university of groningen

faculty of science and engineering

mathematics and applied mathematics

Singular quartics of genus one

Bachelor's Project Mathematics

August 2019

Student: A.A.J. Greven

First supervisor: Dr. J.S. Müller

Second assessor: Prof. Dr. J. Top

Contents

1 Introduction

This chapter will outline the goal of this thesis and will describe shortly what the chapters will discuss. We will then also introduce some motivation behind research into group laws on elliptic curves.

1.1 Outline

The goal of this thesis is to construct a group law on curves of genus one geometrically and prove that the construction indeed satisfies a group law. We will do this construction on a singular quartic of genus one, which is an elliptic curve defined by a polynomial of degree four with two nodal singularities. These curves are birationally equivalent to non-singular curves of genus one, on which the geometric construction coming from the singular curve defines a group law. This thesis will offer insight in the geometric construction, and justify how this construction induces a group law on the non-singular curve of genus one. Before we can get there, however, we need to explore several other concepts.

We start with describing the space our elliptic curves will live in, i.e., the projective plane, and will explain the notion of algebraic curves.

The next chapter will explain how singularities are defined in the projective plane, and will work towards Bézout's theorem. This theorem will be of fundamental importance for this thesis.

We will then look at elliptic curves in Weierstrass form, as these can be seen as an example after which we will model the construction of addition on quartics of genus one. We will explain how the addition on these curves is defined, after which we will give a purely geometric proof that this construction indeed gives a group law on these curves.

As we will take a different approach for the proof of the group law on singular quartics of genus one, we will explore some basic notions of divisor theory. These notions will be a bit harder mathematically, but will present us with a clear and neat proof of the group law later. We also have to introduce the desingularization of the curve, as we develop theory for non-singular curves while our curve of interest is singular. In this chapter, we also prove that the construction of P_3 from P_1 and P_2 for curves in Weierstrass form indeed gives a group law, using the just introduced divisor theory.

We then show how we construct P_3 from P_1 and P_2 on a singular quartic of genus one, after which we will present the proof that this construction defines a group law on the corresponding non-singular curve of genus one. Lastly, we introduce an example, the twisted Edwards curves.

1.2 History of Elliptic Curves

Elliptic curves have a long history, starting in the time of the Ancient Greeks. In those days, ellipses were known shapes, but calculating the arc length of these shapes was uncharted territory. After the invention of calculus, one could express the arc length in integrals, but these integrals could not be calculated explicitly, only approximated by series. Legendre classified several forms of these so-called elliptic integrals [10, Pages 165-166]. Jacobi and Abel later realized that the inverses of these integrals would present more interesting results, where we note that the integrals depended on a variable and could therefore be inverted. These inverses, they called elliptic functions [10, Pages 167-168]. So far, however, these integrals and functions were not yet connected to elliptic curves. This came in the eighteen hundreds with Eisenstein. He found a correspondence between the elliptic functions and cubic equations. From here, elliptic curves have arisen [10, Page 172].

Elliptic curves have risen fast from this point, especially with the rise of computers and the attached need for safety online. Elliptic curves can be used to factor large integers and are used in the proof of Fermat's Last Theorem [10, Page 164], but more important is the role they play in the field of cryptography.

For detailed explanation why elliptic curves are relevant to cryptography, one is referred to [7]. In short, [7] tells us that the security of elliptic curve cryptography depends on a more difficult problem (namely the elliptic curve discrete logarithm problem) than the standard RSA cryptography (which gets its security from the integer factorization problem). This allows for smaller keys when using elliptic curve cryptography than when using RSA cryptography, while still remaining as secure. Smaller key sizes have positive consequences: they allow for gains in speed and more efficient use of power and storage.

2 Curves in the Projective Plane

This chapter will introduce the basic notions required for this thesis: the projective plane and algebraic curves.

2.1 The Projective Plane

Before we can study elliptic curves, we first need to introduce a more general type of curves: plane algebraic curves. For this, we need the notion of a field.

Definition 2.1. [5, Definition 7.1.2] A **field** $\Bbbk$ is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

1. $(\Bbbk, +)$ is an abelian group
2. $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in \Bbbk$
3. In $\Bbbk$, the distributive laws hold: $(a + b) \times c = (a \times c) + (b \times c)$, $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in \Bbbk$
4. $\Bbbk$ is commutative: $a \times b = b \times a$ for all $a, b \in \Bbbk$
5. $\Bbbk$ has an identity element $1 \in \Bbbk$ such that $1 \times a = a \times 1 = a$ for all $a \in \Bbbk$
6. For all non-zero $a \in \Bbbk$, there exists an inverse element $b \in \Bbbk$ such that $a \times b = b \times a = 1$

Examples of fields are the complex numbers or $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, where p is a prime, both with addition and multiplication as we know it.

We will only work with algebraically closed fields for this thesis, simply to make life easier. For this, however, we will need to define when a field is algebraically closed.

Definition 2.2. [5, Definition 13.4.6] A field $\Bbbk$ is said to be **algebraically closed** if every non-constant polynomial with coefficients in $\Bbbk$ has a root in $\Bbbk$.

An example of an algebraically closed field would be the complex numbers with addition and multiplication as we know it.

A notion one can associate to a field is the characteristic of said field. It is defined as follows.

Definition 2.3. [5, Definition 13.1.1] The **characteristic of a field** $\Bbbk$, denoted $char(\Bbbk)$, is defined to be the smallest positive integer p such that $p \times 1_{\Bbbk} = 0$ if such a p exists. Otherwise, $char(\Bbbk) = 0$.

The characteristic of the complex numbers, for example, is zero, as one never obtains zero by adding ones. However, the characteristic of $\mathbb{F}_p$, with p a prime, is p, as $p \equiv 0 \mod p$. One can actually show that the characteristic of a field is either 0 or p, where p is a prime [5, Proposition 13.1.1].

We can now use the notion of a field to construct the space in which the curves will be living. This space will be the projective plane. Before we can explain this projective plane, we need to define the following equivalence relation: we say that two triples of coordinates (a, b, c) and (d, e, f), where not all entries of a coordinate can be zero simultaneously and all entries are elements of $\Bbbk$, are equivalent if there exists a $t \in \Bbbk^*$ such that $a = dt, b = et, c = ft$. It can easily be seen that this relation is symmetric, transitive and reflexive and therefore an equivalence relation. We then denote the class of coordinates equivalent to (a, b, c) as $[a, b, c]$ [11, Page 267]. With this equivalence relation, we can define the projective plane as follows:

Definition 2.4. [11, Page 267] The **projective plane** $\mathbb{P}^2(\Bbbk)$ is the set of equivalence classes of coordinates, i.e. $\mathbb{P}^2(\Bbbk) = \{[a_0, a_1, a_2] : a_0, a_1, a_2 \in \Bbbk \text{ are not all zero}\}$.

Another way of thinking about the projective plane is to take the Euclidean plane $\Bbbk^2$ and add points "at infinity" such that any two parallel lines have an intersection point, too. One then naturally asks how many points would need to be added, would one be enough? For this, we look at the following instance (depicted in figure 2.1): Let L_1 and L_2 be parallel lines with point of intersection P. Let L'_1 and L'_2 be another pair of parallel lines such that they intersect at P'. Suppose that L_1 and L'_1 are not parallel, then they must have an "ordinary" (i.e., not at infinity) point of intersection, here denoted Q. But two lines only have one point in their intersection, which implies that $P \in L_1$ and $P' \in L'_1$ must be distinct, as Q is already the point in their intersection and $Q \neq P$ or P'. We thus conclude that we have to add an extra point for each direction in the ordinary plane [11, §A.1].

We call the line through all points at infinity the **line at infinity**.

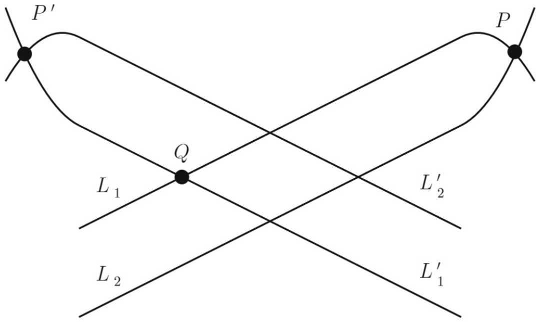

Figure 2.1: Two sets of parallel lines with intersection points at infinity [11, Figure A.1].

2.2 Algebraic Curves

As we have seen the space in which our curves will live, we can now define an algebraic curve. We first define these curves in the affine (Euclidean) plane.

Definition 2.5. [3, Definition 1.1] A **plane affine algebraic curve** is defined to be the set of solutions to a polynomial equation, i.e. $C = \{(x, y) \in \Bbbk^2 : F(x, y) = 0\}$, where F is a non-constant polynomial of some degree over a field.

The definition for a curve in the projective plane differs slightly:

Definition 2.6. [11, Page 271] We define a **projective algebraic curve** to be the set of solutions to $F(X, Y, Z) = 0$, i.e.,

$$C = \{[x, y, z] \in \mathbb{P}^2(\Bbbk) : F(x, y, z) = 0\},$$

where $F \in \Bbbk[x, y, z]$ is a non-constant and homogeneous polynomial We then say that $\deg(C) = \deg(f)$.

We say that F is homogeneous of degree d if it satisfies $F(tX, tY, tZ) = t^d F(X, Y, Z)$ for any $t \in \mathbb{Z}$ [11, Page 271]. Moreover, we note that we need the homogeneous condition to make sense of solutions to this equation F in the projective plane: for $[a, b, c] \in \mathbb{P}^2(\Bbbk)$, the condition $F(a, b, c) = 0$ must be independent of the chosen representative (a, b, c).
We will only consider algebraic curves in this thesis, and will therefore refer to the curves in consideration as just an affine or projective curve.

As we would like to switch between thinking about the affine part of a curve and the entire projective curve, we will need to define a relation between the two.

Definition 2.7. [11, Page 275] The degree d **homogenization** of a polynomial $f(x, y) = \sum a_{ij}x^iy^j$ of degree d is defined to be $F(x, y, z) = \sum_{i,j} a_{i,j}x^iy^jz^{d-i-j}$.

This process takes the affine part of a curve and maps it to the projective curve corresponding to it. We can also define a process in the opposite direction:

Definition 2.8. [11, Page 274] The process of replacing the homogeneous polynomial $F(x, y, z)$ by the inhomogeneous polynomial $f(x, y) = F(x, y, 1)$ is called **dehomogenization** (with respect to the variable z).

Remark 2.9. Dehomogenization can also be done with respect to variable x or y: $f(y, z) = F(1, y, z)$ or$f(x, z) = F(x, 1, z)$, respectively.

We observe that $F(x, y, 0)$ is not identically equal to zero by the way we defined the homogenization, which implies that it does not contain the line at infinity. As a consequence, the correspondence between the affine part and the entire projective curve through the processes of homogenization and dehomogenization is one-to-one [11, Page 275]. This will allow us to consider a curve in the space most suitable for the problem.

To clarify some of the introduced concepts, we discuss an example of a curve.

Example 2.10. Let $C : f(x, y) = y^2(2 - x) - x^3 = 0$ be an affine curve. It is called the Cissoid of Diocles. We can draw the graph of this curve in the real plane (see figure 2.2). We remark that the degree of the curve is three, as the defining equation has degree three. We can take this curve to the projective plane to obtain $C : F(x, y, z) = 2y^2z - xy^2 - x^3 = 0$. One can verify that $F(x, y, 1)$ indeed equals $f(x, y)$. We can try plugging in $(tx, ty, tz), t \in \mathbb{Z}$, into $F(x, y, z)$ to see what happens: $F(tx, ty, tz) = 2t^3y^2x - t^3xy^2 - t^3x^3 = t^3F(x, y, z)$. Thus, $F(x, y, z)$ is homogeneous of degree three.

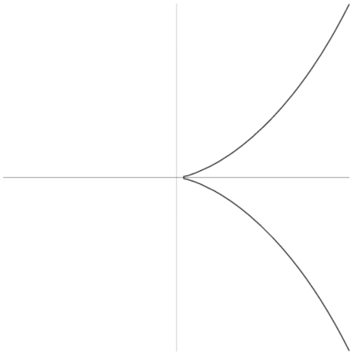

Figure 2.2: Cissoid of Diocles.

3 Bézout's theorem

This chapter will introduce Bézout's theorem, a theorem that is fundamental to this thesis. For this, however, we first have to introduce a few other concepts.

3.1 Singularities and Intersection Multiplicity

While we have seen how a projective plane curve is defined, we have yet to learn how certain properties are defined on these curves. An example of this is singular points.

Definition 3.1. [12, Definition 2.4] A curve C in the projective plane over a field $\Bbbk$ defined by $F(x, y, z) = 0$ is said to be **non-singular** at a point P if at least one of the partial derivatives F_x, F_y, F_z is non-zero at P.

If at a point P all partial derivatives are zero, then P is said to be a singularity of the curve.

Definition 3.2. [8, §2.5] A **nodal** singularity is a point on the curve where the curve intersects itself and where the two tangent lines to the curve have different directions.

The tangent line of a curve over a field like $\mathbb{C}$ can be thought of as the tangent line we are familiar with from calculus, but for the more general concept of tangent lines of curves over fields one is referred to page 13 of [3].

As the definition for nodal singularities is not very practical, we state the following proposition.

Proposition 3.3. [3, Page 15] *Let our curve be given as $C : F(x, y, z) = 0$. Let P denote the singularity. Let P be moved to $[0, 0, 1]$ and assume that the affine part of the resulting equation $F'(x, y, z)$ can be written as $F'(x, y) = F_n(x, y) + G(x, y)$, where F_n is homogeneous of degree n and G only contains terms of degree higher than n. If $n = 2$, then P is a nodal singularity.*

To demonstrate this proposition, we introduce an example:

Example 3.4. Let C be the curve given by $F(x, y) = ax^2 + y^2 - 1 - dx^2y^2 = 0$ for two non-zero elements $a, d \in \Bbbk$, where $\Bbbk$ is a field with characteristic not equal to two. We take the point $P = [1, 0, 0]$ and want to show that this point is a nodal singularity of the curve. The first step is to homogenize the equation $F(x, y)$, which gives us

$$F(x, y, z) = ax^2z^2 + y^2z^2 - z^4 - dx^2y^2.$$

The partial derivatives F_x, F_y, F_z indeed are all equal to zero at P, so P is a singularity of C. We then move P to $[0, 0, 1]$ by substituting x by z, and z by x, and leaving y as itself. We find the new equation

$$C : F(x, y, z) = az^2x^2 + y^2x^2 - x^4 - dz^2y^2,$$

which has affine part $F(x,y) = ax^2 + y^2x^2 - x^4 - dy^2$. This can be written as $F(x,y) = F_n(x,y) + G(x,y)$, where $F_n(x,y) = ax^2 - dy^2$ and $G(x,y) = y^2x^2 - x^4$, and F_n is homogeneous of degree two. Thus, the singularity $P = [1,0,0]$ is indeed a nodal singularity of this curve C.

A concept tightly connected to singularities is the genus of a curve. Let C be an absolutely irreducible curve of degree d (i.e., a non-constant curve of degree d that cannot be factored into the product of two non-constant polynomials over the algebraic closure of $\mathbb{Q}$ [9, Page 18]). Suppose it has singular points $S_1, \ldots, S_k$. To each singular point we will assign a quantity δ that depends on the complexity of the singularity. If the singularity is nodal, we have that $\delta = 1$, and for non-singular points, we have that $\delta = 0$. With this, we can define the genus of a curve in the following way.

Definition 3.5. [3, Chapter 7] The **genus** of a plane projective curve C with singularities as described above has genus defined by

$$g(C) = \frac{(d-1)(d-2)}{2} - \sum_{i=1}^{k} \delta_i.$$

The genus of a curve can also be defined for a general projective curve (that is not necessarily plane). For this, see definition 8.4.8 of [6].

To clarify the concept of the genus of a plane projective curve, we will introduce an example that will become of importance later.

Example 3.6. Let C be a plane projective curve given by a degree four polynomial with two nodal singularities N_1 and N_2 over field $\mathbb{k}$. As the singularity complexity of nodal singularities is one, we thus find that the genus of C is given by

$$g(C) = \frac{3 * 2}{2} - 1 - 1 = 1.$$

Thus a quartic (a curve defined by a degree four polynomial) with two nodal singularities is of genus one.

We have now seen several mentions of nodal singularities, and they will be of relevance later. More specifically, we are interested in the intersection multiplicities in these specific points. Before we can talk about the intersection multiplicity in nodal singularities, however, we first have to introduce the general notion of intersection multiplicity.

To make sense of the following definition of intersection multiplicity, we define the set $\mathcal{F}(\mathbb{k})$ to be the set of pairs of polynomials $f, g \in \mathbb{k}[x,y]$ having no common factor h in $\mathbb{k}[x,y]$ with $h(0,0) = 0$. The intersection number of the curves defined by f and g at the origin requires the following map.

Proposition 3.7. [9, Propostion 1.8] *There is a unique map $\mathcal{I} : \mathcal{F}(\Bbbk) \to \mathbb{N}$ such that*

1. $\mathcal{I}(x, y) = 1$
2. $\mathcal{I}(f, g) = \mathcal{I}(g, f)$ *for all* $(f, g) \in \mathcal{F}(\Bbbk)$
3. $\mathcal{I}(f, gh) = \mathcal{I}(f, g) + \mathcal{I}(f, h)$ *for all* $(f, g), (f, h) \in \mathcal{F}(\Bbbk)$
4. $\mathcal{I}(f, g + hf) = \mathcal{I}(f, g)$ *for all* $(f, g) \in \mathcal{F}(\Bbbk), h \in \Bbbk[x, y]$
5. $\mathcal{I}(f, g) = 0$ *if* $g(0, 0) = 0$

This map, however, does not tell us how this intersection number is defined. For this, we need to remark that the quotient ring $\Bbbk[x, y]_{(0,0)}/(f, g)$ is finite dimensional as a $\Bbbk-$vector space [9, §1.1], where $\Bbbk[x, y]_{(0,0)}$ is the local ring at the maximal ideal (x, y) [9, Page 9]. Setting the intersection number $\mathcal{I}$ to be equal to the dimension of this quotient ring will thus give us a clear definition of this map.

We might be interested in looking at the intersection number at a specific point in the intersection of two curves without having to move it to the origin, for which we define the following:

Definition 3.8. [9, §1.1] Let $C : f(x, y) = 0$ and $D : g(x, y) = 0$ define two affine plane curves. Let $P = (a, b)$ be a point in the intersection of C and D. Then the intersection multiplicity is given by

$$\mathcal{I}(P, C \cap D) := \mathcal{I}(f(x + a, y + b), g(x + a, y + b)).$$

Remark 3.9. [9, Remark 1.13] The intersection multiplicity of a nodal singularity in an intersection will always equal at least two.

3.2 Bézout's Theorem

As we have defined what the intersection multiplicity in a point in the intersection of two curves is, we are ready to state the following theorem.

Theorem 3.10 (Bézout)**.** [3, Theorem 3.2] *Let C, D be two plane projective curves of degrees m, n defined over an algebraically closed field $\Bbbk$. Suppose that they have no common components. Let S be the set of intersection points $C(\Bbbk) \cap D(\Bbbk)$. Then $\sum_{P \in S} \mathcal{I}(P, C \cap D) = mn$.*

This theorem tells us that, for example, a curve defined by a cubic (a degree three polynomial) will have exactly three points in the intersection with a line (which is given by a degree one polynomial) that is not a component of the curve.

Bézout's theorem will feature heavily in the proof of the group law on curves in Weierstrass form, but also in the generalization of the group law to quartics of genus one. It allows us to determine how many points should be in intersections, which will be crucial.

As this theorem is merely an instrument in later proofs, the proof of this theorem is omitted. However, it can be found in section A.4 of [11].

Remark 3.11. A consequence of Bézout's theorem is that when two curves have more points in common that the product of their respective degrees, one can conclude that these curves share a component.

4 Group Law on Elliptic Curves in Weierstrass Form

We are now interested in the polynomial equations in a specific form: the Weierstrass form. The curves defined by these equations are algebraic *elliptic* curves, and will have an explicitly defined group law, which we will discuss after introducing the form.

4.1 The Weierstrass Form

Before we can introduce the Weierstrass form for elliptic curves, we have to introduce elliptic curves.

Definition 4.1. [9, Definition 1.1.c] An **elliptic curve** over $\Bbbk$ can be defined as a non-singular projective plane curve over $\Bbbk$ of the form $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$.

An elliptic curve in Weierstrass Form is given by a more specific equation:

Definition 4.2. [12, Page 9] The **Weierstrass equation** for an elliptic curve over a field $\Bbbk$ with $char(\Bbbk) \neq 2, 3$ is of the form

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \Bbbk$ such that $4A^3 + 27B^2 \neq 0$.

The assumption on A and B prevents the equation from having multiple roots, and therefore, the curve from having singularities [9, Example 1.5]. Curves in Weierstrass form with singularities are beyond the scope of this thesis.

The equation $y^2 = x^3 + Ax + B$ can be homogenized to $y^2z = x^3 + Axz^2 + Bz^3$, from which it is immediately clear that the equation indeed gives an elliptic curve (as the curve is also non-singular).

We require the field $\Bbbk$ to have $char(\Bbbk) \neq 2, 3$ for this definition to hold. In the case that $char(\Bbbk) = 2$ or 3, there is a generalized Weierstrass equation. To consider this, however, is beyond the scope of this thesis. For the interested reader, more information on the generalized Weierstrass form can be found in [12, §2.1].

Curves in Weierstrass form have exactly one point at infinity, which can be shown as follows: if we take any non-singular cubic $y^2 = x^3 + ax + b$ in the affine plane and homogenize it, we find $y^2z = x^3 + axz^2 + bz^3$. We then want to find the intersection of this cubic with the line at infinity $z = 0$. Substituting $z = 0$ into our homogenized cubic, we find $x^3 = 0$, and thus that the cubic and the line intersect at points at infinity three times. More specifically, they intersect in the same point at infinity three times. From this, we deduce that there is only one point at infinity in the set of points on the curve of a cubic, and thus on curves in Weierstrass form [11, Page 23]. Moreover, we know that the point at infinity is given by $[0, 1, 0]$.

A curve C in Weierstrass form has genus one, which follows from the fact that the curve has no singularities and is defined by a degree three polynomial: $g(C) = \frac{2*1}{2} - 0 = 1$.

To get an idea what curves in Weierstrass form look like, we introduce an example.

Example 4.3. We look at the curve C defined over $\mathbb{C}$ by $f(x, y) = x^3 - 2x + 2 - y^2$. The real points on C are visualized in figure 4.1. We can verify that for this curve $4A^3 + 27B^2$ indeed is nonzero. Thus, this curve is indeed a curve in Weierstrass form.

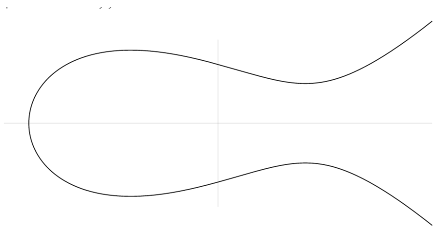

Figure 4.1: An elliptic curve in Weierstrass form.

4.2 Addition on an Elliptic Curve in Weierstrass Form

As we now know how elliptic curves in Weierstrass form are defined, we can define the addition of points on these curves (following [12, §2.2]). For this, we assume that C is defined by an equation in Weierstrass form. We also take two points on this curve: P_1 and P_2.
We now find the point $P_3 := P_1 + P_2$ by taking the line through the points P_1 and P_2 and looking at the intersections of the line and the curve. From Bézout's theorem, we know that there should be three points in this intersection (counting multiplicities). Trivially, P_1 and P_2 are in this intersection and we denote the third point by P_3'. We then obtain P_3 by reflecting this point in the x-axis. This point P_3 will also lie on C: if (x_3, y_3) is on C, it satisfies $y^2 = x^3 + Ax + B$, and then $(x_3, -y_3)$ trivially satisfies the equation, too, and therefore P_3 is on C.
The points P_1 and P_2 might not be distinct. If $P_1 = P_2$, then we take the tangent line of the curve at P_1 and count the point P_1 to have multiplicity two. The third point is again denoted P_3', which will then be reflected in the x-axis.
We can also consider the case where the first coordinates of P_1 and P_2 are the same, but the second differ. In this case, the line through the two points is a vertical line, which will intersect the curve in the points P_1, P_2 and the point at infinity. Then $P_3 = \infty$.
We can have that the points P_1 and P_2 are the same and that both y-coordinates are zero. In this case, we again find that the line through them is vertical, and we similarly

find that $P_3 = \infty$.
It is also possible that either of the points P_1 and P_2 is the point at infinity. Without loss of generality, assume that $P_1 = \infty$. Then the line through P_1 and P_2 is the vertical line through P_2, and the third point Q of intersection will be the reflection of P_2 in the x-axis. Then reflecting Q gives us that $P_3 = P_2$.
The process of finding the point P_3 from the points P_1 and P_2 (where we assume $P_1 \neq P_2$ and neither is at infinity) is visualized in figure 4.2. Here the continuous line is the curve in Weierstrass form, the dash-dotted line is the line through P_1 and P_2, and the dotted line is the line through P_3' and ∞.

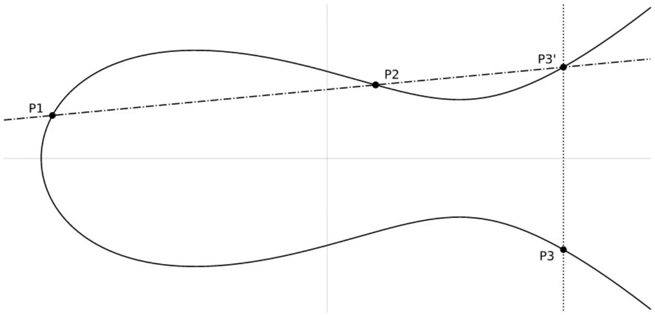

Figure 4.2: Visualization of Group Law on Elliptic Curves.

The geometric construction of addition of points on Weierstrass Curves as described above gives the following theorem for explicit formulas for P_3 depending on P_1 and P_2.

Theorem 4.4 (Addition of Points on Elliptic Curves in Weierstrass Form)**.** [12, Page 14] *Let C be an elliptic curve defined by an equation in Weierstrass form. We take two points on C: $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ such that neither is at infinity. We then define addition on the elliptic curve $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*

1. *If $x_1 \neq x_2$, then*

$$x_3 = m^2 - x_1 - x_2, \ \ y_3 = m(x_1 - x_3) - y_1, \ \ \textit{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. *If $x_1 = x_2$, but $y_1 \neq y_2$, then*

$$P_1 + P_2 = \infty.$$

3. *If $P_1 = P_2$ and $y_1 \neq 0$, then*

$$x_3 = m^2 - 2x_1, \ \ y_3 = m(x_1 - x_3) - y_1, \ \ \textit{where } m = \frac{3x_1^2 + A}{2y_1}.$$

4. *If $P_1 = P_2$ and $y_1 = 0$, then*

$$P_1 + P_2 = \infty.$$

Here, m denotes the slope of the line through P_1 and P_2.
Moreover, we define

$$P + \infty = P$$

for all points P on C.

To illustrate how this group law would work in practice, we discuss two examples of curves defined by an equation in Weierstrass form and the addition of two points on these curves.

Example 4.5. Let C be the curve defined by $y^2 = x^3 + 1$. On this curve, we take the following two points: $P_1 = (0, 1), P_2 = (2, 3)$. Using the theorem above, we then find that

$$P_1 + P_2 = P_3 = (-1, 0).$$

Example 4.6. Let C be the curve defined by $y^2 = x^3 + 4x - 1$. On this curve, we take the following two points: $P_1 = (1, 2), P_2 = (1, -2)$. Following the theorem above, we then find that

$$P_1 + P_2 = P_3 = \infty.$$

4.3 Group Law

We have now defined the operation of addition of points on an elliptic curve in Weierstrass form, but have yet to show that it indeed is a group law. For this, we look at the following theorem.

Theorem 4.7. [12, Theorem 2.1] *The addition of points on an elliptic curve C as defined above satisfies the following properties: closure, existence of the identity element, existence of the inverse elements, commutativity and associativity. This makes the addition on elliptic curves as defined above an abelian group law on elliptic curves in Weierstrass form.*

Proof. We explained earlier how adding points of an elliptic curve in Weierstrass form returns another point on the curve (as the reflection of P_3' in the x-axis returned an element on the curve), which proves the closure condition.
For the existence of the unit element, we observe that the point at infinity satisfies our needs here, by the way we constructed the addition.
For the inverse element, we note that for any point $P = (x, y)$, the point $-P \coloneqq (x, -y)$ gives us that $P + (-P) = \infty$, and therefore is the inverse element we look for.
The commutativity is satisfied by noting that the line through points A and B is the same line as the line through the points B and A.
The associativity of this addition is harder to prove, and requires Bézout's theorem. Here, we will only discuss the generic case, with which we mean the situation that $P_1 \neq P_2$ and neither points are the point at infinity. For a detailed proof of the associativity, taking into account all technicalities, one is referred to [12, §2.4].

We take any three distinct points P, Q, R on the elliptic curve E but not at infinity. This case is pictured in figure 4.3. We then have to show that $(P+Q)+R = P+(Q+R)$, or equivalently, that $-((P+Q)+R) = -(P+(Q+R))$. To compute $-((P+Q)+R)$, we have to consider the lines

l_1**:** The line through P and Q;

m_2**:** The line through $P+Q$ and infinity;

l_3**:** The line through R and $P+Q$.

These lines have been depicted in figure 4.3, too.

Then, to compute $-(P+(Q+R))$, we need to consider the lines

m_1**:** The line through Q and R;

l_2**:** The line through $Q+R$ and infinity;

m_3**:** The line through P and $Q+R$.

These lines are also depicted in figure 4.3. All the lines l_i have been depicted with dotted lines, and the lines m_i have been drawn as thin continuous lines. The thick black line is the curve in Weierstrass form. In this figure, the point $P+Q$ before reflection is denoted $P*Q$, and analogously for the other points.

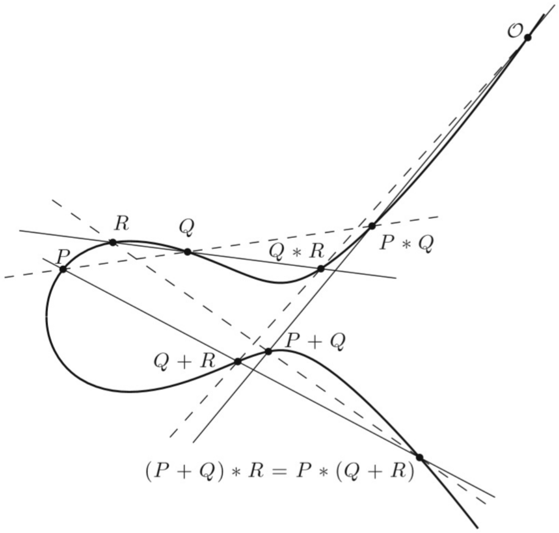

Figure 4.3: Visualization of the lines required for the associativity [11, Figure 1.9].

We can now define the points $P_{ij} = l_i \cap m_j$ unambiguously as two distinct lines will always have exactly one point in their intersection, which gives us the following identification:

P_{11}	Q
P_{12}	-(R+Q)
P_{13}	∞
P_{21}	P
P_{22}	Q+R
P_{23}	S
P_{31}	-(Q+R)
P_{32}	R
P_{33}	P+Q

Here, S denotes the element we hope to equal $-((P+Q)+R) = -(P+(Q+R))$, and of which we hope it is on E.

We can construct two degree three curves by taking each to be the union of three lines, such that these curves have all nine points P_{ij}, $i, j \in \{1, 2, 3\}$, in their intersection. We then recall that we know eight of these points to also lie on the curve C, which gives us that the ninth point (i.e., S) must also be on C [11, Pages 286-288].
Then, as l_3 intersects E at the points $R, P+Q$ and $-((P+Q)+R)$, we must have that $S = -((P+Q)+R)$. Also, as m_3 intersects E at $P, Q+R$ and $-(P+(Q+R))$, we also find that $S = -(P+(Q+R))$. Thus, we find that indeed $-((P+Q)+R) = -(P+(Q+R))$, and thus have thus proven associativity for the group law on elliptic curves in Weierstrass form (for the generic case).

We have thus shown that the addition as defined before is a group law on elliptic curves that are defined by equations in Weierstrass form. □

5 Divisor Theory

As we want to take a different approach to proving the group law on general quartics of genus one than we have seen in the case of curves in Weierstrass Form, we need to introduce the required concepts. This chapter will discuss the basic notions required from divisor theory, and will introduce a theorem that will allow us to transfer a group structure onto a non-singular quartic of genus one. As our curve of interest is singular, we will have to introduce the notion of desingularization. We will end this chapter with a section on curves in Weierstrass form in which we prove, with the introduced divisor theory, that the construction of P_3 out of P_1 and P_2 as seen in the previous chapter gives a group law.

5.1 The Degree Zero Class Group

First, we need to introduce the notion of a function field of a plane projective curve C, denoted $\Bbbk(C)$. Let $C : F(x, y, z) = 0$ be a plane projective curve over $\Bbbk$, and

$$\Bbbk[X, Y, Z] = \Bbbk[x, y, z]/(F(x, y, z)).$$

We then say that $\Bbbk(X, Y, Z)$ is the field of fractions of $\Bbbk[X, Y, Z]$ [5, Page 260].

Definition 5.1. [9, Page 30] The **function field** of a plane projective curve C as given above is defined as $\Bbbk(C) = \{g/h \in \Bbbk(X, Y, Z) \mid g, h$ are homogeneous of the same degree $d\}$.

We can view its elements as functions on C, and it is a subfield of $\Bbbk(X, Y, Z)$. We require this algebraic structure to define the divisor of a function on a curve.

Definition 5.2. [6, Definition 7.6.1, 7.6.3] Let C be a curve over $\Bbbk$ that is plane and projective. A **divisor** on C is a formal sum

$$D = \sum_{P \in C(\Bbbk)} n_P(P),$$

where $n_P \in \mathbb{Z}$ and only finitely many n_P are non-zero. The **support** of the divisor D is then defined to be $\text{Supp}(D) = \{P \in C(\Bbbk) : n_P \neq 0\}$, and the **degree** of the divisor D is the integer $\deg(D) = \sum_{P(\Bbbk)} n_P$.

These integers n_P can be chosen arbitrarily (as long as only finitely many of them are non-zero), and any choice will result in a valid divisor for the curve C.
One can also introduce a partial order on the set of divisors in the following way:

Definition 5.3. [9, Page 32] For two divisors $\sum n_P(P)$ and $\sum m_P(P)$, we say that

$$\sum n_P(P) \leq \sum m_P(P)$$

if and only if $n_P \leq m_P$ for all P.

The set of all divisors forms a group under coefficient-wise addition, as stated by the following lemma.

Lemma 5.4. [6, Lemma 7.6.4] *The set of all divisors of a curve, denoted* $\mathrm{Div}_{\Bbbk}(C)$*, defines a group under addition. The set* $\mathrm{Div}^0_{\Bbbk}(C) = \{D \in \mathrm{Div}_{\Bbbk}(C) : \deg(D) = 0\}$ *defines a subgroup of* $\mathrm{Div}_{\Bbbk}(C)$*.*

We now define the divisor of a function over a plane projective curve C.

Definition 5.5. [9, Page 32] Let $\phi \in \Bbbk(C)^*$, then there exist two polynomials $G(x, y, z)$, $H(x, y, z)$ of the same degree defining plane projective curves D and E, respectively, such that $\phi \not| G$ and $\phi \not| H$ and $\phi = \frac{G(x,y,z)}{H(x,y,z)}$. For any point $P \in C$, set

$$v_P(\phi) = \mathcal{I}(P, C \cap D) - \mathcal{I}(P, C \cap E).$$

Then

$$\mathrm{div}(\phi) = \sum_{P \in C(\Bbbk)} v_P(\phi)(P)$$

More intuitively, using notation as above, one can say that the divisor of a function ϕ is given by the points of intersection of C and D minus the points of intersection of C and E, taking into account multiplicities.

The divisor of a function is also called a **principal divisor** [6, Definition 7.7.2]. We define

$$\mathrm{Prin}_k(C) = \{\mathrm{div}(f) : f \in \Bbbk(C)^*\}.$$

The concepts of a divisor and a divisor of a function can also be defined over projective curves (not necessarily plane), which are projective varieties of dimension one. In this case, $v_P(\phi)$ is defined as in definition 7.4.5 of [6]. To define these concepts in this more general setting is beyond the scope of this thesis. For non-singular projective curves, this can be found in [6].

The divisors of a function over a non-singular projective curve actually form a subgroup of all divisors over said curve, as given by the following lemma.

Lemma 5.6. [6, Lemma 7.7.6] $\mathrm{Prin}_{\Bbbk}(C)$ *is a subgroup of* $\mathrm{Div}_{\Bbbk}(C)$ *under addition.*

We can also state the following theorem.

Theorem 5.7. [6, Theorem 7.7.11] *Let* C *be a projective curve over* $\Bbbk$ *and let* $f \in \Bbbk(C)^*$*. Then* $\deg(\mathrm{div}(f)) = 0$*.*

Proof. We will prove this theorem for plane projective curves. The more general proof can be found in [6].
Let C be a plane projective curve. We recall that $f \in \Bbbk(C)^*$ can be written as a fraction of two polynomials of same degree, i.e., $f = \frac{g}{h} \in \Bbbk(C)^*$. We then know that the divisor of f on C is given by the zeroes of g minus the zeroes of h, taking into account multiplicities. By Bézout's theorem, we know that there will be exactly as many points in the intersection of the curve defined by $g = 0$ and C as in the intersection of the curve defined by $h = 0$ and C. As the degree of the divisor equals the number of points in the first intersection minus the number of points in the second intersection, we find that the degree of the divisor of f will equal zero. □

This theorem tells us that all principal divisors have degree zero, which has major implications: if all principal divisors have degree zero, we can conclude that $\mathrm{Prin}_{\Bbbk}$ is a subgroup of $\mathrm{Div}^0_{\Bbbk}$, which is important for defining the degree zero divisor class group:

Definition 5.8. [6, Definition 7.8.1] The (degree zero) **divisor class group** of a non-singular projective curve C over $\Bbbk$ is $\mathrm{Pic}^0_{\Bbbk}(C) = \mathrm{Div}^0_{\Bbbk}(C)/\,\mathrm{Prin}_{\Bbbk}(C)$.

We remark that this group is well-defined as the principal divisors over a non-singular curve always have degree zero and thus form a subgroup of the degree zero divisors on said curve. We also have to note that all groups defined in this section are abelian (since the group law on $\mathrm{Div}_{\Bbbk}(C)$ is abelian), and we thus find that the quotient $\mathrm{Pic}^0_{\Bbbk}(C)$ is well-defined.

Now that we have defined all important algebraic structures within divisor theory, we introduce a definition on linear equivalence.

Definition 5.9. [6, Definition 7.8.1] For any two divisors $D, D' \in \mathrm{Div}_{\Bbbk}(C)$ on a non-singular projective curve C, we say that they are **linearly equivalent** (denoted $D \sim D'$) if there exists a function $f \in \Bbbk(C)^*$ such that $\mathrm{div}(f) = D - D'$. In this case, we know that $D - D' \in \mathrm{Prin}_{\Bbbk}(C)$.

We can now also define the intersection divisor. We assume that the points $P_1, \ldots, P_n$ are the points in the intersection of C and D, then the intersection divisor is defined as follows:

Definition 5.10. The **intersection divisor** of curves C and D is given as $(C \cdot D) = \sum_{j=1}^{n} \mathcal{I}(P_j, C \cap D)(P_j)$.

We note that the intersection divisor is an element of the divisors on C, but also of the divisors on D as the points with non-trivial coefficients are on both C and D.

5.2 One-to-one Correspondence

Using the degree zero divisor class group, we can define a one to one correspondence between elements in this group and points of specific curves in the following way:

Theorem 5.11. [6, Theorem 7.9.8] *Let C be a non-singular projective curve of genus one, and let $\mathcal{O}$ be a point on C. Then there is a one-to-one correspondence between this curve C and $\mathrm{Pic}^0_{\Bbbk}(C)$ given by $P \mapsto [(P) - (\mathcal{O})]$.*

Here, $[(P) - (\mathcal{O})]$ denotes the class of the divisor $(P) - (\mathcal{O})$.

Remark 5.12. The point $\mathcal{O}$ can be chosen arbitrarily.

The proof of this theorem will be omitted, but can be found in section 7.9 of [6].

This one-to-one correspondence, which we will denote by α, will allow us to transfer the group structure of the $\mathrm{Pic}^0_{\Bbbk}$ group to the curve of genus one. To show this, we now fix an element $\mathcal{O}$.
The map α takes points P from the curve C and maps them to the class of divisors of degree zero $[(P) - (\mathcal{O})]$. If we take two points P and Q on our curve C of genus one, then we find that $\alpha(P) + \alpha(Q) = [(P) - (\mathcal{O})] + [(Q) - (\mathcal{O})] = [(P) + (Q) - 2(\mathcal{O})]$. But how do we then define the addition $P + Q$ on our curve?
For this we recall that our map α is bijective, and thus has an inverse, which we denote by $\beta = \alpha^{-1}$. We define $R \coloneqq \beta(\alpha(P) + \alpha(Q))$, then $P + Q \coloneqq R$. We observe that the maps α and β are bijective, and that therefore, the element R as we defined it here is unique. It remains to check the group axioms for this addition on our curve.

We first look at the **identity element**: We find that $\alpha(\mathcal{O}) = 0$, from which it follows that for all $P \in C$, $\alpha(P) + \alpha(\mathcal{O}) = \alpha(P)$. This gives us that $P + \mathcal{O} = P$ for all $P \in C$, and thus that $\mathcal{O}$ is the unit element for our addition on the curve of genus one.

To show that the addition on the curve satisfies the **closure** axiom is trivial: the map is defined to take elements from our curve to an element on our curve. Thus, this addition on our non-singular curve of genus one satisfies the closure axiom.

To show the **existence of an inverse**, we use that we just determined the unit element of this addition on our curve of genus one, i.e. we want to find for any $P_1 \in C$ the existence of an element $P_2 \in C$ such that $P_1 + P_2 = \mathcal{O}$, where P_2 would then be called the inverse of P_1. We note that we know of the existence of an inverse element in the $\mathrm{Pic}^0_{\Bbbk}(C)$ group: there exists a $D \in \mathrm{Pic}^0_{\Bbbk}(C)$ such that $\alpha(P_1) + D = 0$. We now define $P_2 \coloneqq \beta(D)$. Then P_2 will be well-defined as the correspondence is one-to-one, and will satisfy that $P_1 + P_2 = \mathcal{O}$ with $P_2 \in C$.

The proof of **associativity** of the addition on curves of genus one also follows from the bijectivity of the maps α and β and the fact that $\mathrm{Pic}^0_{\Bbbk}(C)$ is a group, but will not be shown explicitly.

We conclude that theorem 5.11 indeed allows us to transfer the group structure from the group $\mathrm{Pic}^0_{\Bbbk}(C)$ to the non-singular curve C of genus one.

Corollary 5.13. Let C be a non-singular projective curve of genus one and let $\mathcal{O} \in C$. We can define an abelian group law on C with unit element $\mathcal{O}$ as follows: $C \times C \to C$ is given by $(P_1, P_2) \mapsto \beta(\alpha(P_1) + \alpha(P_2))$.

5.3 Desingularization

The previous two sections defined divisor theory for non-singular projective curves, which leads us to a problem: the curve we want to consider will be singular. We will require the theory defined above, and will thus have to justify our use of it. This section will introduce a non-singular curve that is almost bijective with our singular quartic and will solve our problem.

Proofs of the results of this section are beyond the scope of this thesis. For the special case of twisted Edwards curves, all results of this section were made explicit in [6].

We first have to introduce the curve that is of our interest: the singular quartic of genus one.

Definition 5.14. A **singular quartic of genus one** is a plane projective curve defined by a polynomial of degree four that has two nodal singularities.

This curve is usually denoted Q, and we know from example 3.5 that a quartic with two nodal singularities will indeed be of genus one. With this curve, however, we will not be able to use the one-to-one correspondence to transfer the group law from $\mathrm{Pic}_{\Bbbk}(Q)$ to Q. The following theorem will be the first step in the justification of our use of the theory discussed for non-singular curves.

Theorem 5.15. [4, §4.4.1] *Let Q be a plane projective quartic curve over field $\Bbbk$ with two nodal singularities N_1, N_2 (i.e., of genus one). Then there exists a non-singular projective curve $\tilde{Q}$ over field $\Bbbk$ of genus one and a map $\pi : \tilde{Q} \to Q$ such that*

1. $\#\pi^{-1}(P) = 1$ *for all* $P \in Q \setminus \{N_1, N_2\}$
2. $\#\pi^{-1}(N_i) = 2$ *for* $i \in \{1, 2\}$

This theorem tells us that the non-singular points of Q are in one-to-one correspondence with points on $\tilde{Q}$, which gives us an almost bijective relation between the two curves. The singularities have a different correspondence to the new curve, which makes the relation not a proper bijection. In other words, this theorem tells us that there is a birational equivalence between the curves Q and $\tilde{Q}$ given by map π; they are equivalent except for a small set: here the singular points on Q.

Throughout the remaining sections of the thesis, we will denote points $\tilde{P} \in \tilde{Q}$ such that $\pi(\tilde{P}) = P$ for all $P \in Q$ that are non-singular.

Before we state the following theorem, we need to recall that the curves Q and $\tilde{Q}$ are varieties over $\Bbbk$ of dimension one.

Theorem 5.16. [6, Theorem 5.5.28] *Let X and Y be varieties over $\Bbbk$. Then X and Y are birationally equivalent over $\Bbbk$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$ (isomorphic as fields).*

We thus find that Q and $\tilde{Q}$ have isomorphic function fields. The map $\pi^* : \Bbbk(Q) \to \Bbbk(\tilde{Q})$ given by $\phi \mapsto \phi \circ \pi$ is an isomorphism.

We know that a group law exists on $\tilde{Q}$ from corollary 5.13, and the fact that the function fields of Q and $\tilde{Q}$ are isomorphic will allow us to describe this group law on $\tilde{Q}$ using geometry on Q. Before we can do that, however, we need to relate the divisors of functions on Q and $\tilde{Q}$ to each other. For this, we state the following fact. It follows from the definition of $v_{\tilde{P}}(\tilde{\phi})$ and the fact that we have isomorphic function fields.

Fact 5.17. For $P \in Q \setminus \{N_1, N_2\} := Q^{ns}$ and $\phi \in \Bbbk(Q)^*$, we have $v_P(\phi) = v_{\tilde{P}}(\tilde{\phi})$, where $\tilde{P} \in \tilde{Q}$ such that $\pi(\tilde{P}) = P$ and $\tilde{\phi} \in \Bbbk(\tilde{Q})$ such that $\tilde{\phi} := \pi^*(\phi)$.

From this, it follows that the divisor of a function over Q can be identified with the divisor of the same function over $\tilde{Q}$ by identifying P with $\tilde{P}$ for all points $P \in Q^{ns}$ when the functions on Q do not contain zeroes or poles at the singularities. But if the divisor contains no nodes on Q, then it is not immediately clear that it also does not contain nodes on $\tilde{Q}$. For this, we have the following theorem, which follows directly from the isomorphic function fields of Q and $\tilde{Q}$:

Theorem 5.18. *Let $\phi \in \Bbbk(Q)^*$, and let $\tilde{\phi} := \pi^*(\phi) \in \Bbbk(\tilde{Q})^*$. Let $P \in Q$. If $(P) \notin \operatorname{div}(\phi)$, then*

$$\pi^{-1}(P) \cap \operatorname{div}(\tilde{\phi}) = \varnothing.$$

This theorem holds for both non-singular and singular points $P \in Q$. We thus have that if the divisor on Q contains no nodal singularities, the divisor also will not contain points on $\tilde{Q}$ that map to the nodal singularities under π^{-1}. Taking into account that the divisor over Q can be identified with the divisor over $\tilde{Q}$, we thus remark that we can compute $\operatorname{div}(\tilde{\phi})$ in $\operatorname{Div}^0_{\Bbbk}(\tilde{Q})$ using functions on Q.

We have now justified our use of a geometric construction on Q using only the non-singular points to describe a group law on $\tilde{Q}$. The next chapter will thus deal with two curves: the singular plane quartic of genus one (denoted Q), and the corresponding non-singular curve of genus one (denoted $\tilde{Q}$). We will describe a group law on $\tilde{Q}$, using a geometric construction on Q.

5.4 Curves in Weierstrass Form

To demonstrate how one would show that a geometric construction gives a group law on a curve using divisor theory, we will do so for curves in Weierstrass form. For these curves, we understand the group law and its construction well, and, most importantly, we already know that the construction gives a group law.

We recall that a point P_3 is constructed from P_1 and P_2 by taking the line through P_1 and P_2, which we will denote $L_1 : l_1 = 0$. This line will have a third intersection point with the curve in Weierstrass form, denoted P_3'. We will then find P_3 by taking the line through $\mathcal{O}$ (the point at infinity, which was earlier denoted ∞) and P_3' to find the third intersection point, which will be P_3. This line through P_3' and $\mathcal{O}$, we denote by $L_2 : l_2 = 0$.
We recall that a curve in Weierstrass form is non-singular, and we thus do not need the previous section on desingularization for this example.
We find the following theorem.

Theorem 5.19. *Let C be a curve in Weierstrass form over $\Bbbk$. Let the points $P_1, P_2, P_3, \mathcal{O} \in C$ be as above. Then we have that*

$$\operatorname{div}\left(\frac{l_1}{l_2}\right) = (P_1) + (P_2) - (P_3) - (\mathcal{O}).$$

Proof. The polynomials l_1, l_2 are of the same degree and both define curves over $\Bbbk$. Moreover, $\frac{l_1}{l_2} \in \Bbbk(C)^*$, so we find that the divisor of $\frac{l_1}{l_2}$ is given by the points of intersection of C and l_1 minus the points of intersection of C and l_2, taking into account multiplicities. We thus find that

$$\begin{aligned}\operatorname{div}\left(\frac{l_1}{l_2}\right) &= (P_1) + (P_2) + (P_3') - (P_3') - (P_3) - (\mathcal{O}) \\ &= (P_1) + (P_2) - (P_3) - (\mathcal{O}).\end{aligned}$$

□

While we now have now found this divisor, we have yet to figure out how this gives us a group law on the curve in Weierstrass form. This requires the following theorem.

Theorem 5.20. *Let $P_1, P_2, P_3, \mathcal{O}$ as above. Then $P_1 + P_2 = P_3$, where "+" is addition on C with unit element $\mathcal{O}$.*

Proof. We recall that two divisors D and D' were defined to be linearly equivalent if there exists a function $f \in \Bbbk(C)^*$ such that its divisor equals $D - D'$. We then knew that $[D - D'] = 0$ in $\operatorname{Pic}^0_{\Bbbk}(C)$.
Using the previous theorem, we thus find that

$$[(P_1) + (P_2) - (P_3) - (\mathcal{O})] = 0,$$

or equivalently,

$$[(P_1) - (\mathcal{O})] + [(P_2) - (\mathcal{O})] = [(P_3) - (\mathcal{O})],$$

or

$$\alpha(P_1) + \alpha(P_2) = \alpha(P_3),$$

where we recall the map α from section 5.2. We can now use the map $\beta = \alpha^{-1}$ to find

$$P_3 = \beta(\alpha(P_1) + \alpha(P_2).$$

We recall that a curve in Weierstrass Form is non-singular and of genus one, which means that by corollary 5.13 we find that the geometric construction given in chapter four defines a group law on C. □

This proof is much shorter and cleaner than the proof we gave in chapter four, which is why we will present a similar proof for the group law on quartics of genus one in the following chapter.

6 Quartics of Genus One

After having seen the group law on elliptic curves in Weierstrass form and having discussed the required divisor theory, we would like to construct the group law on quartics of genus one. We first introduce the addition of points on a singular quartic of genus one (i.e. a quartic with two nodal singularities), and will then show that this addition indeed defines a group law on the corresponding non-singular curve of genus one.

We remark that throughout this chapter, all points $P_1, P_2, P_3, \mathcal{O}, \mathcal{O}'$ must be non-singular.

6.1 Construction of P_3

Taking the naive approach, one would add two points $P_1, P_2 \in Q$, where Q is our singular quartic of genus one, by again taking the line through them and looking at the points of intersection of this line with the quartic. However, Bézout's theorem tells us that there will be two extra points (aside from P_1 and P_2) in this intersection. Because of this, addition would not be well-defined when taking this approach.
Instead of intersecting the quartic with the line through P_1 and P_2, we want to intersect it with the conic through the two points. However, two points do not uniquely define a conic. For this, one needs five points (of which no three are collinear, and counting multiplicities) [11, Page 286]. We thus need to define five points on our quartic, of which P_1 and P_2 are two points. For this, we consider the singularities N_1 and N_2 (recall that we have a quartic of genus one, i.e. a quartic with two singularities as seen in example 3.6). Additionally, we choose a point, denoted $\mathcal{O}'$ on our quartic that is not one of the singularities, and take the conic defined by the five points $P_1, P_2, N_1, N_2, \mathcal{O}'$.
We construct a point P_3 from P_1 and P_2 as follows:
We first take the conic $C : \phi = 0$ through the points $P_1, P_2, \mathcal{O}', N_1$ and N_2. This conic will have eight points of intersection with the quartic, seven of which have been found taking into account that the multiplicity of the nodal singularities will be at least two. We denote the eighth point of intersection by R. We then take the line through R and N_1 and denote it $L_1 : l_1 = 0$. The intersection between this line and the quartic will consist of four points (counting multiplicities) and we so far have three (as the nodal singularity counts as at least two points). We denote the fourth point of intersection with P_3.
We also construct the line $L_2 : l_2 = 0$ that goes through $\mathcal{O}'$ and N_2. This line will have that its fourth intersection point with the quartic is $\mathcal{O}$, as the nodal singularity again counts as at least two points.
Similarly to the curves in Weierstrass form, this construction can be visualized, as seen in figure 6.1. The star-shaped figure in the center is the curve Q, the dash-dotted line is the conic, and the dotted line is the line through R and N_1

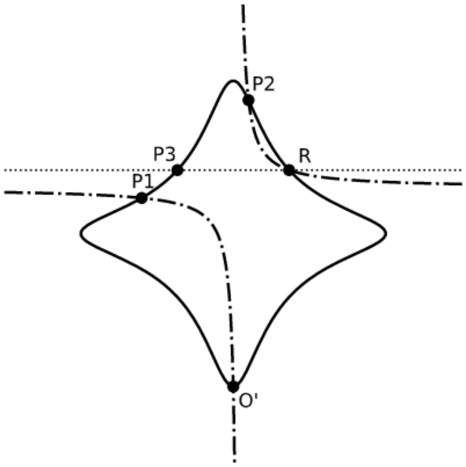

Figure 6.1: Visualization of finding P_3 from P_1 and P_2.

6.2 Group Law

We have defined the construction of a third point out of two points on a singular quartic of genus one. Left now, is to show that the construction as described above gives us a well-defined group law on the non-singular curve of genus one $\tilde{Q}$, which we will prove after the following theorem.

Theorem 6.1. *Let Q be a quartic with two nodal singularities N_1 and N_2 over $\Bbbk$. Let P_1, P_2 and P_3 be as above. Then we have*

$$\operatorname{div}\left(\frac{\phi}{l_1 l_2}\right) = (P_1) + (P_2) - (P_3) - (\mathcal{O}).$$

Proof. We will let our quartic be defined by a polynomial $F(x, y)$ of degree four, i.e. $Q : F(x, y) = 0$. We take the conic through the points $P_1, P_2, \mathcal{O}', N_1, N_2$ and let ϕ be a degree two polynomial giving the conic as required, i.e. $C : \phi = 0$ gives us the conic through these five points.
We now consider the intersection divisor $(C \cdot Q)$. By the way we constructed the conic, and taking into account that the singularities are nodal and thus have intersection multiplicity at least two, we find that

$$(P_1) + (P_2) + (\mathcal{O}') + 2(N_1) + 2(N_2) \leq (C \cdot Q).$$

Counting these points, including their multiplicities, we find that the intersection only consists of seven points. By Bézout's theorem, we then find that there must exist an eighth point of intersection, denoted R. With this, we thus find that

$$(P_1) + (P_2) + (\mathcal{O}') + 2(N_1) + 2(N_2) + (R) = (C \cdot Q).$$

We remark that R can be one of the points already in the intersection (and with that increasing the intersection multiplicity of that point by one), but does not have to be.

We now recall two lines that we defined in the previous section. The first line, we recall to be the line through R and N_1, and was denoted $L_1 : l_1 = 0$. The intersection of this line and the quartic contains one more point: P_3.
The second line we recall to be the line through $\mathcal{O}'$ and N_2, and was denoted $L_2 : l_2 = 0$. It had one more point in the intersection with the quartic, denoted $\mathcal{O}$.
To summarize, we had defined two lines L_1, L_2 such that they have the following intersection divisors on the quartic Q:

$$(Q \cdot L_1) = (R) + (P_3) + 2(N_1),$$
$$(Q \cdot L_2) = (\mathcal{O}) + (\mathcal{O}') + 2(N_2).$$

We notice that all three curves C, L_1, L_2 are given by polynomials, and that ϕ is of the same degree as $l_1 l_2$. Moreover, we remark that our quartic Q does not divide $l_1 l_2$. Then we know (by definition 5.5) that

$$\operatorname{div}\left(\frac{\phi}{l_1 l_2}\right) = \sum_{P \in C(\Bbbk} v_P\left(\frac{\phi}{l_1 l_2}\right)(P).$$

This equation tells us that the divisor of the fraction $\frac{\phi}{l_1 l_2}$ equals the points of intersection of the conic and the quartic minus the points of intersection of both lines and the quartic. For this equation, however, we also need to take into account multiplicities. We recall that the multiplicity of a nodal singularity in these intersections will be at least 2, while the other points will have intersection multiplicity at least one (as the point R is allowed to equal any of the other points). With this, we find that

$$\operatorname{div}\left(\frac{\phi}{l_1 l_2}\right) = (P_1)+(P_2)+(\mathcal{O}')+2(N_1)+2(N_2)+(R)-(\mathcal{O})-(\mathcal{O}')-2(N_1)-(R)-(P_3)-2(N_2).$$

Cancelling terms gives us:

$$\operatorname{div}\left(\frac{\phi}{l_1 l_2}\right) = (P_1) + (P_2) - (P_3) - (\mathcal{O}).$$

□

We found a divisor over Q in which all points are non-singular. This means that we can also consider the divisor over the non-singular curve $\tilde{Q}$:

$$\operatorname{div}\left(\frac{\tilde{\phi}}{\tilde{l}_1 \tilde{l}_2}\right) = (\tilde{P}_1) + (\tilde{P}_2) - (\tilde{P}_3) - (\tilde{\mathcal{O}}).$$

Using this divisor on our non-singular curve $\tilde{Q}$, we will now show that the construction of P_3 as defined above on Q defines a group law on $\tilde{Q}$ with unit element $\tilde{\mathcal{O}}$.

Theorem 6.2. *Let $P_1, P_2, P_3, \mathcal{O}, \mathcal{O}'$ be as in theorem 6.1. Then $\tilde{P}_1 + \tilde{P}_2 = \tilde{P}_3$, where "+" is addition on $\tilde{Q}$ with unit element $\mathcal{O}$.*

Proof. We recall that we said two divisors $\tilde{D}$ and $\tilde{D}'$ to be linearly equivalent if there exists a function $\tilde{f} \in \Bbbk(\tilde{Q})^*$ such that its divisor equals $\tilde{D} - \tilde{D}'$. In this case, $[\tilde{D} - \tilde{D}'] = 0$ in $\mathrm{Pic}^0_{\Bbbk}(\tilde{Q})$. We note that $\frac{\tilde{\phi}}{\tilde{l}_1 \tilde{l}_2} \in \Bbbk(\tilde{Q})$, and thus find that in $\mathrm{Pic}_{\Bbbk}(\tilde{Q})$,

$$[(\tilde{P}_1) + (\tilde{P}_2) - (\tilde{P}_3) - (\tilde{\mathcal{O}})] = 0.$$

This is equivalent to

$$[(\tilde{P}_1) - (\tilde{\mathcal{O}})] + [(\tilde{P}_2) - (\tilde{\mathcal{O}})] = [(\tilde{P}_3) - (\tilde{\mathcal{O}})]$$

From this, it follows that

$$\alpha(\tilde{P}_1) + \alpha(\tilde{P}_2) = \alpha(\tilde{P}_3).$$

Using the inverse map β, we thus find that

$$\tilde{P}_3 = \beta(\alpha(\tilde{P}_3)) = \beta(\alpha(\tilde{P}_1) + \alpha(\tilde{P}_2)) = \tilde{P}_1 + \tilde{P}_2.$$

We recall now that $\tilde{Q}$ is a non-singular curve of genus one, which means that by corollary 5.13, $\tilde{P}_3 = \tilde{P}_1 + \tilde{P}_2$ defines a group law on $\tilde{Q}$ with unit element $\tilde{\mathcal{O}}$.

We have thus shown that the construction of addition of non-singular points on Q defines a group law on $\tilde{Q}$. □

Remark 6.3. To describe the group law on $\tilde{Q}$ for points not satisfying the conditions of theorem 6.1 after mapping them to Q, one would have to work with $\tilde{Q}$ explicitly. For twisted Edwards curves, this is done in theorem 9.12.18 of [6].

Remark 6.4. This group law is not unique, as we also could have taken any other non-singular point for $\mathcal{O}'$, or could have taken the line through R and N_2 to find P_3. These choices would have resulted in a well-defined group law on $\tilde{Q}$, too.

6.3 Twisted Edwards Curves

While we have kept the proof of the non-singular curves of genus one being a group with the addition coming from the corresponding singular quartic as described in section 6.1 very abstract, we remark that we can also apply this to specific examples of quartics of genus one. For this, we study the twisted Edwards curves. These curves were introduced by Edwards in 2007 [2].

Definition 6.5. [2, Definition 2.1] Twisted Edwards curves are quartics and given by

$$ax^2 + y^2 = 1 + dx^2y^2,$$

where the polynomial is taken over a field $\Bbbk$ with characteristic not two and for which we fix two distinct and non-zero elements $a, d \in \Bbbk$.

The name of these twisted Edwards curves implies that non-twisted Edwards curves also exists, and they can be found by setting $a = 1$. These curves are called Edwards curves.

Lemma 6.6. [1, §2] *A twisted Edwards curve is a singular quartic of genus one, whose two singularities are at infinity and are nodal.*

Proof. Trivially, the twisted Edwards curve is a quartic. From example 3.4, we know that $N_1 = [1, 0, 0]$ is indeed a singularity and is nodal. Entirely analogously, one can show that $N_2 = [0, 1, 0]$ is also a nodal singularity of the twisted Edwards curve. Lastly, we note that N_1 and N_2 are both points at infinity.
One can also show, similarly to example 3.4, that the twisted Edwards curve has no other singularities.
From this, it follows that the twisted Edwards curve is indeed singular, and, by example 3.5, it is indeed a curve of genus one. □

The point $\mathcal{O}'$ is given to be the point $(0, -1)$ in [1]. We would now like to use the approach seen in the previous sections to find the point $\mathcal{O}$ explicitly using that $\mathcal{O}'$ is given as such, and to visualize what addition on a curve $E_{a,d}$ would look like in these cases.

Example 6.7. We can find two different valid group laws on this twisted Edwards curve as noted in remark 6.4, and we will discuss and visualize both.
First, we look at the case where $\mathcal{O}$ is found by taking the line through $\mathcal{O}'$ and N_2. We observe that we know both points defining the line, which allows us to give the explicit formula. For this, we first take the point $\mathcal{O}'$ to the projective plane to find $\mathcal{O}' = [0, -1, 1]$. Then the line through $\mathcal{O}'$ and N_2 is given by

$$L_1 : l_1 = -x + y + z = 0.$$

We recall that N_2 will have multiplicity two in the intersection between $E_{a,d}$ and L_2 and thus find that the fourth point $\mathcal{O}$ is given by $\mathcal{O} = [0, 1, 1]$. This point is given by $(0, 1)$ in the affine plane.
We now find the point P_3 using the line through R and N_1. This case has been visualized in figure 6.2.

Analogously, taking the line through $\mathcal{O}'$ and N_1 to find $\mathcal{O}$ gives us the line

$$L_1 : l_1 = x = 0.$$

With this, we find that the fourth point of intersection between $E_{a,d}$ and L_1 is $\mathcal{O} = [0, -1, 1] = \mathcal{O}'$, or $\mathcal{O} = (0, -1)$ in affine coordinates.
Switching the line to find $\mathcal{O}$ also implies that we find a different point P_3 that will equal $P_1 + P_2$. This case is visualized in figure 6.3.

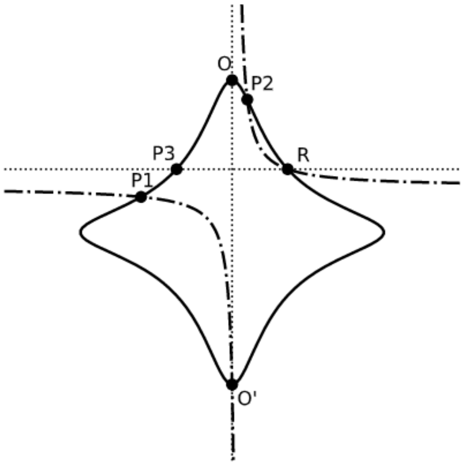

Figure 6.2: Visualization of finding $\mathcal{O}$ with L_2.

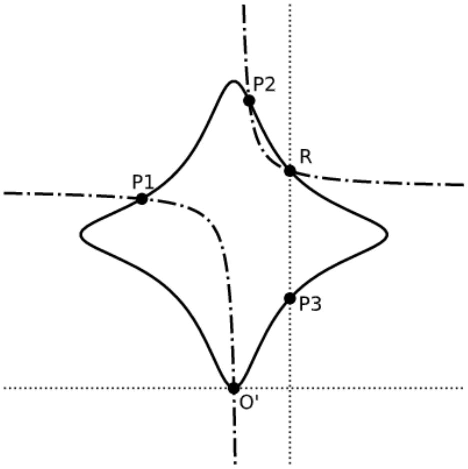

Figure 6.3: Visualization of finding $\mathcal{O} = \mathcal{O}'$ with L_1.

In the figures 6.2 and 6.3, the black line is the twisted Edwards curve with constants $a = 1$, $d = -30$, the dash-dotted line is the conic and the dashed lines are the lines L_1 and L_2.

Remark 6.8. Changing the point $\mathcal{O}'$ can actually give us the same group law if it leaves $\mathcal{O}$ unchanged, as we use the same correspondence to $\mathrm{Pic}^0_{\Bbbk}$. We can visualize this for the twisted Edwards curve $E_{1,-30}$ we saw before. In figure 6.4, we set the point $\mathcal{O}'$ to be $\mathcal{O}$. In this case, we find $\mathcal{O}$ from $\mathcal{O}'$ by taking the line through $\mathcal{O}'$ and N_1, which means the point P_3 is found by taking the line through R and N_2, as can be seen in figure 6.4. We observe, by comparing figures 6.2 and 6.4, that the point P_3 indeed is the same in both cases (here we took the same twisted Edwards curve and points P_1, P_2 for this comparison).
This holds not only in the case of these specific points P_1 and P_2. We note that by taking the conic through $\mathcal{O}$ instead of through $\mathcal{O}'$, we find that the eight intersection point (denoted here R) is the reflection of the point R in the original case over the line $y = -x$. As we now change the line through which we find $\mathcal{O}$ from $\mathcal{O}'$, we also change the line with which we find P_3 from the eight point of intersection between the conic and the quartic. This change, together with the reflection of the eight point of intersection, results in P_3 being the same point in both cases.
We can thus conclude that for each choice of $\mathcal{O}$, we find a unique group law.

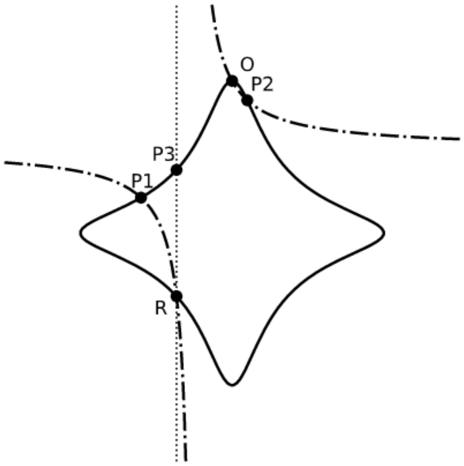

Figure 6.4: Visualization of $P_1 + P_2 = P_3$ with $\mathcal{O}' = \mathcal{O}$.

References

[1] Christophe Arene, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler, *Faster pairing computation*, arXiv preprint arXiv:0904.0854 (2009).

[2] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted edwards curves*, International conference on cryptology in africa, 2008, pp. 389–405.

[3] Frits Beukers, *Notes on algebraic curves*, 2011.

[4] Henri Cohen and Gerhard Frey, *Handbook of elliptic and hyperelliptic curve cryptography*, Taylor Francis Group, LLC, 2006.

[5] David Steven Dummit and Richard M Foote, *Abstract algebra*, third, John Wiley and Sons, Inc., Hoboken, New Jersey, 2004.

[6] Steven D. Galbraith, *Mathematics of public key cryptography. version 2.0*, Cambridge University Press, Cambridge, 2012.

[7] Darrel Hankerson, Alfred Menezes, and Scott Vanstone, *Guide to elliptic curve cryptography*, Springer, 2004.

[8] Barry Mazur, *Arithmetic on curves*, Bulletin of the American Mathematical Society **14** (1986), no. 2, 207–259.

[9] J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006.

[10] Adrian Rice and Ezra Brown, *Why ellipses are not elliptic curves*, Mathematics Magazine **85** (2012), no. 3, 163–176.

[11] Joseph H Silverman and John Torrence Tate, *Rational points on elliptic curves: Undergraduate texts in mathematics*, second, Springer, Cham, 2015.

[12] Lawrence C Washington, *Elliptic curves: number theory and cryptography*, second, Chapman and Hall/CRC, Boca Raton, Florida, 2003.