rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Branched covering spaces of an elliptic curve that branch only above a single point.

Master's thesis in Mathematics

August 2011

Student: A.S.I. Anema

First supervisor: prof. dr. J. Top

Second supervisor: prof. dr. H. Waalkens

Contents

Chapter 1

Introduction

This master's thesis is about branched covering spaces of an elliptic curve. An elliptic curve is a curve of genus one with a special point. Moreover an elliptic curve has a group structure defined on it, where the special point is the unit of the group. Another way to consider an elliptic curve is as a Riemann surface. From a topological perspective the surface is homeomorphic to a torus.

In chapter 2 we give an overview of some topics from algebraic topology and Riemann surfaces. For example we introduce the concept of a covering spaces and show how to construct covering spaces. A topic from Riemann surfaces we discuss, is the analytic continuation of a covering space to a branched covering space. Finally we put these theories together and make a statement about branched covering spaces of a torus that branch only above a single point.

In chapter 3 we mention the various results from the theory of commutative algebra, algebraic geometry and elliptic curves. In particular we discuss concepts related to the ramification index. Using some of these results we construct an explicit example of a branched covering space of the type we are interested in. The other results lay the foundation on which the subsequent chapter is build.

In chapter 4 we set out to construct a family of branched covering spaces of the elliptic curve $C : 4a^3 + 27b^2 = 1$ by adjoining points of some finite order on another elliptic curve to the function field of C. We are interested in the ramification index at points on these spaces.

Chapter 2

Covering spaces

In this chapter we study the existence of branched covering spaces from a topological perspective. We give a short overview of covering spaces and fundamental groups in the first section. In the second section we discuss some results about Riemann surfaces. In the last section we address the existence of branched covering spaces of a torus. We shall assume that the topological spaces in this chapter are Haussdorff [1].

2.1 Covering spaces and fundamental groups

We give an overview of the theory of covering spaces and fundamental groups corresponding to a topological space. More background information on algebraic topology can be found in the books [1, 3, 7].

Definition 2.1. Let Y be a topological space. If X is a topological space and $p : X \to Y$ is a continuous map with an open covering $\mathcal{V}$ of Y such that for all $V \in \mathcal{V}$ there are disjoint open subsets $U_i \subset X$ such that $p^{-1}(V) = \bigcup U_i$ and $p|_{U_i} : U_i \to V$ a homeomorphism, then X is a *covering space* of Y with $p : X \to Y$ the corresponding *covering map.*

Definition 2.2. Let X be a covering space of some space Y with $p : X \to Y$ the corresponding covering map. If $f : X \to X$ is a homeomorphism such that $p \circ f = p$, then $f : X \to X$ is a *deck transformation.* Write $\mathrm{Deck}(X/Y)$ for the set of all deck transformations.

The set of deck transformations is a group with the composition of maps being the group operation. This group is a special case of a group action on a topological space.

Definition 2.3. Let X be a topological space and G a group. An *action* of G on X is an injective group homomorphism $G \to \mathrm{Homeo}(X, X)$. If for all $x \in X$ there exists an open subset $U \subset X$ with $x \in U$ such that $U \cap g(U) = \emptyset$ for all non-unit $g \in G$, then it is called a *properly discontinuous* action.

We give an example of these definitions. Let $\mathbb{R}$ be the real line and S^1 be the unit circle embedded in the complex plane. Now $\mathbb{R}$ is a covering space of S^1 with

[1] Note that Zariski topology in algebraic geometry is not Haussdorff.

the covering map $p : \mathbb{R} \to S^1$ such that $x \mapsto e^{i2\pi x}$. The deck transformations are of the form $f_n : \mathbb{R} \to \mathbb{R}$ with $x \mapsto x + n$ and $n \in \mathbb{Z}$. Thus $\mathrm{Deck}\left(\mathbb{R}/S^1\right) \cong \mathbb{Z}$.

Definition 2.4. Let X be a covering space of Y with covering map $p : X \to Y$. If for all $y \in Y$ and $x, x' \in p^{-1}(y)$ there is a $g \in \mathrm{Deck}(X/Y)$ such that $x' = gx$, then the covering space is called *regular*.

Given a properly discontinuous action G on a topological space X, we can construct a new topological space X/G. Let $Gx = \{gx : g \in G\}$ be the *orbit* of $x \in X$. Define X/G to be the set of all orbits in X with the quotient topology induced by the map $p_G : X \to X/G$ defined as $x \mapsto Gx$.

Proposition 2.5. *Let X be a path-connected space and G a group with a properly discontinuous action on X. Then X is a regular covering space of X/G with covering map $p_G : X \to X/G$ and deck transformation group G.*

Proof. See [7, proposition 1.40]. □

Proposition 2.6. *If X is a regular path-connected covering space of Y with surjective covering map $p : X \to Y$ and deck transformation group G, then X/G and Y are homeomorphic.*

We need that a local homeomorphism is open, before we can prove the above proposition. Recall that if $f : X \to Y$ is a continuous map and for all open subsets $A \subset X$ the image $f(A)$ is also open, then f is called *open*.

Lemma 2.7. *If $f : X \to Y$ is a local homeomorphism, then it is also open.*

Proof. Let $U \subset X$ be any open subset. For all $x \in X$ denote by $V_x \subset X$ the open subset such that $x \in V_x$ and $f|_{V_x}$ homeomorphism. Notice that $U = \bigcup_{x \in X} U \cap V_x$, so that $f(U) = \bigcup_{x \in X} f(U \cap V_x)$. The sets $f(U \cap V_x)$ are open, because $f|_{V_x}$ is a homeomorphism for all $x \in X$. Thus $f(U)$ a union of open sets, which is again an open set. Hence $f : X \to Y$ is open. □

Proof of proposition 2.6. Let $p_G : X \to X/G$ be the covering map from proposition 2.5. The map p factors through p_G, because $p(x) = p(gx)$ for all $x \in X$ and $g \in G$. Denote by $q : X/G \to Y$ the continuous map such that $p = q \circ p_G$. The map p is open by lemma 2.7 and is surjective by assumption. So q is also open and surjective.

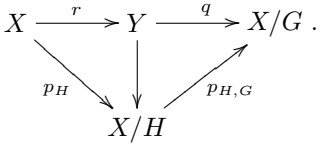
The map q is injective. Let $Gx_1, Gx_2 \in X/G$ be such that $q(Gx_1) = q(Gx_2)$. For $i = 1, 2$ there are $x_i \in X$ such that $p_G(x_i) = Gx_i$. There exists a $g \in G$ such that $x_2 = gx_1$, because X is a regular covering of Y and $p(x_1) = p(x_2)$. Thus $Gx_2 = Ggx_1 = Gx_1$.

Hence q is a homeomorphism. □

Not only is X a covering space of X/H for any subgroup $H \subset G$, but X/H is also a covering space of X/G. This allows us to construct various covering spaces of X/G.

Proposition 2.8. *Let X be a path-connected space and G a group with a properly discontinuous action on X. If $H \subset G$ is a subgroup, then X/H is a covering space of X/G with covering map $p_{H,G} : X/H \to X/G$ defined as $Hx \mapsto Gx$. Moreover X/H is a regular covering space of X/G if and only if H is a normal subgroup.*

Proposition 2.9. *Let X be a path-connected and locally path-connected topological space and G a group with a properly discontinuous action on X. If Y is a path-connected covering space of X/G with covering map $q : Y \to X/G$ and X is a covering space of Y with covering map $r : X \to Y$ such that $p_G = q \circ r$, then there exists a subgroup $H \subset G$ such that X/H and Y are homemorphic and the following diagram commutes*



Proof. See [7, exercise 1.3.24]. □

With the following proposition, we are able to compute the size of $p_{H,G}^{-1}(Gx)$ for some point $Gx \in X/G$. If X is a path-connected covering space of Y with covering map $p : X \to Y$, then $p^{-1}(y)$ is of the same size for all $y \in Y$ and is called the number of *sheets*.

Proposition 2.10. *Let X be a path-connected topological space and G a group with a properly discontinuous action on X. If $H \subset G$ is a subgroup, then*

$$\left|p_{H,G}^{-1}(Gx)\right| = [G : H]$$

for all $Gx \in X/G$.

Proof. Let $Gx \in X/G$ be any point and $x \in X$ be a point such that $p_G(x) = Gx$. Define $\rho : \{Hg : g \in G\} \to p_{H,G}^{-1}(Gx)$ as $Hg \mapsto Hgx$. For all $Hy \in p_{H,G}^{-1}(Gx)$ there exists a $y \in X$ such that $p_H(y) = Hy$ and a $g \in G$ such that $y = gx$. Therefore $\rho(Hg) = Hgx = Hy$, that is ρ is surjective.

Suppose that $\rho(Hg_1) = \rho(Hg_2)$, then $Hg_1x = Hg_2x$. So there exists $h_1, h_2 \in H$ such that $h_1g_1x = h_2g_2x$. The unique lifting property [7, proposition 1.34] gives $h_1g_1 = h_2g_2$. Hence $Hg_2 = Hg_1$, so that ρ is injective.

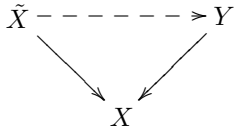
The map ρ is a bijection between the set of right-cosets and $p_{H,G}^{-1}(Gx)$. The index $[G : H]$ is the cardinality of the set of cosets. Thus $[G : H]$ is equal to the cardinality of $p_{H,G}^{-1}(Gx)$. □

Let X be a topological space. We assign a group $\pi_1(X, x_0)$ called the *fundamental group* to the space X with $x_0 \in X$ some point called the *basepoint*. Define a continuous map $f : I \to X$ with $I = [0, 1]$ to be a *path*. If $f(0) = x_0 = f(1)$, then f is called a *loop* at x_0. Let $g : I \to X$ be another path. The paths f and g are equivalent, if there exists a continuous map $F : I \times I \to X$ such that $F(s, 0) = f(s)$ and $F(s, 1) = g(s)$ for all $s \in I$ and $F(0, t)$ and $F(1, t)$ constant for all $t \in I$. As a set $\pi_1(X, x_0)$ is the set of equivalence classes of loops at x_0. The group law follows from concatenating two paths f and g.

If X is a path-connected space with a trivial fundamental group, then X is called *simply-connected*.

Definition 2.11. Let X be a path-connected topological space. If $\tilde{X}$ is a simply-connected covering space of X, then $\tilde{X}$ is called the *universal* covering space of X.

A universal covering space $\tilde{X}$ of X has a universal property. If Y is a path-connected covering space of X, then $\tilde{X}$ is also a universal covering space of Y such that the following diagram commutes



where the maps are the covering maps. This property implies that the universal covering space is unique, if it exists.

Proposition 2.12. *If X is a path-connected, locally path-connected and locally simply-connected space, then there exists a universal covering space of X.*

Proof. Special case of [1, theorem III.8.4] or [3, theorem 13.20]. □

We are now able to classify all the path-connected covering spaces of X, if X is locally path-connected and has a universal covering space $\tilde{X}$. A universal covering space is regular, thus proposition 2.6 implies that X and $\tilde{X}/G$ with $G = \mathrm{Deck}\left(\tilde{X}/X\right)$ are homeomorphic. Let Y be any path-connected covering space of X, then $\tilde{X}$ is also a covering space of Y by the universal property. So there exists a subgroup $H \subset G$ such that Y and $\tilde{X}/H$ are isomorphic covering spaces by proposition 2.9.

Proposition 2.13. *Let $\tilde{X}$ be the universal covering space of X and $x_0 \in X$ be any point. Then* $\mathrm{Deck}\left(\tilde{X}/X\right) \cong \pi_1(X, x_0)$.

Proof. See [1, corollary III.6.10], [7, proposition 1.39] or [3, theorem 13.11]. □

The next proposition we present is a special case of the van Kampen theorem. It allows us to compute the fundamental group of a space.

Proposition 2.14. *Let X be a topological space and $x_0 \in X$ some point. If $U, V \subset X$ are path-connected subsets such that $U \cap V$ is simply-connected, $X = U \cup V$ and $x_0 \in U \cap V$, then*

$$\pi_1(U, x_0) * \pi_1(V, x_0) \cong \pi_1(X, x_0)$$

where $*$ denotes the free product of groups.

Proof. See [1, corollary III.9.5], [3, corollary 14.9] or [7, theorem 1.20]. □

2.2 Riemann surfaces

In this section we discuss some of the aspects of the theory of Riemann surfaces. We focus on branched covering spaces and analytic continuations thereof. More information on Riemann surfaces can be found in [2, 3].

First we give the definition of a Riemann surface. Let X be a topological space. An open subset $U \subset X$ with a homeomorphism $\varphi_U : U \to V_U \subset \mathbb{C}$ is a *chart*. If X is connected and there exists a set of charts such that the set of all open subsets $\mathcal{U}$ is an open cover of X and $\varphi_{U_2} \circ \varphi_{U_1}^{-1} : \varphi_{U_1}(U_1 \cap U_2) \to$

$\varphi_{U_2}(U_1 \cap U_2)$ is a holomorphism for all $U_1, U_2 \in \mathcal{U}$, then X with this set of charts is called a *Riemann surface*.

Next we give the definition of a holomorphism between Riemann surfaces. Let X be a Riemann surface with $\mathcal{U}$ the set of charts and let Y be another Riemann surface with $\mathcal{V}$ the set of charts. If $f : X \to Y$ is a continuous map such that $\varphi_V \circ f \circ \varphi_U^{-1} : \varphi_U\left(U \cap f^{-1}(V)\right) \to \varphi_V(V)$ is a holomorphism for all $U \in \mathcal{U}$ and $V \in \mathcal{V}$, then f is called a *holomorphism*.

Definition 2.15. Let X and Y be Riemann surfaces. If $p : X \to Y$ is a non-constant holomorphic map, then X is a *branched covering space* of Y. A point $x \in X$ is called a *ramification point*, if for all open subsets $U \subset X$ with $x \in U$ the map $p|_U$ is not injective. The image of a ramification point is called a *branch point*.

We may restrict a branched covering space with a proper holomorphic map to a covering space. Recall that a continuous map $f : X \to Y$ is *proper*, if for all compact subsets $B \subset Y$ the inverse image $f^{-1}(B)$ is also compact.

Proposition 2.16. *Let X be a branched covering space of Y with the map $p : X \to Y$. If p is proper, then a closed discrete subset $A \subset X$ exists such that $X' = X \setminus A$ is a covering space of $Y' = Y \setminus p(A)$ with covering map $p|_{X'} : X' \to Y'$.*

Proof. See [2, remark 4.23]. □

In some cases we can do the opposite of the above proposition, that is we extend a covering space to a larger branched covering space.

Proposition 2.17. *Let X' and Y be Riemann surfaces and $B \subset Y$ a closed discrete subset. If X' is a covering space of $Y' = Y \setminus B$ with a proper holomorphic covering map $p' : X' \to Y'$, then p' extends to a unique proper holomorphic map $p : X \to Y$ with $X' \subset X$ and $p|_{X'} = p'$. Moreover if X is a covering space of Y, then* $\mathrm{Deck}(X'/Y') = \mathrm{Deck}(X/Y)$.

Proof. The proposition follows from [2, theorems 8.4 and 8.5]. □

The covering map in the previous proposition needs to be proper. In the next section we are interested in covering spaces with a finite number of sheets. It turns out that for such covering spaces the covering map is always proper.

Proposition 2.18. *Let X be a covering space of Y with covering map $p : X \to Y$. If the number of sheets is finite, then p is proper.*

Proof. Denote by n the finite number of sheets. Let $B \subset Y$ be any compact subset. Define $A = f^{-1}(B)$ and suppose that $\mathcal{U}$ is an open covering of A.

Let $y \in B$ be any point and $p^{-1}(y) = \{x_1, x_2, \ldots, x_n\}$. There exist open subsets $W_i \subset X$ for $i = 1, \ldots, n$ and $V \subset Y$ such that the W_i's are disjoint, $x_i \in W_i$, $y \in V$ and $p|_{W_i} : W_i \to V$ a homeomorphism, because p is a covering map. Moreover for all x_i there exists a $U_{y,i} \in \mathcal{U}$ such that $x_i \in U_{y,i}$. Define $V_y = \bigcap_{i=1}^n p(U_{y,i} \cap W_i)$. This subset of Y is open, because $U_{y,i}$ and W_i are open, p is an open map by lemma 2.7 and the intersection is finite. Obviously $y \in V_y$ and $V_y \subset V$. Define $W_{y,i} = p^{-1}(V_y) \cap W_i$, then $p^{-1}(V_y) = \bigcup_{i=1}^n W_{y,i}$. Furthermore $W_{y,i} \subset U_{y,i}$, because if $x \in W_{y,i}$ then $x \in W_i$ and $p(x) \in V_y \subset$

$p(U_{y,i} \cap W_i)$ so there is a $y \in U_{y,i} \cap W_i$ such that $p(x) = p(y)$ which implies $x = y \in U_{y,i}$ since $p|_{W_i}$ is a homeomorphism.

The collection of sets $\mathcal{V} = \{V_y : y \in B\}$ is an open covering of B and B is compact, so there exists a finite subcovering. Let $y_1, \ldots, y_m \in B$ be the points such that $B \subset \bigcup_{i=1}^{m} V_{y_i}$. The finite subcollection

$$\widetilde{\mathcal{U}} = \{U_{y_i,j} \in \mathcal{U} : i = 1, \ldots, m \text{ and } j = 1, \ldots, n\}$$

is an open covering of A, because if $x \in A$ then $p(x) \in V_{y_i}$ for some i so

$$x \in p^{-1}(V_{y_i}) = \bigcup_{j=1}^{n} W_{y_i,j} \subset \bigcup_{j=1}^{n} U_{y_i,j} \subset \bigcup_{U \in \widetilde{\mathcal{U}}} U.$$

Hence for any open covering $\mathcal{U}$ of A there exists a finite subcovering $\widetilde{\mathcal{U}}$, so A is compact. Thus for any compact subset B, the inverse image A is also compact. Hence p is proper. □

Proposition 2.19. *Let X be a covering space of Y with covering map $p : X \to Y$. If Y is a Riemann surface, then it induces a complex structure on X such that X is a Riemann surface and p a holomorphism.*

Proof. See [2, theorem 4.6]. □

Suppose that we have a Riemann surface Y and $B \subset Y$ a closed discrete subset. From the previous three propositions follows that a covering space of Y/B with a finite number of sheets can be extended to a branched covering space of Y. This is summarized in the next theorem.

Theorem 2.20. *Let Y be a Riemann surface and $B \subset Y$ a closed discrete subset. If X' is a covering space of $Y' = Y \setminus B$ with $p' : X' \to Y'$ the covering map and a finite number of sheets, then X' extends to a Riemann surface X and p' to a proper holomorphic map $p : X \to Y$. Moreover if X is a covering space of Y, then* $\mathrm{Deck}(X/Y) = \mathrm{Deck}(X'/Y')$.

Proof. Let X' be a finite covering space of $Y' = Y \setminus B$ with $p' : X' \to Y'$ the covering map and a finite number of sheets. There exists a complex structure such that Y' is a Riemann surface and p' is a holomorphism by proposition 2.19. The map p' is proper by proposition 2.18. Now X' extends to a Riemann surface X and p' to a proper holomorphic map $p : X \to Y$ by proposition 2.17. The last statement follows directly from the latter proposition. □

Proposition 2.21. *Let X be a Riemann surface and G a group with a properly discontinuous action on X. If g is a holomorphism for all $g \in G$, then the space X/G is a Riemann surface and the covering map $p : X \to X/G$ is holomorphic.*

Let X be a branched covering space of Y with covering map $p : X \to Y$. For all points $x \in X$ there exists charts $\varphi_{U_X} : U_X \to V_{U_X}$ with $x \in U_X \subset X$ and $\varphi_{U_Y} : U_Y \to V_{U_Y}$ with $p(x) \in U_Y \subset Y$ such that $\varphi_{U_Y} \circ p \circ \varphi_{U_X}^{-1}(z) = z^n$ for all $z \in V_{U_X}$ and some $n_x \in \mathbb{Z}_{>0}$. The number n_x is called the *ramification index* of p at x and is denoted by $e_p(x)$. Notice that $e_p(x) > 1$ if and only if x is a ramification point.

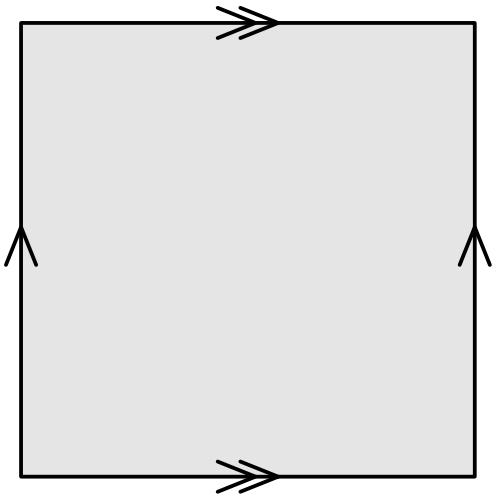


Figure 2.1: A torus can be defined as a square with opposite edges identified as indicated by the arrows.

Proposition 2.22 (Riemann-Hurwitz)**.** *Let X and Y be compact Riemann surfaces. If X is a branched covering space of Y with covering map $p : X \to Y$ and n sheets, then*

$$2\left(g_X - 1\right) = 2n\left(g_Y - 1\right) + \sum_{x \in X} \left(e_p\left(x\right) - 1\right)$$

where g_X is the genus of X and g_Y the genus of Y.

Proof. See [2, remark 17.14] or [3, theorem 19.15]. □

2.3 Branched covering spaces of a torus

In this section we will study branched covering spaces of a torus. We give the definition of a torus. Hereafter we describe all covering spaces of a torus by using the techniques from section 2.1. We also prove the existence of branched covering spaces of a torus branched above exactly one point by using the results from section 2.2.

We can define a torus in several ways. For example a torus can be defined as a square with opposite edges identified as shown in figure 2.1. We define it as $T = S^1 \times S^1$, that is, a product of two unit circles.

The universal covering space of a torus can be obtained as follows. Recall that $\mathbb{R}$ is a covering space of S^1 with the covering map $\mathbb{R} \to S^1$ defined as $x \mapsto e^{i2\pi x}$. The product of two covering spaces is again a covering space. Thus we obtain a covering space $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ of $T = S^1 \times S^1$ with covering map $p : \mathbb{R}^2 \to T$ defined as $(x_1, x_2) \mapsto \left(e^{i2\pi x_1}, e^{i2\pi x_2}\right)$. In fact this is the universal covering space of the torus, because $\mathbb{R}^2$ is simply-connected.

Proposition 2.23. *Let $p : \mathbb{R}^2 \to T$ be the universal covering of a torus. There exists a group isomorphism $\mathbb{Z}^2 \to \mathrm{Deck}\left(\mathbb{R}^2/T\right)$.*

Proof. Define a map $\rho : \mathbb{Z}^2 \to \mathrm{Deck}\left(\mathbb{R}^2/T\right)$ as $n \longmapsto (x \mapsto x+n)$. This is well-defined because $e^{i2\pi(x_i+n_i)} = e^{i2\pi x_i}$ for $n_i \in \mathbb{Z}$. Clearly ρ is an injective homomorphism. Suppose that $f : \mathbb{R}^2 \to \mathbb{R}^2$ is a deck transformation. Thus for all $x = (x_1, x_2) \in \mathbb{R}^2$ holds that $p \circ f(x) = p(x)$, that is

$$\left(e^{i2\pi f_1(x)}, e^{i2\pi f_2(x)}\right) = \left(e^{i2\pi x_1}, e^{i2\pi x_2}\right).$$

This implies that $f(x) = x + n_x$ with $n_x \in \mathbb{Z}^2$ for all $x \in \mathbb{R}$. Define $g = f - \mathrm{id}_{\mathbb{R}^2}$. Notice that $g(x) = n_x \in \mathbb{Z}^2$ for all $x \in \mathbb{R}^2$, so that $g : \mathbb{R}^2 \to \mathbb{Z}^2$. Since g is continuous, $\mathbb{R}^2$ is connected and $\mathbb{Z}^2$ discrete, then g must be constant. Thus there exists a $n \in \mathbb{Z}^2$ such that $g(x) = n$ for all $x \in \mathbb{R}^2$, that is $f = \rho(n)$. Hence ρ is also surjective, which makes ρ a group isomorphism. □

Now we have obtained another way to define a torus. Recall that a universal covering space is regular. So from proposition 2.6 and 2.23 follows that $\mathbb{R}^2/\mathbb{Z}^2$ and T are homeomorphic. Moreover $\mathbb{R}^2$ can be considered as a Riemann surface $\mathbb{C}$ and $\mathbb{Z}^2$ acts analytically on $\mathbb{C}$, so that $\mathbb{R}^2/\mathbb{Z}^2$ is also a Riemann surface by proposition 2.21.

We are now able to write down all the connected covering spaces of a torus. Proposition 2.9 tells us that any connected covering space of a torus corresponds to a subgroup of $G = \mathbb{Z}^2$. These subgroups have rank at most two. The universal covering space corresponds to the trivial group, that is the subgroup of rank zero. A subgroup of rank one corresponds to a infinitely long cylinder and is a covering space with an infinite number of sheets. In particular a finite connected covering space of the torus is itself a torus and corresponds to a subgroup of rank two.

All the connected covering spaces of a torus are now known. We like to construct a connected branched covering space of the torus, which branches only above a single point of the torus. Thus we seek a covering space of $S = T - t$ for some point $t \in T$ such that it can be continued to a branched covering space of T, but not to a covering space of T.

First we will compute the fundamental group of S. Consider the definition of a torus in figure 2.1. Let L_1 be the line with the single arrow, L_2 be the line with the double arrow, t be the corner point of the square and s_0 the point in center of the square. Define the open sets $U = S \setminus L_1$ and $V = S \setminus L_2$. Notice that $U \cap V = S \setminus (L_1 \cup L_2)$ is simply-connected and $U \cup V = S$. Thus by proposition 2.14 we have

$$\pi_1(S, s_0) = \pi_1(U, s_0) * \pi_1(V, s_0) \cong \mathbb{Z} * \mathbb{Z},$$

because U, V are homotopy equivalent with S^1 and $\pi_1\left(S^1, \cdot\right) \cong \mathbb{Z}$. Hence we have proved the following proposition.

Proposition 2.24. *Let $s_0 \in S$ be any point. Then $\pi_1(S, s_0) \cong \mathbb{Z} * \mathbb{Z}$.*

We are now able to prove the following theorem.

Theorem 2.25. *There exists a branched covering space of a torus with precisely one branch point.*

Proof. Recall that T is a Riemann surface and $S = T - t$ for some point t. Thus S is also a Riemann surface. Moreover S is path-connected, locally path-connected and locally simply-connected. Therefore S has a universal covering space $\tilde{S}$ with the deck transformation group

$$\mathrm{Deck}\left(\tilde{S}/S\right) \cong \pi_1(S, s) \cong \mathbb{Z} * \mathbb{Z}$$

by propositions 2.12 and 2.13.

Let $G = \langle a, b\rangle = \mathbb{Z} * \mathbb{Z}$ be the free group on two generators a and b. Consider the surjective homomorphism $f : G \to S_3$ defined as $a \mapsto (12)$, $b \mapsto (23)$. Define $H = \ker f$. Let $X = \tilde{S}/H$ be the covering space of S corresponding to H. It is a regular covering space, because H is normal. The number of sheets is finite, because S_3 is finite and proposition 2.10. Theorem 2.20 implies that X extends to a branched covering space Y of T. By construction it does not branch above any point of S. Suppose that t is also not a branch point, then Y is a covering space of T, so that $\mathrm{Deck}(X/S) = \mathrm{Deck}(Y/T)$ and $\mathrm{Deck}(Y/T)$ is abelian. However $\mathrm{Deck}(X/S) \cong S_3$ is not abelian. Therefore Y is not a covering space of T and must branch in t. □

In the above proof we constructed a branched covering space of a torus with six sheets. The following proposition shows that the number of sheets can be reduced to three.

Proposition 2.26. *There exists a branched covering space of a torus with three sheets and precisely one ramification point. The ramification index of that point is three.*

Proof. Let G and $f : G \to S_3$ be as in the proof of theorem 2.25. Define $\tilde{A} = \{\mathrm{id}, (12)\}$. It is a non-normal subgroup of S_3 and corresponds to a non-normal subgroup $A \subset G$ such that $H \subset A$. Let X_A be the covering space of S corresponding to A. It has three sheets, because $[G : A] = \left[S_3 : \tilde{A}\right] = 3$ and proposition 2.10. The space X_A extends to a branched covering space Y_A of T with a proper holomorphic covering map $p : Y_A \to T$ by theorem 2.20. Again it does not branch above S. Suppose that t is not a branch point, then Y is non-regular covering space of T, but any covering space of T is regular. Thus t is a branch point. Notice that T is compact and the covering map p is proper, therefore Y_A is also compact. From proposition 2.22 and $e_p(x) = 1$ for all $x \in X_A$ follows that

$$\sum_{x \in p^{-1}(t)} (e_p(x) - 1) \equiv 0 \mod 2.$$

Moreover $\sum_{x \in p^{-1}(t)} e_p(x)$ equals the number of sheets and $\left|p^{-1}(t)\right| < 3$. Hence $\left|p^{-1}(t)\right| = 1$ and $e_p(y) = 3$ for $y \in p^{-1}(t)$. □

We remark that the branched covering space of the torus constructed in the above proposition has genus two as follows from proposition 2.22.

Chapter 3

Algebraic geometry and elliptic curves

In this chapter we present an overview of the completion of a discrete valuation ring, algebraic geometry, elliptic curves and small Galois extension. We give references to the literature if necessary. At the end of this chapter we present an explicit example of a branched covering space of an ellitpic curve that branches only above a single point.

3.1 Discrete valuations and completions

We will give an overview of the theory of fields with a discrete valuation, the completion of a discrete valuation ring and field extensions thereof. For more information on discrete valuations see [8].

Definition 3.1. Let K be a field. A *discrete valuation* is a surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that $v(xy) = v(x) + v(y)$ and $v(x \pm y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

A field with a discrete valuation has useful properties. A *discrete valuation ring* is the set $R = \{x \in K : v(x) \geq 0\}$. It is a ring and has a unique maximal ideal $m = \{x \in K : v(x) > 0\}$. The ideal m is generated by any *uniformizer*, which is an element $x \in K$ such that $v(x) = 1$. An element $x \in R$ is a unit of R if and only if $v(x) = 0$. If t is a uniformizer of R and $x \in R$ is non-zero, then there is a unit $u \in R$ such that $x = ut^n$ with $n = v(x)$.

A field with a discrete valuation has a norm defined on it, namely $|x|_v = c^{-v(x)}$ for all $x \in K$ with $c \in \mathbb{R}_{>1}$ some constant. Thus the field and the discrete valuation ring are metric spaces and we could ask if they are complete. Below we define the completion of a discrete valuation ring.

Definition 3.2. Let K be a discrete valuation field with R its discrete valuation ring. The *completion* of R is

$$\hat{R} = \left\{(x_1, x_2, \ldots) \in R/m \times R/m^2 \times \cdots : \rho_n(x_{n+1}) = x_n \ \forall n \geq 1\right\}$$

with $\rho_n : R/m^{n+1} \to R/m^n$ the homomorphism obtained from factoring the canonical homomorphism $\pi_n : R \to R/m^n$ through $\pi_{n+1} : R \to R/m^{n+1}$. The quotient field of $\hat{R}$ and is denoted by $\hat{K}$.

Proposition 3.3. *Let R be a discrete valuation ring. The set $\hat{R}$ is a discrete valuation ring. The map $\pi : R \to \hat{R}$ defined as $x \mapsto (\pi_1(x), \pi_2(x), \ldots)$ is an injective homomorphism such that $v(x) = v \circ \pi(x)$ for all $x \in R$. Moreover $\hat{R}$ and $\hat{K}$ are complete.*

Proof. The set $\hat{R}$ is a subring of the product of rings $R/m \times R/m^2 \times \cdots$ as a straightforward calculation will show. Define $v_{\hat{R}} : \hat{R} \to \mathbb{Z} \cup \{\infty\}$ as

$$v_{\hat{R}}(x) = \begin{cases} \infty & \text{if } x = 0, \\ \min\{n \in \mathbb{Z}_{\geq 0} : x_{n+1} \neq 0\} & \text{otherwise.} \end{cases}$$

Let $x, y \in \hat{R}$. If $x = 0$ or $y = 0$, then $v_{\hat{R}}(xy) = v_{\hat{R}}(x) + v_{\hat{R}}(y)$ and $v_{\hat{R}}(x \pm y) \geq \min\{v_{\hat{R}}(x), v_{\hat{R}}(y)\}$ are trivial. Suppose that $x \neq 0$ and $y \neq 0$. Denote $n_x = v_{\hat{R}}(x)$ and $n_y = v_{\hat{R}}(y)$. Define $n = n_x + n_y$ and let $\tilde{x}, \tilde{y} \in R$ be such that $\pi_{n+1}(\tilde{x}) = x_{n+1}$ and $\pi_{n+1}(\tilde{y}) = y_{n+1}$. Notice that $v(\tilde{x}) = n_x$ and $v(\tilde{y}) = n_y$. Thus $v(\tilde{x}\tilde{y}) = v(\tilde{x}) + v(\tilde{y}) = n_x + n_y = n$. So

$$(xy)_{n+1} = x_{n+1}y_{n+1} = \pi_{n+1}(\tilde{x})\,\pi_{n+1}(\tilde{y}) = \pi_{n+1}(\tilde{x}\tilde{y}) \neq 0.$$

If $n > 0$, then in the same way $(xy)_n = 0$. Thus $v_{\hat{R}}(xy) = n = n_x + n_y = v_{\hat{R}}(x) + v_{\hat{R}}(y)$. Define $m = \min\{n_x, n_y\}$. If $m = 0$, then $v_{\hat{R}}(x \pm y) \geq 0 = m$, else $\pi_m(\tilde{x}) = 0$ and $\pi_m(\tilde{y}) = 0$ so that

$$(x \pm y)_m = x_m \pm y_m = \pi_m(\tilde{x}) \pm \pi_m(\tilde{y}) = 0$$

that is $v_{\hat{R}}(x \pm y) \geq m$. Therefore

$$v_{\hat{R}}(x \pm y) \geq m = \min\{n_x, n_y\} = \min\{v_{\hat{R}}(x), v_{\hat{R}}(y)\}.$$

Hence $\hat{R}$ is a discrete valuation ring with discrete valuation $v_{\hat{R}}$.

The map $\pi : R \to \hat{R}$ is a homomorphism, because $\pi_n : R \to R/m^n$ are homomorphisms for all $n \in \mathbb{Z}_{>0}$. Assume that $x \in \ker \pi$, then $\pi_n(x) = 0$ for all $n \in \mathbb{Z}_{>0}$, that is $x \in m^n$ for all $n \in \mathbb{Z}_{>0}$. So $x \in \bigcap_{n=1}^{\infty} m^n = \{0\}$, since R is Noetherian [8, lemma 8.3]. Hence $x = 0$, that is π is injective.

Let $\left(x^{(n)}\right)$ with $x^{(n)} \in \hat{R}$ be a Cauchy sequence. For all $n \in \mathbb{Z}_{>0}$ there exists a $N_n \in \mathbb{Z}_{>0}$ such that $\left|x^{(i)} - x^{(j)}\right| < c^{-n}$ for all $i, j \in \mathbb{Z}_{\geq N_n}$. Moreover $\left|x^{(i)} - x^{(j)}\right| = c^{-v_{\hat{R}}\left(x^{(i)} - x^{(j)}\right)}$. Therefore $v_{\hat{R}}\left(x^{(i)} - x^{(N_n)}\right) > n$ for all $i \in \mathbb{Z}_{\geq N_n}$. Define $y_n = x_n^{(N_n)}$ for all $n \in \mathbb{Z}_{>0}$ and $y = (y_1, y_2, \ldots)$. Now $y \in \hat{R}$, because for all $n \in \mathbb{Z}_{>0}$ it holds that $\rho_n\left(x_{n+1}^{(i)}\right) = x_n^{(i)}$, $x_n^{(i)} = x_n^{(N_n)}$ and $x_{n+1}^{(i)} = x_{n+1}^{(N_{n+1})}$ for all $i \in \mathbb{Z}_{\geq \max\{N_n, N_{n+1}\}}$, so that for all $n \in \mathbb{Z}_{>0}$ and $N = \max\{N_n, N_{n+1}\}$

$$\rho_n(y_{n+1}) = \rho_n\left(x_{n+1}^{(N_{n+1})}\right) = \rho_n\left(x_{n+1}^{(N)}\right) = x_n^{(N)} = x_n^{(N_n)} = y_n.$$

Let $\varepsilon > 0$ and $n = \min\left\{n' \in \mathbb{Z}_{>0} : n' > -\log_c\left(\frac{\varepsilon}{2}\right)\right\}$, then $\left|x^{(i)} - x^{(N_n)}\right| < \frac{\varepsilon}{2}$ for all $i \in \mathbb{Z}_{\geq N_n}$. Moreover $\left(x^{(N_n)} - y\right)_n = 0$, that is $v_{\hat{R}}\left(x^{(N_n)} - y\right) \geq n$. Therefore $\left|x^{(i)} - y\right| \leq \left|x^{(i)} - x^{(N_n)}\right| + \left|x^{(N_n)} - y\right| < \frac{\varepsilon}{2} + c^{-n} = \varepsilon$ for all $i \in \mathbb{Z}_{\geq N_n}$. Hence $\lim_{n\to\infty} x^{(n)} = y \in \hat{R}$, that is $\hat{R}$ is complete.

Consider a Cauchy sequence $\left(x^{(n)}\right)$ in $\hat{K}$. Assume that there exists a subsequence $\left(y^{(n)}\right)$ such that $v_{\hat{K}}\left(y^{(n)}\right) > v_{\hat{K}}\left(y^{(n+1)}\right)$ for all $n \in \mathbb{Z}_{>0}$, then it is

again a Cauchy sequence. So for all $n \in \mathbb{Z}$ there exists a $N_n \in \mathbb{Z}_{>0}$ such that $\left|y^{(i)} - y^{(j)}\right| < c^{-n}$ for all $i, j \in \mathbb{Z}_{\geq N_n}$. Thus $v_{\hat{K}}\left(y^{(i)}\right) = v_{\hat{K}}\left(y^{(i)} - y^{(N_n)}\right) > n$ for all $i \in \mathbb{Z}_{>N_n}$, which contradicts that $\left(v_{\hat{K}}\left(y^{(n)}\right)\right)$ is a strictly monotonically decreasing sequence in $\mathbb{Z}$. So the subsequence $\left(y^{(n)}\right)$ does not exists. Therefore there is a $m \in \mathbb{Z}$ such that $v_{\hat{K}}\left(x^{(n)}\right) \geq m$ for all $n \in \mathbb{Z}_{>0}$. Let t be a uniformizer of $\hat{R}$. The sequence $\left(z^{(n)}\right)$ with $z^{(n)} = x^{(n)} t^{-m}$ is Cauchy in $\hat{R}$ and has a limit $z \in \hat{R}$. So $x = zt^m$ is the limit of the sequence $\left(x^{(n)}\right)$. Hence $\hat{K}$ is complete. □

In some sense the completion of a discrete valuation ring is simpler than than the original ring. For example we can compute the roots of a polynomial in a number of cases using Hensel's Lemma [10, lemma IV.1.2].

Theorem 3.4 (Hensel's lemma)**.** *Let R be a discrete valuation ring and $F \in \hat{R}[X]$ be a polynomial. If an element $x' \in \hat{R}$ satisfies $v(F(x')) = n$ for some $n \in \mathbb{Z}_{>0}$ and $v\left(\frac{dF}{dX}(x')\right) = 0$, then there exists a unique element $x \in \hat{R}$ such $F(x) = 0$ and $v(x - x') \geq n$.*

Suppose that we have two discrete valuation rings R_K and R_L. If R_K is a subring of R_L and m_K a subset of m_L, then $\hat{R}_K$ is a subring of $\hat{R}_L$. In some cases the completions are in fact equal.

Proposition 3.5. *Let K and L be discrete valuation fields such that $R_K \subset R_L$ and $m_K \subset m_L$. If $R_L \subset \hat{K}$, then $\hat{K} = \hat{L}$.*

Proof. Let $x \in R_L$ be non-zero. From $R_L \subset \hat{K}$ follow that there exists a unit $u \in \hat{R}_K$ such that $x = u t_K^{v_K(x)}$ with t_K a uniformizer of R_K. In fact u is also a unit of $\hat{R}_L$. Therefore

$$v_L(x) = v_L(u) + v_K(x)\, v_L(t_K) = v_K(x)\, v_L(t_K).$$

It follows that $v_L(t_K) = 1$, because $1 = v_L(t_L) = v_K(t_L)\, v_L(t_K)$ for a uniformizer $t_L \in R_L$ and $v_L(t_K) \geq 0$ since $R_K \subset R_L$. Thus $v_L(x) = v_K(x)$. So $R_K \subset R_L \subset \hat{R}_K$ and $m_K \subset m_L \subset \hat{m}_K$. Hence $\hat{K} \subset \hat{L} \subset \hat{K}$, that is $\hat{K} = \hat{L}$. □

The ring of formal power series $k[[X]]$ over a field k is a discrete valuation ring. The valuation assigns to an element $a = \sum_{i=0}^{\infty} a_i X^i$ the integer n such that a_n is non-zero and $a_i = 0$ for all $i = 0, \ldots, n-1$. In some special cases the completion of a discrete valuation ring is isomorphic to some formal power series ring as the following proposition shows.

Proposition 3.6. *Let R be a discrete valuation ring. If $k \subset R$ is a field such that $\pi_1|_k : k \to R/m$ is surjective, then $\hat{R} = k[[t]]$ for any uniformizer t of R.*

Proof. Let t be a uniformizer of R. If the map $\alpha : k[[X]] \to \hat{R}$ given by

$$\sum_{i=0}^{\infty} a_i X^i \longmapsto \sum_{i=0}^{\infty} a_i t^i.$$

is a well-defined isomorphism, then the proposition follows.

The map α is a well-defined map of sets, because the infinite sum $\sum_{i=0}^{\infty} a_i t^i$ is the limit of the Cauchy sequence $\left(\sum_{i=0}^{n} a_i t^i\right)$ and $\hat{R}$ is a complete metric space. It is a ring homomorphism for a similar reason.

The map α is injective. Assume that there exists a non-zero $x \in \ker \alpha$, then $x = uX^n$ for some unit u and integer $n = v(x)$. Since a unit cannot be in the kernel of a ring homomorphism, then $n > 0$, so $X^n \in \ker \alpha$, which contradicts $\alpha(X^n) = t^n \neq 0$. Hence such a x does not exist.

The map α is also surjective. Let $x \in \hat{R}$ be any element. The map $\pi_1|_k$ is injective, because k is a field. So $\pi_1|_k$ is an isomorphism and let ρ be the inverse. Notice that $\pi_1 \circ \rho = \mathrm{id}_{R/m}$. Define $a_0 = \rho \circ \pi_1(x)$, then $\pi_1(x - a_0) = \pi_1(x) - \pi_1(a_0) = 0$ so that $v(x - a_0) > 0$. If $a_0, \ldots, a_n \in k$ are defined such that $v\left(x - \alpha\left(\sum_{i=0}^{n} a_i X^i\right)\right) > n$, then let $y \in \hat{R}$ be such that $x - \alpha\left(\sum_{i=0}^{n} a_i X^i\right) = yt^{n+1}$. Define $a_{n+1} = \rho \circ \pi_1(y)$, then

$$\begin{aligned} v\left(x - \alpha\left(\sum_{i=0}^{n+1} a_i X^i\right)\right) &= v\left(yt^{n+1} - a_{n+1}t^{n+1}\right) \\ &= v(y - a_{n+1}) + n + 1 > n + 1, \end{aligned}$$

because $\pi_1(y - a_{n+1}) = \pi_1(y) - \pi_1(a_{n+1}) = 0$. By induction this gives an element $\sum_{i=0}^{\infty} a_i X^i \in k[[X]]$ such that $\alpha\left(\sum_{i=0}^{\infty} a_i X^i\right) = x$.

Hence $\alpha : k[[X]] \to \hat{R}$ is a ring isomorphism. □

Proposition 3.7. *Let L/K be discrete valuation fields such that $R_K \subset R_L$ and $m_K \subset m_L$. If L/K is an algebraic extension, then R_L/m_l is also an algebraic extension of R_K/m_K.*

Proof. Denote $l_K = R_K/m_K$ and $l_L = R_L/m_L$. Let $\pi_K : R_K \to l_K$ and $\pi_L : R_L \to l_L$ be the canonical homomorphisms. Write the injective homomorphism corresponding to $R_K \subset R_L$ as $i : R_K \to R_L$. The kernel of the ring homomorphism $\pi_L \circ i : R_K \to l_L$ contains the maximal ideal m_K, so it is equal to m_K. Hence the map factors through π_K and induces an injective ring homomorphism $\tilde{\imath} : l_K \to l_L$. Thus l_L is an extension of l_K.

Suppose that L is algebraic over K. Let $\tilde{x} \in l_L$, then there is a $x \in R_L$ such that $\pi_L(x) = \tilde{x}$. In fact $x \in L$ so there is a $F = \sum_{i=0}^{n} a_i X^i \in K[X]$ of positive degree n such that $F(x) = 0$. Assume that $m = \min_{i=0,\ldots,n} v(a_i) = 0$, otherwise $G = t^{-m}F$ for some uniformizer t does satisfy this condition. In particular $v(a_i) = 0$ for some $i > 0$, otherwise

$$0 = v(a_0) = v\left(\sum_{i=1}^{n} a_i x^i\right) \geq \min_{i=1,\ldots,n} \left(v(a_i) + v\left(x^i\right)\right) > 0$$

since $v(a_i) > 0$ for $i = 1, \ldots, n$ and $v(x) = 0$. Thus $\tilde{F} = \sum_{i=0}^{n} \tilde{a}_i X^i \in l_K[X]$ with $\tilde{a}_i = \pi_K(a_i)$ has positive degree and $\tilde{F}(\tilde{x}) = \pi_L(F(x)) = 0$. So $\tilde{x}$ is algebraic over l_K. Hence l_L is an algebraic extension of l_K. □

The ring of formal Laurent series $k((X))$ is the quotient field of $k[[X]]$. Given that the field k is algebraically closed and of characteristic zero, then any finite extension of the formal Laurent series ring is again such a ring $k((Y))$ with $Y^n = X$ and n some positive integer [14]. We describe this in the following proposition and corollary.

Proposition 3.8. *Let L/K be discrete valuation fields such that $R_K \subset R_L$, $m_K \subset m_L$, $k_K \subset R_K$ with $\pi_K|_{k_K}$ an isomorphism and $k_L \subset R_L$ with $\pi_L|_{k_L}$ an isomorphism. If k_L/k_K is finite and k_K has characteristic zero, then $\hat{L}/\hat{K}$ is also finite.*

Proof. Let $t_K \in R_K$ and $t_L \in R_L$ be uniformizers. Proposition 3.6 implies that $\hat{R}_K = k_K[[t_K]]$ and $\hat{R}_L = k_L[[t_L]]$. Define $n = v_L(t_K)$ with v_L the discrete valuation of L. Let $u \in R_L$ be a unit such that $t_K = ut_L^n$. Notice that $n > 0$, because $m_K \subset m_L$. Define $F = X^n - u \in \hat{R}_L[X]$, then $\frac{dF}{dX} = nX^{n-1}$. Consider $G = X^n - u' \in k_L[X]$ with $u' = \pi_L|_{k_L}^{-1} \circ \pi_L(u) \in k_L$. Since u is a unit, then u' is also a unit. Let k_M be a splitting field for G and x' be a root of G [5, theorem 7.3], then k_M/k_L is finite. Define $\hat{R}_M = k_M[[t_L]]$ and denote the discrete valuation by v_M. Now $v_M(F(x')) > 0$ and $\frac{dF}{dX}(x')$ is a unit. Hensel's lemma implies that there exists a $x \in \hat{R}_M$ such that $F(x) = 0$. Define $t_M = xt_L$, then $t_M^n = t_K$. Also $t_M \in \hat{R}_M$ is a uniformizer, because x is a unit. Hence $\hat{R}_K \subset \hat{R}_L \subset \hat{R}_M = k_M[[t_M]]$ with $t_K = t_M^n$ and k_M/k_L finite.

The extension k_M/k_K is finite, because k_M/k_L and k_L/k_K are finite. Let $x_1, \ldots, x_m \in k_M$ be a basis of k_M/k_K. Take any $f = \sum_i a_i t_K^i \in k_M((t_K))$. There exists $a_{ij} \in k_K$ such that $a_i = a_{i1}x_1 + \cdots + a_{im}x_m$. Define $f_j = \sum_i a_{ij}t_K^i \in \hat{K}$. Now $f = f_1x_1 + \cdots + f_mx_m$, so that $\{x_1, \ldots, x_m\}$ is a set of generators for $k_M((t_K))/\hat{K}$.

Define $\hat{M} = k_M((t_M))$ and $y_i = t_M^i$ for $i = 0, \ldots, n-1$. The y_i's are linear independent over $k_M((t_K))$, otherwise $c_0y_0 + \ldots c_{n-1}y_{n-1} = 0$ with $c_i \in k_M((t_K))$ not all zero and $v_M(c_\alpha y_\alpha) = v_M(c_\beta y_\beta)$ for some $\alpha \neq \beta$, but $v_M(c_iy_i) \equiv i \mod n$ and $\alpha \not\equiv \beta \mod n$. Take any $f = \sum_i a_i t_M^i \in \hat{M}$ and define $f_j = \sum_i a_{ni+j}t_K^i \in k_M((t_K))$, then $f = f_0y_0 + \cdots + f_{n-1}y_{n-1}$. Thus the set $\{y_0, \ldots, y_{n-1}\}$ is a basis of $\hat{M}/k_M((t_K))$.

The extension $\hat{L}/\hat{K}$ is finite, because $\hat{L} \subset \hat{M}$ and both $\hat{M}/k_M((t_K))$ and $k_M((t_K))/\hat{K}$ are finite. □

Corollary 3.9. *Let L/K be discrete valuation fields such that $R_K \subset R_L$, $m_K \subset m_L$, $k_K \subset R_K$ an algebraically closed field of characteristic zero and $\pi_K|_{k_K}$ an isomorphism. If R_L/m_L is an algebraic extension of R_K/m_K, then $\hat{L}/\hat{K}$ is Galois and $\mathrm{Gal}\left(\hat{L}/\hat{K}\right) \cong \mathbb{Z}/n\mathbb{Z}$ with $n = v_L(t_K)$ for any uniformizer $t_K \in R_K$.*

Proof. Denote $k = k_K$. Notice that $R_L/m_L = R_K/m_K$, because $R_K/m_K \cong k$ is algebraically closed. Thus $\pi_L|_{k_L}$ with $k_L = k$ is also an isomorphism. Let k_M, t_M and $\hat{M}$ be as in the proof of the proposition, then also $k = k_M$. Therefore $\hat{K} = k((t_K))$ and $\hat{L} = \hat{M} = k((t_M))$. In fact $\hat{L} = \hat{K}(t_M)$ with t_M a root of $F = X^n - t_K$. Let $\omega \in k_K$ be a primitive n-th root of unity, then $F = \prod_{i=0}^n \left(X - \omega^i t_M\right)$. The polynomial F is irreducible over $\hat{K}$, otherwise $t_M^m \in \hat{K}$ for some $0 < m < n$ and $t_K = t_M^n$ so that $0 < v_K(t_M^m) < 1$. The extension $\hat{L}/\hat{K}$ is normal and separable, because $\hat{L}$ is a splitting field for F and $\omega^i t_M \neq \omega^j t_M$ for $i \neq j$. So $\hat{L}/\hat{K}$ is Galois.

Let $\sigma \in \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$, then $\sigma(t_M) = \omega^i t_M$. Moreover $\sigma(t_M)$ determines σ

$$\sigma\left(c_0 + c_1t_M + \cdots + c_{n-1}t_M^{n-1}\right) = c_0 + c_1\sigma(t_M) + \cdots + c_{n-1}\sigma(t_M)^{n-1}.$$

Define $\sigma_i \in \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$ such that $\sigma_i(t_M) = \omega^i t_M$. The map $\mathbb{Z} \to \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$ defined as $i \mapsto \sigma_i$ is a surjective group homomorphism, because $\sigma_{i+j}(t_M) = \omega^{i+j}t_M = \sigma_i \circ \sigma_j(t_M)$ and $\sigma = \sigma_i$ for some i. The kernel is $n\mathbb{Z}$, because $\sigma_n = \mathrm{id}$ and $\sigma_i = \mathrm{id}$ implies that $\omega^i = 1$, that is, n divides i since ω is a primitive n-th root of unity. Hence it induces a group isomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$. □

This corollary allows us to determine the value of $v_L(t_K)$ using only the completions $\hat{L}$ and $\hat{K}$. In particular if L is an algebraic extension of K, then R_L/m_L is an algebraic extension of R_K/m_K by proposition 3.7, so that $\hat{L}$ is a finite Galois extension of $\hat{K}$ by corollary 3.9.

3.2 Algebraic geometry

We give an overview of some results from algebraic geometry. For more in depth information we refer the reader to [4, 6, 10].

Let k be an algebraically closed field. A curve C over k is defined as a one dimensional non-singular projective variety over k. We assign to a curve C the field $k(C)$ of all rational functions from C to k, which is a function field of dimension one over k.

Definition 3.10. If K is a finitely generated extension of k with transcendence degree one, then K is called a function field of dimension one over k.

Suppose that C and D are curves over k. If $\phi : C \to D$ is a surjective morphism, then it induces an inclusion $\phi^* : k(D) \to k(C)$ of function fields defined as $f \mapsto f \circ \phi$.

Proposition 3.11. *There exists an arrow-reversing equivalence of categories of the category of non-singular projective curves over k with surjective morphisms and the category of function fields of dimension one over k with homomorphisms fixing k. The contravariant functor is*

$$\begin{array}{rcl} C & \longmapsto & k(C) \\ \phi : C \to D & \longmapsto & \phi^* : k(D) \to k(C) \end{array}$$

Proof. See [6, corollary I.6.12]. □

Corollary 3.12. *Let C, D_1 and D_2 be curves over k and $\phi_1 : D_1 \to C$ and $\phi_2 : D_2 \to C$ be surjective morphisms. A surjective morphism $\lambda : D_1 \to D_2$ such that $\phi_1 = \phi_2 \circ \lambda$ corresponds to a homomorphism $\lambda^* : k(D_2) \to k(D_1)$ fixing k such that $\phi_1^* = \lambda^* \circ \phi_2^*$.*

The definition of a branched covering space in algebraic geometry is analogous to the definition in the theory of Riemann surfaces.

Definition 3.13. Let C and D be curves over k. If $\phi : C \to D$ is a surjective morphism, then C is called a branched covering space of D with ϕ the covering map.

Definition 3.14. Let C and D be curves over k and $\phi : C \to D$ be a surjective morphism. If $\lambda : C \to C$ is a surjective morphism such that $\phi \circ \lambda = \phi$, then $\lambda : C \to C$ is called a deck transformation.

This definition of a deck transformation of a branched covering space is the same as the definition in the previous chapter. Again the set of all such morphisms is a group. Moreover corollary 3.12 implies that the groups $\mathrm{Deck}(C/D)$ and $\mathrm{Gal}(k(C)/\phi^* k(D))$ are isomorphic.

Let C be a curve over k. At a point $P \in C$ we define the local ring as

$$R_P = \{f \in k(C) : f \text{ regular at } P\}.$$

The ring R_P is a discrete valuation ring, because C is non-singular by definition and [10, proposition II.1.1]. A function in R_P may have a zero in P. The discrete valuation measures the multiplicity of this zero. Any point $P \in C$ corresponds to a discrete valuation v_P on $k(C)$ by [4, corollary 7.1.4].

We are now ready to define the ramification index.

Definition 3.15. Let C and D be curves over k, $\phi : C \to D$ be a surjective morphism and $P \in C$ be a point. The ramification index of ϕ at P is defined as

$$e_\phi(P) = v_P\left(\phi^*\left(t_{\phi(P)}\right)\right)$$

where v_P is the discrete valuation at P and $t_{\phi(P)}$ a uniformizer of the discrete valuation ring at $\phi(P)$. The morphism ϕ is ramified at P, if $e_\phi(P) > 1$, otherwise ϕ is unramified at P.

Remark that the ramification index is always larger or equal to one, because if $f \in R_{\phi(P)}$ has a zero in $\phi(P)$ then $\phi^* f(P) = f \circ \phi(P) = 0$. Thus the homomorphism ϕ^* restricts to an injective homomorphism $R_{\phi(P)} \to R_P$ such that $m_{\phi(P)}$ is mapped into m_P.

The ramification index is restricted by the following two propositions.

Proposition 3.16. *Let C and D be curves over k and $\phi : C \to D$ be a surjective morphism. For all points $Q \in D$*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = [k(C) : \phi^* k(D)].$$

Moreover if $k(C)$ is a Galois extension of $\phi^* k(D)$, then for all $P \in \phi^{-1}(Q)$

$$n e_\phi(P) = [k(C) : \phi^* k(D)],$$

where $n = \left|\phi^{-1}(Q)\right|$.

Proof. The first part is proven in [10, proposition II.2.6.a]. The second part is proven in [13, corollary 3.7.2], where $f(P) = 1$ since k is algebraically closed. □

Proposition 3.17. *Let C, D and E be curves over k. If $\phi : C \to D$ and $\lambda : D \to E$ are surjective morphisms, then for any point $P \in C$*

$$e_{\lambda \circ \phi}(P) = e_\lambda(\phi(P))\, e_\phi(P).$$

Proof. See [10, proposition II.2.6.c]. □

The Riemann-Hurwitz formula is a relation between the genus of two curves and the ramification index of the morphism between those curves. It is given in the proposition below.

Proposition 3.18. *Let C and D be curves over k and $\phi : C \to D$ be a surjective morphism. If $k(C)$ is a separable extension of $\phi^* k(D)$ and in the case that the characteristic of k is positive it does not divide $e_\phi(P)$ for any point $P \in C$, then*

$$2(g_C - 1) = 2[k(C) : \phi^* k(D)](g_D - 1) + \sum_{P \in C} (e_\phi(P) - 1)$$

where g_C and g_D are the genus of C and D respectively.

Proof. See [6, corollary IV.2.4] or [10, theorem II.5.9]. □

The following proposition relates the subgroup of deck transformations that fix a particular point to the ramification index at that point via corollary 3.9.

Proposition 3.19. *Let C and D be curves over k and $\phi : C \to D$ be a surjective morphism. If $k(C)$ is a Galois extension of $\phi^* k(D)$, then for all points $P \in C$ the subgroup*

$$\{\sigma \in \mathrm{Deck}(C/D) : \sigma(P) = P\}$$

is isomorphic to $\mathrm{Gal}\left(k(C)_P / \phi^* k(D)_Q\right)$ *where* $Q = \phi(P)$.

Proof. Let $G = \mathrm{Gal}\left(k(C)_P / \phi^* k(D)_Q\right)$. A deck transformation σ that fixes a point P corresponds to a $\sigma^* \in \mathrm{Gal}\left(k(C)/\phi^* k(D)\right)$ such that σ^* maps the local ring at P to itself. In this case σ^* extends to a unique element in G. The proposition now follows from the fact that $\hat{\tau}(k(C)) \subset k(C)$ for all $\hat{\tau} \in G$. □

3.3 Elliptic curves

In this section we will give an overview of some concepts from the theory of elliptic curves. For more background information see [10, 11, 12].

Let k be a perfect field of characteristic different from two and three. An elliptic curve defined over k is a curve E defined over k of genus one with a point O on E. The curve E is isomorphic to a non-singular curve given by the so-called Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in k$. In this case O corresponds to the point at infinity.

Proposition 3.20. *The curve $E : y^2 = x^3 + ax + b$ with $a, b \in k$ is irreducible.*

Proof. Let $F = Y^2 - X^3 - aX - b \in \bar{k}[X, Y]$. The curve E is irreducible if and only if (F) is a prime ideal if and only if F is irreducible, because of Hilbert's Nullstellensatz and $\bar{k}[X, Y]$ is a unique factorization domain.

Consider F as in $R[Y]$ with $R = \bar{k}[X]$. Assume that $X^3 + aX + b$ does not have a zero of multiplicity three, then $X^3 + aX + b$ has a zero x of multiplicity one, so that F is an Eisenstein polynomial for $X - x$, thus F is irreducible. On the other had if $X^3 + aX + b$ does have a zero of multiplicity three, then $F = Y^2 - X^3$, which is also irreducible since X^3 is not a square in R. □

We define two attributes of a curve given by a Weierstrass equation. The first attribute is the discriminant $\Delta = 4a^3 + 27b^2$. The discriminant is non-zero if and only if the curve is non-singular. The second attribute is the j-invariant $j = 1728\frac{4a^3}{\Delta}$.

Let E and E' be elliptic curves defined over k with Weierstrass equations $y^2 = x^3 + ax + b$ and $\eta^2 = \xi^3 + \alpha\xi + \beta$ respectively. If l is an extension of k, then the elliptic curves E and E' are isomorphic over l if and only if there exists a $u \in l^*$ such that $\alpha = u^4 a$ and $\beta = u^6 b$. The isomorphism is given by the change of coordinates $\xi = u^2 x$ and $\eta = u^3 y$. Clearly the j-invariant does not change by such a transformation, but the discriminants are related as $\Delta(E') = u^{12}\Delta(E)$.

An elliptic curve E is also a group and the point O is the unit element. If E is defined over k, then the points on E over k form a subgroup $E(k)$ of E.

For a positive integer n, write the subgroup of E containing the points of order dividing n as $E[n]$.

Let $P \in E[n]$ be any point different from O. In this case $P = (x, y)$ for some $x, y \in \bar{k}$. For example we can consider an extension of k that contains both coordinates. Denote the smallest field extension of k containing the x and y coordinates of all points in $E[n] - O$ by $k(E[n])$. Similar write $k(E[n]_x)$ for the smallest field extension of k containing only the x-coordinates.

Proposition 3.21. *Let E be an elliptic curve defined over k. If $n \in \mathbb{Z}_{\geq 2}$, then $k(E[n])$ and $k(E[n]_x)$ are Galois extensions of k.*

Proof. The proposition is proven in [12, section VI.2] for $\mathbb{Q}(E[n])$, however the adoption to $k(E[n])$ and $k(E[n]_x)$ is straightforward. □

We can consider the Galois group of the extension $k(E[n])$ of k as a subgroup of the special linear group over $\mathbb{Z}/n\mathbb{Z}$ by the following proposition.

Proposition 3.22. *Let E be an elliptic curve defined over k. If k contains a n-th primitive root of unity with $n \in \mathbb{Z}_{\geq 2}$ prime to the characteristic of k, then there exists an injective homomorphism $\rho_n : \mathrm{Gal}(k(E[n])/k) \to SL_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. There is an action of $\mathrm{Gal}(\bar{k}/k)$ on $E(\bar{k})$ and it respects the group law of the elliptic curve, because the curve is defined over k. In fact

$$n\sigma(P) = \sigma(nP) = \sigma(O) = O$$

for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and $P \in E[n]$. So $\mathrm{Gal}(\bar{k}/k)$ acts on $E[n]$. Denote the action by $\rho_n : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(E[n])$. Clearly $\mathrm{Gal}(\bar{k}/k(E[n])) \subset \ker \rho_n$. For all $\sigma \in \ker \rho_n$ and $P = (x, y) \in E[n] - O$

$$(x, y) = \rho_n(\sigma)(x, y) = (\sigma(x), \sigma(y)),$$

that is $\sigma(x) = x$ and $\sigma(y) = y$, so that $\mathrm{Gal}(\bar{k}/k(E[n])) \supset \ker \rho_n$. Therefore $\mathrm{Gal}(\bar{k}/k(E[n]))$ is a normal subgroup of $\mathrm{Gal}(\bar{k}/k)$. Hence the action ρ_n induces an injective homomorphism $\rho_n : \mathrm{Gal}(k(E[n])/k) \to \mathrm{Aut}(E[n])$.

Let $e_n : E[n] \times E[n] \to \mu_n$ be the Weil-paring where μ_n is the group of n-th roots of unity. It is a bilinear, alternating and Galois invariant map [10, proposition III.8.1]. There exists points $S, T \in E[n]$ with $e_n(S, T)$ a primitive n-th root of unity [10, corollary III.8.1.1]. Assume that $aS + bT = O$ for some $a, b \in \mathbb{Z}_{\geq 0}$, then

$$\begin{aligned} e_n(S, T) &= e_n(S + aS + bT, T) = e_n((1 + a)S, T)\, e_n(bT, T) \\ &= e_n(S, T)^{1+a}\, e_n(T, T)^b = e_n(S, T)^{1+a} \end{aligned}$$

and

$$\begin{aligned} e_n(S, T) &= e_n(S, T + aS + bT) = e_n(S, aS)\, e_n(S, (1 + b)T) \\ &= e_n(S, S)^a\, e_n(S, T)^{1+b} = e_n(S, T)^{1+b}, \end{aligned}$$

so that $e_n(S, T)^a = 1$ and $e_n(S, T)^b = 1$, that is n divides a and b. Thus the subgroup generated by S, T contains at least n^2 elements. In fact $|E[n]| = n^2$ [10, corollary III.6.4]. Hence $\{S, T\}$ is a basis of the $\mathbb{Z}/n\mathbb{Z}$-module $E[n]$.

Let $\sigma \in \mathrm{Gal}\left(k\left(E\left[n\right]\right)/k\right)$ and $a, b, c, d \in \mathbb{Z}$ such that $\sigma\left(S\right) = aS + cT$ and $\sigma\left(T\right) = bS + dT$. Then

$$\begin{aligned} e_n\left(S,T\right) &= \sigma\left(e_n\left(S,T\right)\right) = e_n\left(\sigma\left(S\right),\sigma\left(T\right)\right) = e_n\left(aS+cT,bS+dT\right) \\ &= e_n\left(aS,bS\right)e_n\left(aS,dT\right)e_n\left(cT,bS\right)e_n\left(cT,dT\right) \\ &= e_n\left(S,S\right)^{ab}e_n\left(S,T\right)^{ad}e_n\left(T,S\right)^{bc}e_n\left(T,T\right)^{cd} \\ &= e_n\left(S,T\right)^{ad}e_n\left(S,T\right)^{-bc} = e_n\left(S,T\right)^{ad-bc}, \end{aligned}$$

where the first equality follows from $\mu_n \subset k$. Thus $e_n\left(S,T\right)^{ad-bc-1} = 1$, that is $ad - bc \equiv 1 \mod n$. Since the a, b, c, d are unique up to a multiple of n, this means that the matrix representation of σ with respect to the basis $\{S, T\}$ has determinant one.

Hence the injective homomorphism $\rho_n : \mathrm{Gal}\left(k\left(E\left[n\right]\right)/k\right) \to \mathrm{Aut}\left(E\left[n\right]\right)$ combined with the matrix representation $\mathrm{Aut}\left(E\left[n\right]\right) \to \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)$ gives an injective homomorphism $\mathrm{Gal}\left(k\left(E\left[n\right]\right)/k\right) \to \mathrm{SL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)$. □

Let K be a perfect field of characteristic different from two and three with a discrete valuation v_K. Denote the discrete valuation ring by R_K and the residue field by k_K. Write the canonical homomorphism as $\pi_K : R_K \to k_K$.

Proposition 3.23. *The reduction map $\pi : \mathbb{P}^2\left(K\right) \to \mathbb{P}^2\left(k_K\right)$ defined as*

$$\left(x_0 : x_1 : x_2\right) \mapsto \left(\pi_K\left(x_0 t^{-n_x}\right) : \pi_K\left(x_1 t^{-n_x}\right) : \pi_K\left(x_2 t^{-n_x}\right)\right)$$

with $n_x = \min_{i=0,1,2} v_K\left(x_i\right)$ and a fixed uniformizer t is well-defined.

Proof. The minimum $n_x \in \mathbb{Z}$, because $x_i \neq 0$ for some i. The element $x_i t^{-n_x} \in R_K$ for all i, since $v_K\left(x_i t^{-n_x}\right) = v_K\left(x_i\right) - n_x \geq 0$. In particular $x_i t^{-n_x} \in R_K$ is a unit for some i, because $v_K\left(x_i\right) = n_x$ for some i. Thus $\pi_K\left(x_i t^{-n_x}\right)$ well-defined for all i and non-zero for at least one i.

Let $\left(y_0 : y_1 : y_2\right) \in \mathbb{P}^2\left(K\right)$ be another representation of $\left(x_0 : x_1 : x_2\right)$, that is $y_i = c x_i$ for all i and some non-zero $c \in K$. Let $u \in R_K$ be a unit such that $c = u t^{n_c}$ with $n_c = v_K\left(c\right)$, then $n_y = n_x + n_c$ so that

$$\pi_K\left(y_i t^{-n_y}\right) = \pi_K\left(u x_i t^{-n_y+n_c}\right) = \pi_K\left(u\right)\pi_K\left(x_i t^{-n_x}\right)$$

with $\pi_K\left(u\right) \in k_K$ again a unit independent of i. Hence the image of both representations are also equivalent.

The map $\pi : \mathbb{P}^2\left(K\right) \to \mathbb{P}^2\left(k_K\right)$ is well-defined, because it is well-defined on a representation of a point in $\mathbb{P}^2\left(K\right)$ and different representations of the same point are mapped to the same point in $\mathbb{P}^2\left(k_K\right)$. □

Corollary 3.24. *Let L be a finite extension of K. If v_L is a discrete valuation on L such that $R_K \subset R_L$ and $m_K \subset m_L$, then the reduction map*

$$\pi : \mathbb{P}^2\left(\hat{L}\right) \to \mathbb{P}^2\left(k_L\right)$$

is Galois equivariant.

Proof. Let t_L be a uniformizer of $\hat{R}_L$. Take any automorphism $\sigma \in \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$. It restricts to an automorphism of $\hat{R}_L$ that fixes $\hat{R}_K$ and it induces an automorphism $\tilde{\sigma} : k_L \to k_L$ that fixes k_K. Moreover $\pi_L \circ \sigma = \tilde{\sigma} \circ \pi_L$. In particular $\sigma(t_L) = u t_L$ for some unit $u \in \hat{R}_L$. Therefore

$$\begin{aligned}\pi_L\left(\sigma(x_i)\, t_L^{-n_{\sigma(x)}}\right) &= \pi_L\left(\sigma\left(x_i t_L^{-n_{\sigma(x)}}\right) u^{n_{\sigma(x)}}\right) \\ &= \pi_L \circ \sigma\left(x_i t_L^{-n_{\sigma(x)}}\right) \pi_L(u)^{n_{\sigma(x)}} \\ &= \tilde{\sigma} \circ \pi_L\left(x_i t_L^{-n_{\sigma(x)}}\right) \pi_L(u)^{n_{\sigma(x)}}\end{aligned}$$

Notice that $n_x = n_{\sigma(x)}$. Moreover $\pi_L(u)$ is a unit in k_L independent of i. Thus $\pi \circ \sigma = \tilde{\sigma}\pi$. Hence the reduction map is equivariant for all $\sigma \in \mathrm{Gal}\left(\hat{L}/\hat{K}\right)$. □

Let E be an elliptic curve defined over K. The discrete valuation on K allows us to study the group E via another elliptic curve defined over the residue field k_K. Denote the Weierstrass equation of E by $y^2 = x^3 + ax + b$ with $a, b \in K$. This equation is called minimal if $v_K(a) \geq 0$ and $v_K(b) \geq 0$ with $v_K(\Delta)$ minimal with respect to change of coordinates.

Definition 3.25. Let E be an elliptic curve defined over K with the minimal Weierstrass equation $y^2 = x^3 + ax + b$. The reduced curve of E is defined as

$$\tilde{E} : \tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x} + \tilde{b},$$

where $\tilde{a} = \pi_K(a)$ and $\tilde{b} = \pi_K(b)$.

Earlier in this section we mentioned that a curve with a Weierstrass equation is an elliptic curve if and only if the curve is non-singular. The reduced curve of E is non-singular if and only if the discriminant of $\tilde{E}$ is non-zero, but this is the same as $v_K(\Delta(E)) = 0$. Therefore if the discriminant of E with minimal Weierstrass equation is a unit in R_K, then the reduced curve $\tilde{E}$ is again an elliptic curve.

Proposition 3.26. *Let E be an elliptic curve defined over K. If both K and k_K have characteristic zero and the reduced curve $\tilde{E}$ defined over k_K is non-singular, then the reduction map induces a group homomorphism $\pi : E(K) \to \tilde{E}(k_K)$, which if restricted to the torsion subgroup of $E(K)$ is injective.*

In the proof of this proposition we need the Nagell-Lutz theorem.

Lemma 3.27. *Let the characteristic of K and k_K be zero. If the elliptic curve $E : y^2 = x^3 + ax + b$ with $a, b \in R_K$ is non-singular and $P = (x, y) \in E(K)$ is a point of finite order, then $x, y \in R_K$ and either $y = 0$ or $2v_K(y) \leq v_K(\Delta)$.*

Proof. This is a generalization of the theorem mentioned in [12, section II.5]. □

Proof of proposition 3.26. The reduction map induces a group homomorphism by [10, proposition VII.2.1].

Let $P \in E(K)_{\mathrm{tor}}$ be a point different from O. Then $P = (x : y : 1)$ for some $x, y \in K$. In fact $x, y \in R_K$ according to lemma 3.27. Since

$$\min\{v_K(x), v_K(y), v_K(1)\} = 0,$$

then $\pi(P) = (\pi_K(x) : \pi_K(y) : 1)$. Therefore $\pi(P) \neq O$. Hence the only point of finite order contained in the kernel of π is O. □

From now on we assume that K is complete with respect to the discrete valuation v_K. Let $q \in m_K$ be some non-zero element. We define the Tate curve E_q as the elliptic curve $y^2 + xy = x^3 + a(q)\,x + b(q)$, where $a(q)$ and $b(q)$ are certain series in $q\mathbb{Z}[[q]]$.

Proposition 3.28. *Let E_q be the Tate curve. The curve is defined over K, has j-invariant $j(E_q) = \frac{1}{q} + 744 + \ldots$ and there exists a Galois invariant injective homomorphism $\phi : \bar{K}^*/q^{\mathbb{Z}} \to E_q\left(\bar{K}\right)$.*

Proof. See [11, theorem V.3.1]. □

The statement of the following corollary is mentioned in [11, remark V.6.2].

Corollary 3.29. *The homomorphism $\phi : \bar{K}^*/q^{\mathbb{Z}} \to E_q\left(\bar{K}\right)$ restricted to the torsion subgroup is an isomorphism $\phi_{\mathrm{tor}} : \left(\bar{K}^*/q^{\mathbb{Z}}\right)_{\mathrm{tor}} \to E_q\left(\bar{K}\right)_{\mathrm{tor}}$.*

Proof. Since the homomorphism ϕ is injective, then ϕ_{tor} is also injective.

Assume that $P \in E_q\left(\bar{K}\right)_{\mathrm{tor}}$ is a point different from O. Denote the order of P by n. Write the restriction of ϕ_{tor} to the subgroup of points of order dividing n as ϕ_n. If the characteristic p of K is positive and divides n, then define n' such that p does not divide n' and $n = n'p^e$ with e a positive integer, otherwise define $n' = n$ and take e zero. Let $\omega \in \bar{K}$ be a n'-th primitive root of unity and $x \in \bar{K}$ be a zero of the polynomial $X^n - q \in K[X]$. Suppose that $\omega^i x^j \in q^{\mathbb{Z}}$, say $\omega^i x^j = q^m$ for some $m \in \mathbb{Z}$. In this case

$$q^j = \left(\omega^i x^j\right)^n = q^{mn},$$

so that $jv_K(q) = mnv_K(q)$. Therefore $j = mn$, because $v_K(q) > 0$. So $\omega^i = 1$, which can only be true if n' divides i. Hence $i \equiv 0 \mod n'$ and $j \equiv 0 \mod n$. Let y_{ij} be the image of $\omega^i x^j$ in $\bar{K}^*/q^{\mathbb{Z}}$. The elements y_{ij} have order dividing n and there are ${n'}^2 p^e$ such elements. On the other hand the group $E_q[n]$ contains at most ${n'}^2 p^e$ points, because $E_q[n']$ and $E_q[p^e]$ contain ${n'}^2$ and p^e points respectively by [10, corollary III.6.4] and $E_q[n] \cong E_q[n'] \times E_q[p^e]$. Thus ϕ_n is not only injective, but also surjective. Hence there exists a $y \in \bar{K}^*/q^{\mathbb{Z}}$ of order n such that $\phi_{\mathrm{tor}}(y) = P$. So ϕ_{tor} is also surjective. □

Corollary 3.30. *Let L be a Galois extension of K and $\bar{x} \in \bar{K}^*/q^{\mathbb{Z}}$. Then*

$$\bar{x} \in L^*/q^{\mathbb{Z}} \quad \Longleftrightarrow \quad \phi(\bar{x}) \in E_q(L).$$

Proof. Suppose that $\bar{x} \in L^*/q^{\mathbb{Z}}$, then $\sigma(\bar{x}) = \bar{x}$ for all $\sigma \in \mathrm{Gal}\left(\bar{K}/L\right)$. The homomorphism ϕ is Galois invariant. Therefore $\sigma(\phi(\bar{x})) = \phi(\sigma(\bar{x})) = \phi(\bar{x})$ for all $\sigma \in \mathrm{Gal}\left(\bar{K}/L\right)$. Hence $\phi(\bar{x}) \in E_q(L)$.

Assume that $\phi(\bar{x}) \in E_q(L)$, then $\sigma(\phi(\bar{x})) = \phi(\bar{x})$ for all $\sigma \in \mathrm{Gal}\left(\bar{K}/L\right)$. In particular $\phi(\sigma(\bar{x})) = \sigma(\phi(\bar{x})) = \phi(\bar{x})$, because ϕ is Galois invariant. Moreover $\sigma(\bar{x}) = \bar{x}$, since ϕ is injective. Hence $\bar{x} \in L^*/q^{\mathbb{Z}}$. □

Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. To this curve we assign an additional value, namely define $\gamma(E) = -\frac{1}{18}\frac{a}{b}$. It is important for the following proposition.

Proposition 3.31. *Let E be an elliptic curve defined over K. If the j-invariant $j(E) \notin R_K$, then there exists a $q \in m_K$ such that $j(E_q) = j(E)$. Moreover E and E_q are isomorphic over K if and only if $\gamma(E)$ is a square in K^*.*

Proof. See [11, theorem V.5.3]. □

We deduce from this proposition that the Tate curve provides an alternative to the reduced curve as a way to study the points of finite order on an elliptic curve. A combination of both methods will prove to be fruitful.

3.4 Galois theory of small field extensions

In this section we discuss the properties of field extension of degree two, three and six. To prepare for the next section, we need to know when an extension of degree six is Galois.

Proposition 3.32. *Let k be a field of characteristic different from two. If l is a degree two extension of k, then the extension is Galois.*

Proof. Let $x \in l \setminus k$ be any element and $F \in k[X]$ its minimum polynomial. The tower law of field extensions gives

$$[l : k(x)]\,[k(x) : k] = [l : k] = 2.$$

Thus $[k(x) : k] = 2$, because $[k(x) : k] > 1$ by assumption. So $l = k(x)$ and $\deg F = 2$. In fact l is a splitting field for F, because a degree one polynomial remains after dividing out a factor $X - x$ from F. Hence l is a finite normal extension of k. Suppose that F is not separable, then the characteristic p of k is positive and F is of the form [5, theorem 10.6]

$$F = \sum_{i=0}^{n} a_i X^{np}.$$

This is impossible, because $\deg F = 2$ and $p \neq 2$. So F is separable. Hence l is a finite, normal and separable extension of k, that is the extension is Galois. □

Proposition 3.33. *Let k be a field of characteristic different from three that contains a primitive third root of unity. If $F = X^3 - c \in k[X]$ is irreducible, then the splitting field for F is a Galois extension of degree three.*

Proof. Denote the splitting field for F by l. By definition it is normal. Suppose that F is not separable, then the characteristic p of k is positive and F is of the form [5, theorem 10.6]

$$F = \sum_{i=0}^{n} a_i X^{np},$$

but $np = 3$ and $p \neq 3$. So F is separable. Therefore l is also separable. Hence l is a Galois extension of k.

The degree of the extension l of k is three, because $[l : k] \geq \deg F = 3$ and for $x \in l$ a zero of F

$$F = (X - x)\,(X - \omega x)\left(X - \omega^2 x\right)$$

where $\omega \in k$ is a primitive third root of unity. □

Proposition 3.34. *Let k be a field of characteristic different from two and three that contains a primitive third root of unity, l be a field extension of k of degree two and m be the splitting field for an irreducible polynomial $F = X^3 - c \in l[X]$. If m is not a Galois extension of k, then $c \notin k$ and $Y^3 - G(0)$ is irreducible over l where G is the minimum polynomial of c.*

We need the following lemma to prove the proposition.

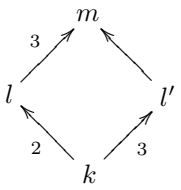
Lemma 3.35. *Let k be a field. If l_1 and l_2 are normal extensions of k, then the smallest field m containing both l_1 and l_2 is also a normal extension of k.*

Proof. For $i = 1, 2$ there exists subsets $S_i \subset k[X]$ such that l_i is a splitting field for S_i by [5, theorem 9.1]. Define $S = S_1 \cup S_2$.

Let $f \in S$. So $f \in S_i$ for some i. Therefore f splits over l_i, which is a subfield of m. Hence every $f \in S$ splits over m. Let m' be the splitting field for S. Recall that l_i is a splitting field for S_i and that every $f \in S_i$ also splits over m'. Therefore $l_i \subset m'$. Since m is the smallest field containing both l_1 and l_2, it follows that $m = m'$. Therefore m is the splitting field of S. Hence m is a normal extension of k by [5, theorem 9.1]. □

Proof of proposition 3.35. The extension m of l is Galois by proposition 3.33 and the extension l of k is Galois by proposition 3.32. So the extension m of k is separable [5, theorem 10.3].

Suppose that $c \in k$, then $F \in k[X]$ and F is also irreducible over k. Define the splitting field for F over k by l'. This extension is Galois of degree three by proposition 3.33. The following diagram shows the extensions with their degrees.



The field m is the smallest field that contains both l and l' as follows from the tower law. In particular both l and l' are normal extensions of k. Thus m is also a normal extension of k by lemma 3.35. So m is a Galois extension of k.

Suppose that $c \notin k$ and that $Y^3 - G(0)$ is reducible over l, where G is the minimum polynomial of c. Let $d \in m$ be a zero of F. Notice that $l = k(c)$ and $m = k(d)$. Denote the minimum polynomial of d over k by $F' \in k[X]$, then $\deg F' = [m : k] = 6$. Recall that F is the minimum polynomial of d over l, so that $F' = FH$ for some monic polynomial $H \in l[X]$ of degree three. Since l is a Galois extension of k, then $\mathrm{Gal}(l/k) = \{\mathrm{id}, \sigma\}$. The automorphism $\sigma : l \to l$ extends an automorphism of $l[X]$. Moreover $l[X]$ is a unique factorization domain, F is irreducible over l and

$$FH = F' = \sigma(F') = \sigma(FH) = \sigma(F)\,\sigma(H).$$

Therefore $\sigma(F) = H$, because $\sigma(c) \neq c$. Notice that $G = (X - c)(X - \sigma(c))$. So $c\sigma(c) = G(0)$. There is an $y \in l$ such that $y^3 = G(0)$ by assumption. Now

$$H = X^3 - \sigma(c) = X^3 - \frac{y^3}{d^3} = \left(X - \frac{y}{d}\right)\left(X - \omega\frac{y}{d}\right)\left(X - \omega^2\frac{y}{d}\right),$$

where $\omega \in k$ is a primitive third root of unity. Thus F and H split over m, so that F' splits over m. Furthermore $[m : k] = \deg F'$. Hence m is the splitting field of F', that the extension m of k is normal. In particular it is Galois. □

3.5 Branched covering space of an elliptic curve

Recall that in proposition 2.26 we proved that there exists a branched covering space of an elliptic curve with three sheets and a single ramification point using the theory of algebraic topology and Riemann surfaces. The theory in this chapter allows us to give an explicit example of this case.

Let k be an algebraically closed field of characteristic different from two and three. Let E and E' be elliptic curves over k. Suppose that $\phi : E' \to E$ is an isogeny of degree two. From proposition 3.32 we deduce that the extension induced by ϕ is separable and the following lemma tells us that there exists a point T' of order two in the kernel of ϕ.

Lemma 3.36. *The extension induced by ϕ is separable if and only if there exists a point $T' \in E'(k) \in \ker \phi$ of order two.*

Proof. Suppose that the extension is separable, then

$$\left|\ker \phi^{-1}\right| = \deg_s \phi = \deg \phi = 2$$

where the first equality follows from [10, theorem III.4.10]. So there exists a point $S' \in E'(k)$ different from O'. It has order two, otherwise $2S'$ is yet another point in $\ker \phi$ which implies that $\left|\ker \phi^{-1}\right| > 2$. Therefore T' exists.

Suppose that T' exists, then

$$\deg \phi = 2 \leq \left|\ker \phi^{-1}\right| = \deg_s \phi \leq \deg \phi$$

where the third relation again follows from [10, theorem III.4.10]. Therefore $\deg_s \phi = \deg \phi$, that is ϕ induces a separable extension. □

Let $D' = 2T' - 2O'$ be a divisor on E' of degree zero. In particular

$$2T' = O' = 2O'$$

in the group $E'(k)$. Therefore D' is a principal divisor by [10, corollary III.3.5], that is $D' = \operatorname{div} f$ for some $f \in k(E')^*$. Define $F = X^3 - f \in k(E')[X]$, which is irreducible by the following lemma.

Lemma 3.37. *The polynomial $F = X^3 - f$ is irreducible over $k(E')$.*

Proof. Assume that F is reducible, then F has a zero g, that is $g^3 = f$. So

$$2\tilde{T} - 2\tilde{O} = \operatorname{div} f = 3 \operatorname{div} g,$$

however three does not divide two. Hence F is irreducible. □

Define the curve C over k such that $k(C)$ is the splitting field of F over $k(E')$. Denote the morphism corresponding to the inclusion of fields by $\chi : C \to E'$. Proposition 3.33 implies that $k(C)$ is a degree three Galois extension of $k(E')$.

Proposition 3.38. *Let $P \in C$ be a point. The morphism $\chi : C \to E'$ is ramified at P if and only if $\chi(P) \in \{O', T'\}$. Moreover the ramification index at P is three, if the morphism χ is ramified at P.*

Proof. Let $P \in C$ be a point such that $\chi(P) = T'$. Let $t_{T'}$ be a uniformizer of the discrete valuation ring at T'. Then

$$3v_P(g) = v_P\left(g^3\right) = v_P(f) = 2v_P(t_{T'}),$$

where the last equality follows from $v_{T'}(f) = 2$. Thus three divides $v_P(t_{T'})$, so $v_P(t_{T'}) \geq 3$. In fact $v_P(t_{T'}) = 3$, because

$$v_P(t_{T'}) \leq \sum_{Q \in \chi^{-1}(T')} v_Q(t_{T'}) = \deg \chi = [k(C) : k(E')] = 3$$

by [10, proposition II.2.6]. Thus $\chi^{-1}(T') = \{P\}$. From the same argument also follows that $\chi^{-1}(O') = \{P'\}$ and $v_{P'}(t_{O'}) = 3$ for $t_{O'}$ a uniformizer of the discrete valuation ring at O'. Hence if $\chi(P) \in \{O', T'\}$, then χ is ramified at P with ramification index three.

Let $P \in C$ be a point such that $\chi(P) = Q \notin \{O', T'\}$. Denote the discrete valuation ring at Q by R_Q and consider the completion $\hat{R}_Q$ thereof. Recall that $k(C)$ is the splitting field of $F = X^3 - f$ over $k(E')$ and that $\operatorname{div} f = 2T' - 2O'$. Thus $\frac{dF}{dX} = 3X^2$ and $v_Q(f) = 0$. Let $g_0 \in R_Q$ be the constant function such that $g_0(Q)$ is a third root of $f(Q)$ in k. In particular $g_0(Q) \neq 0$, since $f(Q) \neq 0$. From Hensel's lemma follows that there exists a $g \in \hat{R}_Q$ such that $F(g) = 0$. Thus $k(C) \subset \widehat{k(E')}_Q$, because $k(C) = k(E')(g)$. The morphism χ induces an inclusion from R_Q to the discrete valuation ring R_P at P. From proposition 3.5 follows that $v_P(t_Q) = 1$, where t_Q is a uniformizer of R_Q. Hence χ is unramified at P. □

In the proposition we proved that the morphism $\chi : C \to E'$ is ramified at two points. Denote these points by T'' and O'' such that $\chi(T'') = T'$ and $\chi(O'') = O'$.

We compose the morphism $\chi : C \to E'$ with the morphism $\phi : E' \to E$ to obtain a morphism $\psi : C \to E$. The morphism ϕ is unramified, because $k(E')$ is a separable extension of $k(E)$ and [10, theorem III.4.10]. The ramification index of ψ at a point $P \in C$ is fixed by

$$e_\psi(P) = e_\chi(P)\, e_\phi(\chi(P)).$$

Hence ψ is ramified in T'' and O'' with index three. At all other points on C the morphism ψ is unramified.

Proposition 3.39. *The curve C has genus three.*

Proof. The genus of an elliptic curve is one, that is $g_E = 1$. According to the Hurwitz formula

$$2(g_C - 1) = 2 \deg \psi (g_E - 1) + \sum_{P \in C} (e_\psi(P) - 1).$$

Since ψ only ramifies at two points on C and the ramification index at these points is three, then the genus of C satisfies $2(g_C - 1) = 4$. Hence $g_E = 3$. □

We choose the elliptic curve E' and E and the isogeny $\phi : E' \to E$ as in [10, example III.4.5]. Let k be an algebraically closed field of characteristic different from two and three. Define the elliptic curve $E' : \eta^2 = \xi^3 + a\xi^2 + b\xi$ over k with $a, b \in k$ such that $b \neq 0$ and $a^2 \neq 4b$. Let $E : y^2 = x^3 - 2ax^2 + \left(a^2 - 4b\right) x$ be another elliptic curve over k. In this case the isogeny of degree two $\phi : E' \to E$ is defined as

$$(\xi, \eta) \longmapsto \left(\frac{\eta^2}{\xi^2}, \frac{\eta\left(b - \xi^2\right)}{\xi^2} \right).$$

The point $T' = (0, 0)$ on E' has order two and lies in the kernel of ϕ.

Lemma 3.40. *The coordinate function $\xi \in k(E')$ has divisor $D' = 2T' - 2O'$.*

Proof. Let $P \in E'$ be any point not equal to O' such that $\xi(P) = 0$. In fact $P = T'$, because $\eta(P) = 0$ as follows from the equation of E'. Notice that T' is a simple point of E' and the line $\eta = 0$ is not parallel to the tangent line $\xi = 0$ of E' in T'. Therefore is η a uniformizer in the point T' by [4, theorem 3.1]. From $\left(\xi^2 + a\xi + b\right)(T') = b \neq 0$ and

$$\xi = \frac{\xi^3 + a\xi^2 + b\xi}{\xi^2 + a\xi + b} = \frac{\eta^2}{\xi^2 + a\xi + b}$$

follows that $v_{T'}(\xi) = 2$. Moreover O' is the only point at infinity and a principal divisor has degree zero by [4, proposition 8.1]. Hence $\operatorname{div} \xi = 2T' - 2O'$. □

Recall that we defined the curve C such that the function field $k(C)$ is the splitting field of $F = X^3 - f$ over $k(E')$. In particular f is any function such that $\operatorname{div} f = D'$. By the previous lemma we may as well take $f = \xi$. Let s be a zero of F, that is $s^3 = \xi$. Define $t = \frac{\eta}{s}$.

Lemma 3.41. *The function field of the curve C is equal to $k(s, t)$.*

Proof. The function field of E' is equal to $k(\xi, \eta)$ by [10, corollary III.3.1.1]. The function field of C is defined as the splitting field of F over $k(E')$, which is $k(E')(s)$ by proposition 3.33. Hence $k(C) = k(\xi, \eta, s) = k(s, t)$. □

We derive the equation for the curve C from the curve E as follows

$$t^2 = \frac{\eta^2}{s^2} = \frac{\xi^3 + a\xi^2 + b\xi}{s^2} = \frac{s^9 + as^6 + bs^3}{s^2} = s^7 + as^4 + bs.$$

The morphism $\chi : C \to E'$ is given by $(s, t) \mapsto \left(s^3, st\right)$.

Proposition 3.42. *The extension $k(C)$ of $k(E)$ is Galois. Moreover the Galois group is isomorphic to S_3.*

Proof. The minimum polynomial of ξ is $G = X^2 + (a - x) X + b$, because

$$x = \frac{\eta^2}{\xi^2} = \frac{\xi^3 + a\xi^2 + b\xi}{\xi^2} = \frac{\xi^2 + a\xi + b}{\xi}$$

and $\xi \notin k(E)$ since otherwise $k(E) = k(E')$. From proposition 3.34 follows that $k(C)$ is a Galois extension of $k(E)$, because $G(0) = b \in k$ and that k is

algebraically closed. In fact $k(C)$ is the splitting field of $F' = X^6 + (a-x)X^3 + b$ over $k(E)$, since

$$F = (X-s)(X-\omega s)\left(X-\omega^2 s\right)\left(X-\frac{c}{s}\right)\left(X-\omega\frac{c}{s}\right)\left(X-\omega^2\frac{c}{s}\right)$$

where $\omega \in k$ is a primitive third root of unity and $c \in k$ is a cubic root of b. There exist $\sigma, \tau \in \mathrm{Gal}(k(C)/k(E))$ such that $\sigma(s) = \omega s$ and $\tau(s) = \frac{c}{s}$. These elements generate a subgroup of order at least six, but the Galois group has order six. Therefore σ and τ generate $\mathrm{Gal}(k(C)/k(E))$. Moreover this group is non-abelian, since $\sigma \circ \tau(s) = \omega^2 \frac{c}{s} \neq \omega \frac{c}{s} = \tau \circ \sigma(s)$. So $\mathrm{Gal}(k(C)/k(E)) \cong S_3$. □

Let H be the subgroup of $\mathrm{Gal}(k(C)/k(E))$ generated by τ and D be the curve over k such that the function field is $k(C)^H$. Since $y = \frac{\eta\left(b-\xi^2\right)}{\xi^2}$, then

$$\tau(t) = \sigma\left(\frac{\eta}{s}\right) = y\frac{\frac{b^2}{\xi^2}}{b-\frac{b^2}{\xi^2}}\frac{s}{c} = -y\frac{b}{b-\xi^2}\frac{s}{c} = -\frac{b\eta}{cs^5} = -\frac{c^2 t}{s^4},$$

because $\tau(s) = \frac{c}{s}$ and $\xi = s^3$. Define $\alpha = s + \frac{c}{s}$ and $\beta = \frac{t}{s^2}\left(s - \frac{c}{s}\right)$. Clearly α is invariant under τ, that is $\alpha \in k(D)$. Also $\beta \in k(D)$, because $t\left(1-\frac{c^2}{s^4}\right)$ is invariant under τ and $\beta = \frac{t}{\alpha}\left(1-\frac{c^2}{s^4}\right)$. Let $\lambda : C \to D$ be the morphism corresponding to the inclusion of $k(D)$ in $k(C)$.

Lemma 3.43. *The function field of the curve D is equal to $k(\alpha, \beta)$.*

Proof. Recall that $\alpha, \beta \in k(D)$. So $k(\alpha, \beta)$ is a subfield of $k(D)$. The element s is a zero of $X^2 - \alpha X + c$, because $\alpha = s + \frac{c}{s}$ implies $s^2 - \alpha s + c = 0$. Assume that this polynomial is reducible, then $s \in k(\alpha, \beta)$ and also $t = \frac{\beta s^2}{s - \frac{c}{s}} \in k(\alpha, \beta)$, that is $k(\alpha, \beta) = k(D) = k(C)$, which contradicts that $k(C)$ is a degree two extension of $k(D)$. Therefore $X^2 - \alpha X + c$ is the minimum polynomial of s over $k(\alpha, \beta)$. From the tower law now follows

$$[k(D) : k(\alpha, \beta)] = \frac{[k(C) : k(\alpha, \beta)]}{[k(C) : k(D)]} = \frac{2}{2} = 1.$$

Hence $k(D) = k(\alpha, \beta)$. □

We derive the equation for the curve D from the curve C like before

$$\begin{aligned}\beta^2 &= \frac{t^2}{s^4}\left(s-\frac{c}{s}\right)^2 \\ &= \left(s^3 + a + \frac{b}{s^3}\right)\left(s^2 - 2c + \frac{c^2}{s^2}\right) \\ &= \left(\alpha^3 - 3c\alpha + a\right)\left(\alpha^2 - 4c\right).\end{aligned}$$

In a similar way we describe the inclusion of $k(E)$ in $k(D)$.

$$\begin{aligned}x &= \frac{\eta^2}{\xi^2} = \frac{t^2}{s^4} = s^3 + a + \frac{b}{s^3} = \alpha^3 - 3c\alpha + a \\ y &= \frac{\eta}{\xi^2}\left(b-\xi^2\right) = -\frac{t}{s^2}\left(s-\frac{c}{s}\right)\left(s^2 + c + \frac{c^2}{s^2}\right) = -\beta\left(\alpha^2 - c\right)\end{aligned}$$

Therefore define the corresponding morphism $\rho : D \to E$ as

$$(\alpha, \beta) \mapsto \left(\alpha^3 - 3c\alpha + a, -\beta\left(\alpha^2 - c\right)\right).$$

Proposition 3.44. *The curve D is irreducible over k.*

Proof. Let $G = Y^2 - \left(X^3 - 3cX + a\right)\left(X^2 - 4c\right) \in k[X, Y]$. If G is irreducible, then (G) is a prime ideal, because $k[X, Y]$ is a unique factorization domain. Moreover D is then irreducible by Hilbert's Nullstellensatz.

The zeros of $X^3 - 3cX + a$ are all different, because the discriminant is $4(-3c)^3 + 27a^2 = 27\left(a^2 - 4b\right)$ and $a^2 \neq 4b$ by definition. Also the zeros of $X^2 - 4c$ are different, because $c \neq 0$. Suppose that the two polynomials have a zero in common. Denote this zero by x. Since

$$X^3 - 3cX + a = X\left(X^2 - 4c\right) + cX + a,$$

then $cx + a = 0$. Together with $x^2 = 4c$ this gives $a^2 = c^2x^2 = 4c^3 = 4b$, which contradicts that $a^2 \neq 4b$. Hence all the zeros of $\left(X^3 - 3cX + a\right)\left(X^2 - 4c\right)$ are different.

Consider $k[X, Y]$ as $R[Y]$ with $R = k[X]$. Let x be a zero of $X^2 - 4c$, then $X - x$ is prime in R. Furthermore $X - x$ divides $\left(X^3 - 3cX + a\right)\left(X^2 - 4c\right)$ only once. Thus G is an Eisenstein polynomial. Hence G is irreducible. □

The curve D has a unique point at infinity. Denote this point by ∞.

Lemma 3.45. *The coordinate function $\alpha, \beta \in k(D)$ have divisors*

$$\begin{aligned}\operatorname{div}\alpha &= \left(0, 2\sqrt{-ac}\right) + \left(0, -2\sqrt{-ac}\right) - 2\infty \\ \operatorname{div}\beta &= (\alpha_1, 0) + \ldots + (\alpha_5, 0) - 5\infty\end{aligned}$$

where the α_i's are the zeros of $G = \left(X^3 - 3cX + a\right)\left(X^2 - 4c\right)$ in k.

Proof. Let $P \in D$ be any point different from infinity. The line tangent to D in P is given by $-\frac{dG}{dX}(\alpha(P))(X - \alpha(P)) + 2\beta(P)(Y - \beta(P))$. Recall from the proof of proposition 3.44 that G does not have double zeros. So if $\alpha(P)$ is zero, then $\frac{dG}{dX}(\alpha(P))$ is non-zero.

Suppose that $\alpha(P) = 0$, then $\beta(P)^2 = -4ac$. In this case the line X through P is not tangent to D. Thus α is a uniformizer at P by [4, theorem 3.1]. So $v_P(\alpha) = 1$. A principal divisor has degree zero. Hence $\operatorname{div}\alpha$ is as claimed.

Assume that $\beta(P) = 0$, then $\alpha(P)$ is zero of G. Now the line Y through P is not tangent to D. Therefore β is a uniformizer at P. So $v_P(\beta) = 1$. Hence $\operatorname{div}\beta$ is also as claimed. □

Lemma 3.46. *The coordinate function $x, y \in k(E)$ have divisors*

$$\begin{aligned}\operatorname{div} x &= 2(0,0) - 2O \\ \operatorname{div} y &= (0,0) + \left(a + 2\sqrt{b}, 0\right) + \left(a - 2\sqrt{b}, 0\right) - 3O.\end{aligned}$$

Proof. The proof is similar to the proofs of lemmas 3.40 and 3.45. □

Proposition 3.47. *The curve D has genus two. The morphism ρ branches only at infinity, where the ramification index is three.*

Proof. The ramification index of a point $P \in D$ is defined as $e_\rho(P) = v_P(r)$, where r is a uniformizer of the discrete valuation ring at $\rho(P)$ on E. From lemma 3.46 follows that $\frac{x}{y}$ is a uniformizer at $O = \rho(\infty)$. Now

$$\frac{x}{y} = -\frac{\alpha^3 - 3c\alpha + a}{\beta(\alpha^2 - c)} = -\frac{\alpha}{\beta}\frac{1 - \frac{3c}{\alpha^2} + \frac{a}{\alpha^2}}{1 - \frac{c}{\alpha^2}}.$$

The factors $1 - \frac{3c}{\alpha^2} + \frac{a}{\alpha^2}$ and $1 - \frac{c}{\alpha^2}$ evaluate to one at ∞ by lemma 3.45. So

$$e_\rho(\infty) = v_\infty\left(\frac{x}{y}\right) = v_\infty\left(\frac{\alpha}{\beta}\right) = v_\infty(\alpha) - v_\infty(\beta) = -2 + 5 = 3.$$

Hence the ramification index of ρ at ∞ is three.

The curve C has genus three by proposition 3.39. First apply the Hurwitz formula to the morphism $\lambda : C \to D$. Then

$$4 = 2(g_C - 1) = 2\deg\lambda(g_D - 1) + \sum_{P \in C}(e_\lambda(P) - 1) \geq 4(g_D - 1),$$

where $\deg\lambda = [k(C) : k(D)] = 2$ by construction of D. Last apply the Hurwitz formula to the morphism $\rho : D \to E$. Then

$$2(g_D - 1) = 2\deg\rho(g_E - 1) + \sum_{P \in D}(e_\rho(P) - 1) = \sum_{P \in D}(e_\rho(P) - 1) \geq 2,$$

where the inequality follows $e_\rho(\infty) = 3$. Combine the two relations to obtain $1 \geq g_D - 1 \geq 1$, that is $g_D = 2$. Moreover $\sum_{P \in D}(e_\rho(P) - 1) = e_\rho(\infty) - 1$, that is $e_\rho(P) = 1$ for all $P \neq \infty$.

Hence the curve D has genus two. The morphism $\rho : D \to E$ is unramified at all points except infinity. At infinity the ramification index is three. □

Chapter 4

Branched covering space of a discriminant

Let k be an algebraically closed field of characteristic zero. We will construct branched covering spaces of some elliptic curve C, but first we will derive some properties of this curve.

We define the elliptic curve $C : 4a^3 + 27b^2 = 1$ over k. The curve C is irreducible, because of proposition 3.20, so the function field $K = k(C)$ is well-defined. Moreover this curve is non-singular, thus for all points $P \in C$ there is a discrete valuation v_P on K. The zeros and poles of the coordinate functions $a, b \in K$ are given by the following lemma.

Lemma 4.1. *Let $a, b \in K$ be the coordinate functions of C. Then*

$$\operatorname{div} a = \left(0, \frac{1}{9}\sqrt{3}\right) + \left(0, -\frac{1}{9}\sqrt{3}\right) - 2O_C$$
$$\operatorname{div} b = \left(\frac{1}{2}\sqrt[3]{2}, 0\right) + \left(\frac{1}{2}\sqrt[3]{2}\zeta, 0\right) + \left(\frac{1}{2}\sqrt[3]{2}\zeta^2, 0\right) - 3O_C,$$

where $\zeta^2 + \zeta + 1 = 0$.

Proof. Let $P \in C$ be a point such that $P \neq O_C$. If $P = (a_P, b_P)$, then $a_P = a(P)$ and $b_P = b(P)$. If $a_P \neq 0$, then $v_P(a) = 0$ by definition of the local ring at P. If $b_P \neq 0$, then $v_P(b) = 0$.

Suppose that $a_P = 0$, then b_P is a root of $b_P^2 = \frac{1}{27}$. Moreover $a - a_P = a$ is a uniformizer, because of [4, theorem 3.1] and $b_P \neq 0$. Hence $v_P(a) = 1$ for $P = \left(0, \pm\frac{1}{9}\sqrt{3}\right)$.

Assume that $b_P = 0$, then a_P is a root of $a_P^3 = \frac{1}{4}$. Thus $b - b_P = b$ is a uniformizer, because $a_P \neq 0$. Hence $v_P(b) = 1$ for $P = \left(\frac{1}{2}\sqrt[3]{2}\zeta^n, 0\right)$ with $\zeta^3 = 1$.

The point $O_C \in C$ is the only point at infinity. The $\operatorname{div} f$ has degree zero for all $f \in K^*$, because of [4, proposition 8.1]. Therefore a and b have a pole of order two and three respectively at infinity. □

We define another curve $E : y^2 = x^3 + ax + b$ with $a, b \in K$ the coordinate functions of C. The curve C is defined such that the discriminant of E is one. Therefore E is an elliptic curve.

A finite field extension L of K corresponds to a curve D over k by proposition 3.11. The inclusion of K into L induces a surjective morphism $\psi : D \to C$. Now D is a branched covering space of C by definition. In the following sections we analyse several spaces of this type.

4.1 Adjoin both x and y coordinates for all points

Let $m \in \mathbb{Z}_{\geq 2}$ and define $L_m = K(E[m])$. This is an Galois extension of K by proposition 3.21. Denote the curve corresponding to L_m by D_m. The inclusion of K into L_m gives the surjective morphism $\psi_m : D_m \to C$.

Proposition 4.2. *If $P \in D_m$ with $\psi_m(P) \neq O_C$, then ψ_m is unramified at P.*

Proof. Let $Q = \psi_m(P)$ be the image of P on C. Denote the local ring of D_m at P by $R_{m,P}$ and the local ring of C at Q by R_Q. The morphism ψ_m induces an inclusion $R_Q \subset R_{m,P}$ of local rings, such that $m_Q \subset m_{m,P}$. Corollary 3.9 implies that $\hat{L}_{m,P}/\hat{K}_Q$ is Galois with Galois group $\mathbb{Z}/n\mathbb{Z}$ for some n, where $\hat{L}_{m,P}$ and $\hat{K}_Q$ are the quotient fields of the completed rings $\hat{R}_{m,P}$ and $\hat{R}_Q$. The ramification index of ψ_m at P is $n = v_P(t_Q)$ for a uniformizer t_Q of R_Q.

The coordinate functions $a, b \in K$ are contained in R_Q by lemma 4.1 and the discriminant $\Delta(E) = 1$. So the Weierstrass equation of E is minimal. The reduced curve $\tilde{E}$ is well-defined and non-singular. Moreover the reduction map

$$\pi : E\left(\hat{L}_{m,P}\right) \to \tilde{E}(k)$$

is a group homomorphism by proposition 3.26. The coordinates of all points in $E[m]$ are contained in L_m. So $E[m]$ is a subgroup of $E(L_m)$. Hence the reduction map restricts to an isomorphism $\pi : E[m] \to \tilde{E}[m]$. This map is Galois equivariant by corollary 3.24. Let $\sigma \in \mathrm{Gal}\left(\hat{L}_{m,P}/\hat{K}_Q\right)$. Then

$$\pi \circ \sigma(R) = \tilde{\sigma} \circ \pi(R) = \pi(R)$$

for all $R \in E[m]$, because k algebraically closed implies $\tilde{\sigma} = \mathrm{id}_k$. Therefore $\sigma(R) = R$. So σ fixes the coordinates of all $R \in E[m]$. Hence σ is the identity on $\hat{L}_{m,P}$. Thus $n = 1$, that is ψ_m is unramified at P. □

Proposition 4.3. *The morphism $\psi_2 : D_2 \to C$ does not branch above O_C.*

Proof. Let $P \in D_2$ be such that $\psi_2(P) = O_C$. Denote the local ring of D_2 at P by $R_{2,P}$ and the local ring of C at O_C by R_{O_C}. The inclusion $R_{O_C} \subset R_{2,P}$ of local rings such that $m_{O_C} \subset m_{2,P}$ is induced by the morphism ψ_2. The three points of order two have x-coordinates that are the roots of $x^3 + ax + b = 0$ and y-coordinates zero. Assume that the roots of this equation are $x_1, x_2, x_3 \in \hat{K}_{O_C}$, then $L_2 = K(x_1, x_2, x_3) \subset \hat{K}_{O_C}$. Proposition 3.5 implies that $\hat{K}_{O_C} = \hat{L}_{2,P}$. So a uniformizer $t_{O_C} \in R_{O_C}$ is also a uniformizer of $R_{2,P}$. Hence ψ_2 is unramified at P.

It remains to show that the roots x_i are elements in $\hat{K}_{O_C}$. Lemma 4.1 implies that $t = \frac{a}{b}$ is a uniformizer at O_C. Moreover $u = bt^3$ is a unit in R_{O_C}. In fact the equation $4a^3 + 27b^2 = 1$ now implies

$$t^6 = 4\left(at^2\right)^3 + 27\left(bt^3\right)^2 = 4u^3 + 27u^2 = u^2(4u + 27).$$

Define $\xi = t^{-1}x$. Then $x^3 + ax + b = 0$ is equivalent to $\xi^3 + u\xi + u = 0$. The main tool is to inductively compute the root of a polynomial over $\hat{R}_{O_C}/t^n$ for $n = 0, 1, 2, \ldots$ up to some finite number such that Hensel's lemma may be used. This procedure and that u is a unit gives $u \equiv -\frac{27}{4} + \frac{4}{729}t^6 \mod t^{12}$. Let $F = X^3 + uX + u$, then $\frac{dF}{dX} = 3X^2 + u$. If $\xi' = 3 - \frac{64}{59049}t^6$, then $F(\xi') \equiv 0 \mod t^{12}$ and $\frac{dF}{dX}(\xi') \equiv \frac{81}{4} \mod t$, so Hensel's lemma implies there exists a $\xi \in \hat{R}_{O_C}$ such that $F(\xi) = 0$ and $\xi \equiv \xi' \mod t^{12}$. Hence $F = (X - \xi)\left(X^2 + \xi X + u + \xi^2\right)$. The latter factor has discriminant

$$\Delta = \Delta\left(X^2 + \xi X + u + \xi^2\right) = -3\xi^2 - 4u \equiv -\frac{16}{6561}t^6 \mod t^{12}.$$

Let $G = Y^2 - \Delta t^{-6}$, then $\eta' = i\frac{4}{81}$ gives $G(\eta') \equiv 0 \mod t^6$ and $\frac{dG}{dY} \equiv i\frac{8}{81} \mod t$. Thus there is an $\eta \in \hat{R}_{O_C}$ such that $G(\eta) = 0$ and $\eta \equiv \eta' \mod t^6$. Hence $F = (X - \xi)\left(X + \frac{\xi + \eta t^3}{2}\right)\left(X + \frac{\xi - \eta t^3}{2}\right)$ with each of the roots in $\hat{K}_{O_C}$. □

We know from proposition 4.2 that ψ_2 does not branch above any point on C different from O_C. The previous proposition says that ψ_2 also does not branch above O_C. According to proposition 3.18 the genus of D_2 must be one. Hence D_2 is an elliptic curve and the morphism $\psi_2 : D_2 \to C$ is unramified.

Proposition 4.4. *If $P \in D_3$ such that $\psi_3(P) = O_C$, then ψ_3 is ramified at P with ramification index two.*

Proof. Given the local ring $R_{3,P}$ of D_3 at P and the local ring R_{O_C} of C at O_C there exists an inclusion $R_{O_C} \subset R_{3,P}$ of local rings such that $m_{O_C} \subset m_{3,P}$ is induced by the morphism ψ_3. The element $t = \frac{a}{b}$ is a uniformizer at O_C and $b = ut^{-3}$ for some unit $u \in R_{O_C}$ such that $t^6 = u^2(4u + 27)$. The x-coordinates of points of order three satisfy the following equation $0 = 3x^4 + 6ax^2 + 12bx - a^2$ from [12, §II.1], which changes into $0 = \xi^4 + 2u\xi^2 + 4u\xi - \frac{1}{3}u^2$ for $\xi = tx$.

Let L be the splitting field for $F = X^4 + 2uX^2 + 4uX - \frac{1}{3}u^2 \in K[X]$. In fact $L = K(\alpha_1, \alpha_2, \alpha_3)$ with α_i^2 the three roots of the cubic resolvent [5, §14.4]

$$G = \left(X - \alpha_1^2\right)\left(X - \alpha_2^2\right)\left(X - \alpha_3^2\right) = X^3 + 4uX^2 + \frac{16}{3}u^2X - 16u^2$$

such that $\alpha_1\alpha_2\alpha_3 = -4u$. Lets introduce a new variable $Y = X + \frac{4}{3}u$ and write G in terms of Y. This reveals that

$$G = Y^3 - \frac{64}{27}u^3 - 16u^2 = Y^3 - \frac{16}{27}t^6,$$

therefore $\alpha_i^2 = -\frac{4}{3}u + \frac{2\sqrt[3]{2}}{3}t^2\omega^i$ with $\omega^2 + \omega + 1 = 0$. Moreover $\alpha_i^2 \in R_{O_C}^*$, since $v_{O_C}\left(-\frac{4}{3}u\right) = 0$ and $v_{O_C}\left(\frac{2\sqrt[3]{2}}{3}t^2\omega^i\right) = 2$. Thus $\alpha_i \in \hat{R}_{O_C}$ such that $\alpha_i \equiv 3 \mod t$ by Hensel's lemma, so $L \subset \hat{K}_{O_C}$. The roots ξ_i of F are units in $\hat{R}_{O_C}$, because $\alpha_i \in \hat{R}_{O_C}$,

$$\xi_1 = \frac{1}{2}(+\alpha_1 + \alpha_2 + \alpha_3)$$
$$\xi_2 = \frac{1}{2}(+\alpha_1 - \alpha_2 - \alpha_3)$$
$$\xi_3 = \frac{1}{2}(-\alpha_1 + \alpha_2 - \alpha_3)$$
$$\xi_4 = \frac{1}{2}(-\alpha_1 - \alpha_2 + \alpha_3)$$

and $\xi_1 \equiv \frac{9}{2} \mod t^4$, $\xi_i \equiv -\frac{3}{2} + \frac{\sqrt[3]{2}}{9}\omega^{i-2}t^2 \mod t^4$ for $i = 2, 3, 4$.

The y-coordinates are solutions of the equation $y^2 = x^3 + ax + b$, which changes into $\eta^2 = t\left(\xi^3 + u\xi + u\right)$ for $\eta = t^2 y$. The element $\xi_i^3 + u\xi_i + u \in \hat{R}_{O_C}$ is a unit for $i = 1$ and is of fourth order for $i = 2, 3, 4$, because $\xi^3 + u\xi + u \equiv (\xi - 3)\left(\xi + \frac{3}{2}\right)^2 \mod t^6$. Define $H_i = Y^2 - t\left(\xi_i^3 + u\xi_i + u\right)$. It is irreducible over $\hat{K}_{O_C}$, otherwise it has a root $\eta_i \in \hat{K}_{O_C}$ and

$$0 \equiv v\left(\eta_i^2\right) \equiv v\left(t\left(\xi_i^3 + u\xi_i + u\right)\right) \equiv 1 \mod 2.$$

From corollary 3.9 follows that there exists a uniformizer $t_{3,P} \in \hat{R}_{3,P}$ and an integer $n \in \mathbb{Z}_{>0}$ such that $t_{3,P}^n = t$. In fact $n > 1$ since $L_3 \not\subset \hat{K}_{O_C}$. Thus ψ_3 is ramified at P. Moreover n is even, otherwise let $m \in \mathbb{Z}$ be such that $n = 2m + 1$, then $Z^2 - t_{3,P}\left(\xi_i^3 + u\xi_i + u\right)$ with $Y = t_{3,P}^m Z$ is again irreducible which contradicts that the y-coordinates are part of L_3. Let $m \in \mathbb{Z}$ be such that $n = 2m$. Proposition 3.6 implies that $\hat{R}_{O_C} = k\left[[t]\right]$ and $\hat{R}_{3,P} = k\left[[t_{3,P}]\right]$. Define $R_M = k\left[[s]\right]$, then $\hat{R}_{O_C} \subset R_M \subset \hat{R}_{3,P}$ and $\hat{m}_{O_C} \subset m_M \subset \hat{m}_{3,P}$ via $t \mapsto s^2$ and $s \mapsto t_{3,P}^m$. Now the polynomial $Y^2 - \xi_1^3 - u\xi_1 - u$ does have a solution $\tilde{\eta}_1 \in R_M$ by Hensel's lemma and $\eta_1 = s\tilde{\eta}_1$ is a root of H_1. Similar for $i = 2, 3, 4$ the polynomial $Y^2 - t^{-4}\left(\xi_i^3 - u\xi_i - u\right)$ has a root $\tilde{\eta}_i \in \hat{L}$ and $\eta_i = s^5\tilde{\eta}_i$ is a root of H_i. Thus $L_3 \subset M$ with M the quotient field of R_M. An argument similar to proposition 3.5 gives $m = 1$, because $m \geq 1$ and

$$1 = v_{3,P}\left(t'_{3,P}\right) = v_{3,P}\left(u\right) + v_M\left(t'_{3,P}\right) v_{3,P}\left(s\right) = v_M\left(t'_{3,P}\right) m$$

with $t'_{3,P} \in R_{3,P}$ a uniformizer and $u \in R_M$ a unit such that $t'_{3,P} = us^{v_M\left(t'_{3,P}\right)}$. Hence the ramification index is $n = 2$. □

The morphism ψ_3 does not branch above any point on C different from O_C by proposition 4.2. The previous proposition implies that ψ_3 does branch above O_C. Hence D_3 is a branched covering space of the elliptic curve C that branches only above a single point.

We can derive an additional result from the proof of proposition 4.4. Define $L_{3,x} = K\left(E\left[3\right]_x\right)$. Let $D_{3,x}$ be the curve over k corresponding to $L_{3,x}$. Write the surjective morphism induced by the inclusion of K into $L_{3,x}$ as $\psi_{3,x} : D_{3,x} \to C$. Since $L_{3,x} \subset \hat{K}_{O_C}$ as is shown in the proof above, then $\psi_{3,x}$ is unbranched above O_C by proposition 3.5. In section 4.2 we continue studying curves like $D_{3,x}$.

Proposition 4.5. *Let $m \in \mathbb{Z}_{>3}$ be an integer and $p \in \mathbb{Z}_{>3}$ a prime factor of m. If $P \in D_m$ is a point such that $\psi_m\left(P\right) = O_C$, then ψ_m is ramified at P with ramification index divisible by p.*

Proof. Let $R_{m,P}$ be the local ring of D_m at P and R_{O_C} the local ring of C at O_C. The morphism ψ_m induces an inclusion of R_{O_C} in $R_{m,P}$ such that the maximal ideal m_{O_C} is contained in $m_{m,P}$. Let $t_{O_C} = \frac{a}{b}$ be a uniformizer of R_{O_C}, then $a = ut_{O_C}^{-2}$ and $b = ut_{O_C}^{-3}$ for some unit $u \in R_{O_C}$. Denote the completion of K at O_C by $\hat{K}_{O_C}$ and the completion of L_m at P by $\hat{L}_{m,P}$.

Recall that the elliptic curve E has j-invariant

$$j\left(E\right) = 1728\frac{4a^3}{\Delta\left(E\right)} = 1728 \cdot 4u^3 t_{O_C}^{-6}.$$

Therefore there exists a $q \in \hat{m}_{O_C}$ such that the Tate curve E_q has j-invariant $j(E_q) = j(E)$ by proposition 3.31. However E is not isomorphic to E_q over $\hat{K}_{O_C}$, because

$$\gamma(E) = -\frac{a}{18b} = -\frac{1}{18} t_{O_C}$$

is not a square in $\hat{K}^*_{O_C}$. Define $\hat{M} = \hat{L}_{m,P}(\sqrt{t_{O_C}})$, then E is isomorphic to E_q over $\hat{M}$, because t_{O_C} is a square in $\hat{M}$ and the residue field is algebraically closed of characteristic zero. Let $n' = v_P(t_{O_C})$ be the ramification index at P and $n = v_M(t_{O_C})$. If $\sqrt{t_{O_C}} \in \hat{L}_{m,P}$, then $n = n'$, otherwise $n = 2n'$.

There is an injective homomorphism $E(L_{m,P}) \to E\left(\hat{M}\right)$, because $L_{m,P}$ is a subfield of $\hat{M}$. The elliptic curves E and E_q are isomorphic over $\hat{M}$. So there is an isomorphism $E\left(\hat{M}\right) \to E_q\left(\hat{M}\right)$. Therefore $E_q\left(\hat{M}\right)$ contains all points of order dividing m, because $E(L_{m,P})$ contains all m^2 such points. Hence $\hat{M}^*/q^{\mathbb{Z}}$ also contains all points of order dividing m by corollaries 3.29 and 3.30.

Let $t_M \in \hat{R}_M$ be a uniformizer such that $q = t_M^{6n}$. Suppose that $\bar{x} \in \hat{M}^*/q^{\mathbb{Z}}$ is an element of order m. Define $\bar{y} = \bar{x}^{\frac{m}{p}}$, then $\bar{y}$ has order p. Let $y \in \hat{M}^*$ be a representative of $\bar{y}$, then $y^p \in q^{\mathbb{Z}}$, that is $y^p = q^r$ for some $r \in \mathbb{Z}$. Assume that $0 \leq r < p$, otherwise there are $s, r' \in \mathbb{Z}$ such that $r = sp + r'$ and $0 \leq r' < p$ by division with remainder, so that $y' = \frac{y}{q^s}$ is another representative of $\bar{y}$ for which $y'^p = q^{r'}$. If $r > 0$, then p is a divisor of n, because $p > 3$ is prime, $r < p$ and

$$pv_M(y) = v_M(y^p) = v_M(q^r) = 6nr.$$

Assume that $r = 0$, then y is a p-th root of unity. However there are p^2 points of order p in $\bar{x} \in \hat{M}^*/q^{\mathbb{Z}}$ and only p roots of unity. Thus $r > 0$.

Hence p is a divisor of n, that is p is a divisor of the ramification index n'. In particular $n' > 1$, so that the morphism ψ_m is ramified at P. □

From proposition 4.2 we know that the morphism ψ_m is unbranched above any point on C different from O_C. If a prime number larger than three divides m, then ψ_m does branch above O_C. Hence in this case D_m is a branched covering space of the elliptic curve C that branches only above a single point.

In general the precise value of the ramification index of ψ_m above O_C is unknown. However if m is a prime larger than three, then there are only two possibilities as the corollary below shows.

Corollary 4.6. *Let $p > 3$ be a prime number. If $P \in D_p$ is a point such that $\psi_p(P) = O_C$, then the ramification index of ψ_p at P is either p or $2p$.*

We need a restriction on the order of certain elements in $\mathrm{SL}_2(\mathbb{F}_p)$. After the following lemma we will prove the corollary.

Lemma 4.7. *Let $p \in \mathbb{Z}_{>2}$ be prime and $A \in SL_2(\mathbb{F}_p)$. If $p | \operatorname{ord}(A)$, then there exists a $Q \in SL_2\left(\mathbb{F}_{p^2}\right)$ such that*

$$A = Q^{-1} \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} Q$$

where $\alpha = \pm 1$. Moreover if $\alpha = 1$, then $\operatorname{ord}(A) = p$, else $\operatorname{ord}(A) = 2p$.

Proof. Let $f \in \mathbb{F}_p[X]$ be the characteristic polynomial of A, that is $f(X) = \det(A - XI)$. If f is irreducible, then f splits over a degree two extension of $\mathbb{F}_p$ since f has degree two, however any such extension of $\mathbb{F}_p$ is isomorphic to $\mathbb{F}_{p^2}$. Thus f certainly splits over $\mathbb{F}_{p^2}$. Hence there exists a $Q \in M_{2\times 2}(\mathbb{F}_{p^2})$ such that QAQ^{-1} is in the Jordan canonical form. Suppose that

$$QAQ^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

with $\alpha, \beta \in \mathbb{F}_{p^2}$, then $\alpha \neq 0$ and $\beta = \alpha^{-1}$ since $\det(A) = 1$. So $\operatorname{ord}(A)$ divides $\left|\mathbb{F}_{p^2}^*\right| = p^2 - 1$. Therefore also $p|p^2 - 1$, which is impossible. Hence

$$QAQ^{-1} = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

with $\alpha \in \mathbb{F}_{p^2}$. In fact $\alpha = \pm 1$, because $\alpha^2 = 1$.

The order of A follows immediately from

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}^n = \begin{pmatrix} \alpha^n & n\alpha^{n-1} \\ 0 & \alpha^n \end{pmatrix}$$

for all $n \in \mathbb{Z}_{\geq 0}$ and $n\alpha^{n-1} = 0$ only if $p|n$. □

Proof of corollary 4.6. Denote the ramification index at P by n. Now

$$\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Gal}\left(\hat{L}_{p,P}/\hat{K}_{O_C}\right) \cong \{\sigma \in \operatorname{Gal}(L_p/K) : \sigma(P) = P\} \subset \operatorname{Gal}(L_p/K),$$

where the first isomorphism follows from corollary 3.9 and the second isomorphism follows from proposition 3.19 and proposition 3.21. Since $\mathbb{Z}/n\mathbb{Z}$ contains an element of order n, then $\operatorname{Gal}(L_p/K)$ also contains an element of order n, say σ. There exists an injective homomorphism $\rho_p : \operatorname{Gal}(L_p/K) \to \mathrm{SL}_2(\mathbb{F}_p)$ by proposition 3.22. So $\rho_p(\sigma) \in \mathrm{SL}_2(\mathbb{F}_p)$ also has order n. Proposition 4.5 implies that p divides n. From lemma 4.7 follows that $\rho_p(\sigma)$ has order either p or $2p$. Therefore either $n = p$ or $n = 2p$. □

From now on we assume that k is the field of complex number $\mathbb{C}$. Moreover we focus on the curves D_m with m a prime number larger than three. These restrictions allow us to compute the Galois group of the extension L_p of K.

Proposition 4.8. *Let E be an elliptic curve defined over $\mathbb{C}(t)$. If $j(E) = t$, then $\operatorname{Gal}(\mathbb{C}(t, E[n])/\mathbb{C}(t)) \to SL_2(\mathbb{Z}/n\mathbb{Z})$ is an isomorphism.*

Proof. See [9, theorem 1]. □

We extend this proposition to our situation.

Corollary 4.9. *If $p \in \mathbb{Z}_{>3}$ is prime, then the map $\rho_p : \operatorname{Gal}(L_p/K) \to SL_2(\mathbb{F}_p)$ is an isomorphism.*

The lemma below is necessary to derive the corollary. It is a result on normal subgroups of $\mathrm{SL}_2(k)$ with k a field containing more than three elements.

Lemma 4.10. *Let k be a field such that $|k| > 3$. If N is a normal subgroup of $SL_2(k)$, then either $N = SL_2(k)$ or $[SL_2(k) : N] \geq 60$.*

Proof. Denote $\mathrm{SL}_2(k)$ by G. The canonical homomorphism $\pi : G \to G/N$ is well-defined, because N is normal. The group G is perfect, that is $G = [G, G]$.

Assume that N is proper and $[G : N] < 60$, then G/N is a non-trivial group of order less than 60. Any such group is solvable, thus there exists a proper normal subgroup M of G/N such that $(G/N)/M$ is abelian. Denote latter group by H and the canonical homomorphism by $\rho : G/N \to H$. In particular $\rho \circ \pi : G \to H$ is a surjective homomorphism into an abelian group. It induces a surjective homomorphism $G/[G, G] \to H$. However $G/[G, G]$ is trivial and H is non-trivial, so that the map can not be surjective.

Hence $N = G$ or $[G : N] \geq 60$. □

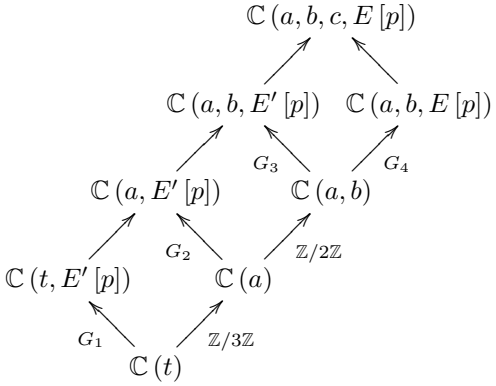
Proof of corollary 4.9. Define $E' : y^2 = x^3 - \frac{27t}{t-1728}x - \frac{54t}{t-1728}$ to be an elliptic curve over $\mathbb{C}(t)$. It has discriminant

$$\Delta(E') = -1728\frac{4 \cdot 27^3 t^2}{(t-1728)^3}$$

and invariant $j(E') = t$. Choose $t = 1728 \cdot 4a^3$ with $a \in K = \mathbb{C}(C)$, then the equation for E' becomes $y^2 = x^3 + 4\frac{a^3}{b^2} + 8\frac{a^3}{b^2}$. The curves E and E' have the same j-invariant. They are isomorphic over $\mathbb{C}(a, b, c)$ with $c^2 = 2\frac{a}{b}$, because they are related by the change of coordinates $E \to E'$ defined as $(x, y) \mapsto \left(c^2 x, c^3 y\right)$. In particular this gives an bijection between $E[p]$ and $E'[p]$. Therefore

$$\mathbb{C}(a, b, c, E[p]) = \mathbb{C}(a, b, c, E'[p]).$$

Consider the following diagram of Galois extensions



where G_i are the Galois for $i = 1, 2, 3, 4$. The homomorphism $G_i \to \mathrm{SL}_2(\mathbb{F}_p)$ is injective for each i by proposition 3.22, since $\mathbb{C}$ contains all roots of unity. So G_i may be considered as a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. Moreover $G_1 = \mathrm{SL}_2(\mathbb{F}_p)$ by proposition 4.8. The extension $\mathbb{C}(a, E'[p])$ of $\mathbb{C}(t, E'[p])$ has degree either one or three. Suppose that it has degree one, then $\mathrm{Gal}(\mathbb{C}(a, E'[p])/\mathbb{C}(a)) = \mathrm{SL}_2(\mathbb{F}_p)$ and G_2 is a normal subgroup of index three, which does not exists by lemma 4.10. Thus $G_2 = \mathrm{SL}_2(\mathbb{F}_p)$. By the same argument $G_3 = \mathrm{SL}_2(\mathbb{F}_p)$. Notice that $|G_4| \leq |G_3|$. Assume that $|G_4| < |G_3|$, then

$$[\mathbb{C}(a, b, c, E[p]) : \mathbb{C}(a, b, E'[p])] < [\mathbb{C}(a, b, c, E[p]) : \mathbb{C}(a, b, E[p])]$$

by the tower law and the degree of the extension on the right is at most two, so that $\mathbb{C}(a,b,c,E[p]) = \mathbb{C}(a,b,E'[p])$ and G_4 a normal subgroup of index at most two, however such a subgroup does not exists by lemma 4.10. Therefore also $G_4 = \mathrm{SL}_2(\mathbb{F}_p)$. Recall that $L_p = K(E[p])$ and $K = \mathbb{C}(a,b)$. Hence $\mathrm{Gal}(L_p/K) = \mathrm{SL}_2(\mathbb{F}_p)$. □

The Galois group of the extension L_p of K is now known. This information tells us how many points on D_p lie above a particular point on C.

Proposition 4.11. *Let $p \in \mathbb{Z}_{>3}$ be prime and $Q \in C$ be a point. If $Q = O_C$, then the inverse image of O_C under ψ_p contains either p^2-1 or $\frac{1}{2}(p^2-1)$ points depending on whether the ramification index above O_C is p or $2p$, otherwise the inverse image of Q under ψ_p contains $(p-1)p(p+1)$ points.*

We need the size of the Galois group. It is calculated in the following lemma.

Lemma 4.12. *Let $p \in \mathbb{Z}$ be prime. Then $|SL_2(\mathbb{F}_p)| = (p-1)p(p+1)$.*

Proof. Consider the following matrix in $\mathrm{SL}_2(\mathbb{F}_p)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

that is $a,b,c,d \in \mathbb{F}_p$ such that $ad - bc = 1$.

Suppose that $ad = 0$, then either both a and d are zero or one of both is zero and the other is non-zero. There are $1 + 2(p-1) = 2p-1$ such combinations of a and d. In this case $bc = -1$, that is $p-1$ combinations of b and c. Hence there are $(p-1)(2p-1)$ matrices with $ad = 0$. A similar argument shows that there are also $(p-1)(2p-1)$ matrices with $ad = 1$.

Assume that $ad \neq 0, 1$, then $bc = ad - 1 \neq 0, -1$. In this case there are $(p-1)(p-2)$ combinations of a and d, and $(p-1)$ combinations of b and c. Hence there are $(p-2)(p-1)^2$ matrices of this form.

Therefore there are

$$2(p-1)(2p-1) + (p-2)(p-1)^2 = (p-1)p(p+1)$$

matrices in $\mathrm{SL}_2(\mathbb{F}_p)$. □

Proof of proposition 4.11. Let $P \in D_p$ be any point. Define $Q = \psi_p(P)$. If n is the number of points above Q, then

$$ne_{\psi_p}(P) = [L_p : K] = |\mathrm{Gal}(L_p/K)| = |\mathrm{SL}_2(\mathbb{F}_p)| = (p-1)p(p+1)$$

where the equalities follow from propositions 3.16 and 3.21, corollary 4.9 and lemma 4.12 respectively. If $Q \neq O_C$, then $e_{\psi_p}(P) = 1$ by proposition 4.2, otherwise $e_{\psi_p}(P)$ is either p or $2p$ by corollary 4.6. This completes the proof. □

Corollary 4.13. *Let $p \in \mathbb{Z}_{>3}$ be prime. If the ramification index of ψ_p above O_C is p, then the genus of D_p is*

$$g_{D_p} = \frac{1}{2}(p^2-1)(p-1) + 1,$$

otherwise the genus of D_p is

$$g_{D_p} = \frac{1}{4}(p^2-1)(2p-1) + 1.$$

Proof. The genus follows immediately from proposition 3.18. □

4.2 Adjoin the x coordinates for all points

Let $m \in \mathbb{Z}_{\geq 2}$ and $L_{m,x} = K\left(E\left[m\right]_x\right)$. Denote the curve over k corresponding to $L_{m,x}$ by $D_{m,x}$. Write the surjective morphism induced by the inclusion of K into $L_{m,x}$ as $\psi_{m,x} : D_{m,x} \to C$. Proposition 3.21 implies that $L_{m,x}$ is a Galois extension of K. We assume that k is the field of complex numbers $\mathbb{C}$ and that p a prime number larger than three.

Proposition 4.14. *Let $P \in D_{p,x}$ be any point. If $\psi_{p,x}\left(P\right) = O_C$, then $\psi_{p,x}$ is ramified at P with ramification index p, otherwise $\psi_{p,x}$ is unramified at P.*

We will prove this proposition after the next two lemmas. The first lemma relates the Galois group of the extension L_p of $L_{p,x}$ to a subgroup of $\mathrm{SL}_2\left(\mathbb{F}_p\right)$. The second lemma restricts the order of certain elements in $\mathrm{PSL}_2\left(\mathbb{F}_p\right)$.

Lemma 4.15. *The subgroup $\mathrm{Gal}\left(L_p/L_{p,x}\right)$ of $\mathrm{Gal}\left(L_p/K\right)$ corresponds to the subgroup $\{I, -I\}$ of $SL_2\left(\mathbb{F}_p\right)$ via the isomorphism $\rho_p : \mathrm{Gal}\left(L_p/K\right) \to SL_2\left(\mathbb{F}_p\right)$.*

Proof. There exists a $\sigma \in \mathrm{Gal}\left(L_p/K\right)$ such that $\rho_p\left(\sigma\right) = -I$. Let $P \in E\left[p\right] - O$ be any point. In this case $P = (x, y)$. Then

$$\left(\sigma\left(x\right), \sigma\left(y\right)\right) = \rho\left(\sigma\right)\left(P\right) = -P = \left(x, -y\right).$$

Thus $\sigma\left(x\right) = x$. So $\sigma \in \mathrm{Gal}\left(L_p/L_{p,x}\right)$, because the x-coordinate of any point P is fixed by σ. Hence $\rho_n\left(\mathrm{Gal}\left(L_p/L_{p,x}\right)\right) \supset \{I, -I\}$.

Let $P \in E\left[p\right]$ be the first point of the ordered basis used for the representation of $\mathrm{SL}_2\left(\mathbb{F}_p\right)$. Take any automorphism $\sigma \in \mathrm{Gal}\left(L_p/L_{p,x}\right)$. Since $P \neq O$, then $P = (x, y)$. Moreover $y^2 = x^3 + ax + b$. So

$$\sigma\left(y\right)^2 = \sigma\left(x^3 + ax + b\right) = \sigma\left(x\right)^3 + a\sigma\left(x\right) + b = x^3 + ax + b = y^2.$$

Therefore $\sigma\left(y\right) = \pm y$. By definition $\sigma\left(x\right) = x$. Hence

$$\rho_p\left(\sigma\right) = \begin{pmatrix} \pm 1 & \beta \\ 0 & \alpha \end{pmatrix}$$

where $\alpha, \beta \in \mathbb{F}_p$ some constants. In fact $\alpha = \pm 1$ and $\beta = 0$, because the determinant is one and σ has order two. Therefore $\rho_n\left(\sigma\right) = \pm I$. Hence also $\rho_n\left(\mathrm{Gal}\left(L_p/L_{p,x}\right)\right) \subset \{I, -I\}$. □

Lemma 4.16. *Let $A \in PSL_2\left(\mathbb{F}_p\right)$. If $p|\operatorname{ord}\left(A\right)$, then $\operatorname{ord}\left(A\right) = p$.*

Proof. Let $\phi : \mathrm{SL}_2\left(\mathbb{F}_p\right) \to \mathrm{PSL}_2\left(\mathbb{F}_p\right)$ be the canonical homomorphism. There exists an element $B \in \mathrm{SL}_2\left(\mathbb{F}_p\right)$ such that $\phi\left(B\right) = A$. Let $n = \operatorname{ord}\left(A\right)$. Since $\phi\left(B^n\right) = A^n = I$, then either $B^n = I$ or $B^n = -I$. Hence $\operatorname{ord}\left(B\right) = n$ or $\operatorname{ord}\left(B\right) = 2n$. In fact either $\operatorname{ord}\left(B\right) = p$ or $\operatorname{ord}\left(B\right) = 2p$, because p divides $\operatorname{ord}\left(B\right)$ and lemma 4.7. Moreover if $\operatorname{ord}\left(B\right) = 2p$, then $B^p = -I$. Therefore $I = \phi\left(B^p\right) = A^p$. Hence $\operatorname{ord}\left(A\right) = p$. □

Proof of proposition 4.14. Denote the surjective morphism corresponding to the inclusion of $L_{p,x}$ into L_p by $\chi : D_p \to D_{p,x}$. Let $Q \in D_p$ be a point such that $\chi\left(Q\right) = P$. Notice that $\psi_p = \psi_{p,x} \circ \chi$. So

$$e_{\psi_p}\left(Q\right) = e_{\psi_{p,x}}\left(P\right) e_\chi\left(Q\right)$$

by proposition 3.17.

Assume that $\psi_{p,x}(P) \neq O_C$, then $\psi_p(Q) \neq O_C$. From proposition 4.2 follows that ψ_p is unramified at Q, that is, $e_{\psi_p}(Q) = 1$. Thus $e_{\psi_{p,x}}(P) = 1$.

Suppose that $\psi_{p,x}(P) = O_C$, then $\psi_p(Q) = O_C$. Moreover $e_{\psi_p}(Q)$ is either p or $2p$ by corollary 4.6. Notice that p does not divide $e_\chi(Q)$, because

$$e_\chi(Q) \leq [L_p : L_{p,x}] = |\mathrm{Gal}(L_p/L_{p,x})| = 2$$

by proposition 3.16 and lemma 4.15. Thus p divides $e_{\psi_{p,x}}(P)$. Let $n = e_{\psi_{p,x}}(P)$.

$$\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}\left(\hat{L}_{p,x,P}/\hat{K}_{O_C}\right) \cong \{\sigma \in \mathrm{Gal}(L_{p,x}/K) : \sigma(P) = P\} \subset \mathrm{Gal}(L_{p,x}/K),$$

where the first isomorphism follows from corollary 3.9 and the second isomorphism follows from proposition 3.19 and proposition 3.21. Since the group $\mathbb{Z}/n\mathbb{Z}$ contains an element of order n and lemma 4.15 gives an isomorphism $\mathrm{Gal}(L_{p,x}/K) \to \mathrm{PSL}_2(\mathbb{F}_p)$, then $\mathrm{PSL}_2(\mathbb{F}_p)$ contains an element of order n. Moreover p divides n. Therefore lemma 4.16 implies that the order is p, that is $n = p$. Hence the ramification index of $\psi_{p,x}$ at P is p. □

We now have enough information to determine the number of points on $D_{p,x}$ above a particular point on C. This allows us compute the genus of $D_{p,x}$.

Corollary 4.17. *Let $Q \in C$ be any point. If $Q = O_C$, then the inverse image of Q under $\psi_{p,x}$ contains $\frac{1}{2}(p^2-1)$ points, otherwise the inverse image of Q under $\psi_{p,x}$ contains $\frac{1}{2}(p-1)p(p+1)$ points.*

Proof. The proof is analogous to the proof of proposition 4.11. □

Corollary 4.18. *The genus of $D_{p,x}$ is*

$$g_{D_{p,x}} = \frac{1}{4}(p^2-1)(p-1) + 1.$$

Proof. The genus follows immediately from proposition 3.18. □

4.3 Adjoin the x coordinate for a single point

Let $m \in \mathbb{Z}_{\geq 2}$ and $P \in E[m]$ be a point of order m. Write the x-coordinate of P as x_P. Adjoin this coordinate to K, that is define $L_{m,P} = K(x_P)$. Denote the curve over k corresponding to $L_{m,P}$ by $D_{m,P}$ and the morphism induced by the inclusion of K into $L_{m,P}$ by $\psi_{m,P} : D_{m,P} \to C$. Again we assume that k is the field of complex numbers $\mathbb{C}$ and that p a prime number larger than three.

Proposition 4.19. *If $R \in D_{p,P}$ is a point such that $\psi_{p,P}(R) \neq O_C$, then $\psi_{p,P}$ is unramified at R. The ramification index is p for some $R \in D_{p,P}$ such that $\psi_{p,P}(R) = O_C$.*

Proof. Let $Q \in E[p]$ be another point of order p such that $\{P, Q\}$ forms an ordered basis for the representation of $\mathrm{SL}_2(\mathbb{F}_p)$. Write x_Q for the x-coordinate of Q. Since $K(x_P, x_Q) \subset L_{p,x}$, then

$$\mathrm{Gal}(L_p/L_{p,x}) \subset \mathrm{Gal}(L_p/K(x_P, x_Q)).$$

Let $\sigma \in \mathrm{Gal}\left(L_p/K\left(x_P, x_Q\right)\right)$ be any automorphism. The points P and Q are chosen such that $\rho_p\left(\sigma\right)\left(P\right) = \pm P$ and $\rho_p\left(\sigma\right)\left(Q\right) = \pm Q$, that is $\rho_p\left(\sigma\right) = \pm I$. Therefore also $\sigma \in \mathrm{Gal}\left(L_p/L_{p,x}\right)$ by lemma 4.15. Hence $L_{p,x} = K\left(x_P, x_Q\right)$.

Let $L_{p,Q} = K\left(x_Q\right)$. Denote the curve with function field $L_{p,Q}$ by $D_{p,Q}$. The inclusion of K into $L_{p,Q}$ gives a surjective morphism $\psi_{p,Q} : D_{p,Q} \to C$. There exists an element $\tau \in \mathrm{Gal}\left(L_p/K\right)$ such that

$$\rho_p\left(\tau\right) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

that is $\rho_p\left(\tau\right)\left(P\right) = Q$ and $\rho_p\left(\tau\right)\left(Q\right) = -P$. In particular $\tau\left(x_Q\right) = x_P$. Thus τ restricts to an isomorphism from $L_{p,Q}$ to $L_{p,P}$ that fixes K. Denote the surjective morphism corresponding to τ by $\lambda : D_{p,P} \to D_{p,Q}$. From corollary 3.12 follows that $\psi_{p,P} = \psi_{p,Q} \circ \lambda$. For any point $R \in D_{p,P}$ proposition 3.17 gives

$$e_{\psi_{p,P}}\left(R\right) = e_{\psi_{p,Q}}\left(\lambda\left(R\right)\right) e_\lambda\left(R\right).$$

In fact $e_\lambda\left(R\right) = 1$, because λ is an isomorphism. Hence the ramification index of $\psi_{p,P}$ at R is the same as the ramification index of $\psi_{p,Q}$ at $\lambda\left(R\right)$.

Assume that $\psi_{p,P}$ is unramified above O_C, then $\psi_{p,Q}$ is also unramified above O_C. Let $\chi_P : D_{p,x} \to D_{p,P}$ and $\chi_Q : D_{p,x} \to D_{p,Q}$ be the surjective morphisms corresponding to the inclusion of $L_{p,P}$ and $L_{p,Q}$ into $L_{p,x}$ respectively. Take a point $R \in D_{p,x}$ such that $\psi_{p,x}\left(R\right) = O_C$. Consider the completions of $L_{p,x}$, $L_{p,P}$, $L_{p,Q}$ and K at R, $\chi_P\left(R\right)$, $\chi_Q\left(R\right)$ and O_C respectively. Now $\hat{L}_{p,P,\chi_P(R)} = \hat{K}_{O_C} = \hat{L}_{p,Q,\chi_Q(R)}$, because the $\psi_{p,P}$ and $\psi_{p,Q}$ are unramified and corollary 3.9. Therefore $L_{p,x} = K\left(x_P, x_Q\right)$ implies that $\hat{L}_{p,x,R} = \hat{K}_{O_C}$, which contradicts that the ramification index of $\psi_{p,x}$ at R is p by proposition 4.14. Hence there exists a point $S \in D_{p,P}$ such that $\psi_{p,P}\left(S\right) = O_C$ and $\psi_{p,P}$ is ramified at S. Let $R \in D_{p,x}$ be a point such that $\chi_P\left(R\right) = S$, then

$$e_{\psi_{p,x}}\left(R\right) = e_{\psi_{p,P}}\left(S\right) e_{\chi_P}\left(R\right).$$

by proposition 3.17 combined with $e_{\psi_{p,x}}\left(R\right) = p$ prime and $e_{\psi_{p,P}}\left(S\right) > 1$ gives that $e_{\psi_{p,P}}\left(S\right) = p$.

Let $S \in D_{p,P}$ be a point such that $\psi_{p,P}\left(S\right) \neq O_C$. There exists a point $R \in D_{p,x}$ such that $\chi_P\left(R\right) = S$. The morphism $\psi_{p,x}$ is unramified at R by proposition 4.14. Hence $\psi_{p,P}$ is also unramified at S by proposition 3.17. □

We see that $D_{p,P}$ is also a branched covering space of the elliptic curve C that branches only above O_C.

Chapter 5

Discussion and conclusions

First we considered an elliptic curve as a Riemann surface of genus one, that is a torus. We mentioned that connected covering spaces of a torus correspond to subgroups of $\mathbb{Z} \times \mathbb{Z}$. In theorem 2.25 we proved that there exists a branched covering space of a torus with a single branch point. We improved this result in proposition 2.26, where we showed that there exists a branched covering space of a torus with one branch point and three sheets. It turns out that three sheets is the minimum.

The proof of theorem 2.25 involved a covering space of the punctured torus with a non-abelian group of deck transformations. Since this group is abelian for all covering spaces of the torus, then the analytic continuation of that particular covering space to a branched covering space of a torus can not be a covering space. We wonder under which conditions the reverse statement is true. Is the analytic continuation of a covering space of the punctured torus with an abelian group of deck transformations again a covering space of the torus?

In section 3.5 we constructed a branched covering space of a particular elliptic curve that only branches above the at infinity point and derived the equations for that curve and covering map. Proposition 3.47 is the algebraic analogue of proposition 2.26.

We have constructed a family of branched covering spaces of the elliptic curve $C : 4a^3 + 27b^2 = 1$ over an algebraically closed field k of characteristic zero. In particular if we take k to be the complex numbers, then we can describe ramification index, the number of points above a point on C and the genus of that branched covering spaces rather well. For example see proposition 4.14 and corollaries 4.17 and 4.18.

The family of branched covering spaces of C also raises a few questions. For example we can ask if proposition 4.8 is also true for other algebraically closed fields of characteristic zero. If this is the case, then our results also hold for that field. We may also ask the following important question. Does the construction in chapter 4 also work for other elliptic curves?

In this master's thesis we encountered a surprising amount of theory. From covering spaces and analytic continuations thereof in chapter 2 to the completion of discrete valuation rings and the Tate curve in chapters 3 and 4.

Bibliography

[1] G.E. Bredon. *Topology and Geometry*, volume 139 of *Graduate texts in mathematics*. Springer, 1993.

[2] O. Forster. *Lectures on Riemann Surfaces*, volume 81 of *Graduate texts in mathematics*. Springer, 1981.

[3] W. Fulton. *Algebraic Topology: A First Course*, volume 153 of *Graduate texts in mathematics*. Springer, 1995.

[4] W. Fulton. *Algebraic Curves. An introduction to Algebraic Geometry*. third edition, 2008. Available from: `http://www.math.lsa.umich.edu/~wfulton/`.

[5] D.J.H. Garling. *A course in Galois theory*. Cambridge University Press, 1986.

[6] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate texts in mathematics*. Springer, 1977.

[7] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2002. Available from: `http://www.math.cornell.edu/~hatcher/AT/ATpage.html`.

[8] Miles A. Reid. *Undergraduate Commutative Algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, 1995.

[9] D.E. Rohrlich. Modular curves, hecke correspondences, and l-functions. In *Modular Forms and Fermat's Last Theorem*, pages 41–100. Springer, 1997.

[10] J.H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate texts in mathematics*. Springer, 1985.

[11] J.H. Silverman. *Advanced topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate texts in mathematics*. Springer, 1994.

[12] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate texts in mathematics. Springer, 1992.

[13] H. Stichtenoth. *Algebraic Function Fields and Codes*, volume 254 of *Graduate texts in mathematics*. Springer, second edition, 2008.

[14] M. van der Put and J. Top. Galois theory. Lecture notes, 2001. Available from: `http://www.math.rug.nl/~top`.