) and Ljubljana (Slovenia, 2006)

2004 - 2006: Participation at the Austrian Mathematical Olympiad (ÖMO) (achieved 4th, 3rd and 2nd place)

Teaching activities:

2010 - 2012: Tutor at the Faculty of Mathematics at the University of Vienna for
“Analysis” (“Calculus”, 2009 - 2010),
“Lineare Algebra für PhysikerInnen” (“Linear algebra for physicists”, 2010 - 2011) and
“Hilfsmittel aus der EDV” (“Introduction to LaTeX and Mathematica”, 2011 - 2012)