rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Tropical Elliptic Curves and j-invariants.

Bachelorondezoek Wiskunde

Augustus 2011

Student: P.A. Helminck

Eerste Begeleider: Prof. dr. J.Top

Tweede Begeleider: Drs. H.G. Vinjamoor

TROPICAL ELLIPTIC CURVES AND j-INVARIANTS

PAUL HELMINCK

ABSTRACT. In this bachelor's thesis, the j-invariant for elliptic curves over the field of Puiseux series, $\mathcal{P}$, will be discussed. For elliptic curves over any algebraically closed field, for instance $\mathbb{C}$ or $\mathcal{P}$, we have that elliptic curves have the same j-invariant if and only if they are isomorphic to each other . Therefore every such j-invariant $\in \mathcal{P}$ will correspond to a class of isomorphic elliptic curves. Katz, Markwig and Markwig showed in [KMM00] that this j-invariant is related to the cycle length in the tropical world. In this paper we shall show that for every j-invariant we can find an elliptic curve and its corresponding tropical counterpart such that they obey the above relation.

This tropical counterpart can be found by the *tropicalisation* process. In this thesis we study the tropicalisation of a plane curve C over $\mathcal{P}$. We take such a curve C and then apply a logarithm map to every point in this curve. This will result in the *amoeba* of C. This new object will contain several tentacles and an eye. By scaling the logarithm map by a factor t, we can make these tentacles and eyes arbitrarily thin in a limiting process. The limit version will be called the *tropicalisation of* C.

This limit process can be generalised to any field k by means of a valuation. This valuation is a mapping $v : k \longrightarrow \mathbb{Q}$. In the limit process, the behaviour of the logarithm is determined precisely by the valuation at every point. Thus we can replace an analytic tool with a purely algebraic one, the valuation. The field of Puiseux series has a natural valuation on it, which is a generalisation of the usual degree of a polynomial.

Applying this to an elliptic curve over the field $\mathcal{P}$, we obtain a piece-wise linear curve known as the *tropical elliptic curve*. Most tropical elliptic curves will contain a bounded complex, also known as a *cycle*. It can be shown that the length of such a cycle is something that is shared by tropical elliptic curves which are related by morphisms. We therefore introduce a new invariant for tropical elliptic curves: j_{trop}.

Katz, Markwig and Markwig showed in [KMM00] that if we have an elliptic curve with $v(j) < 0$, then under certain mild conditions $v(j)$ will equal minus the cycle length. We show in this paper that for every j-invariant we can find an explicit elliptic curve with a tropicalisation having a cycle with length equal to $-v(j)$. That is, if $v(j) < 0$, then we can find an isomorphic elliptic curve with a tropicalisation having a cycle with length equal to $-v(j)$.
To show this we will use the method of reduction. The reduction of an elliptic curve over $\mathcal{P}$ to the field $\mathbb{C}$ deletes all powers of t in the coefficients and points (analogous to the reduction of an elliptic curve over $\mathbb{Z}$ to $\mathbb{Z}_p$). As in the analogous case, this requires the equation to be a so-called *minimal Weierstrass equation*. We show how to obtain such an equation and what properties these equations have.

Afterwards we perform the actual reduction, resulting in a curve over $\mathbb{C}$. This new curve might be singular over $\mathbb{C}$ however. An elliptic curve reducing to a singular curve is said to have *bad reduction*. If it reduces to a non-singular curve (which is then a smooth elliptic curve), we say that it has *good reduction*. These two types of reduction can be related to the valuation of the j-invariant. A curve with bad reduction will have $v(j) < 0$. To find a curve with a proper tropicalisation, we take a curve with bad reduction and show that it has a cycle with length equal to $-v(j)$.

Contents

1. Introduction

The aim of this bachelor's thesis is to understand a connection between certain algebraic varieties and their tropical counterparts. This connection may be vaguely described by saying that we start with something in the "normal" world (by which we mean something which is well understood, i.e. elliptic curves) and then look at what happens when we transfer this to the tropical world. This last world has received increased attention over the last 10 years (over 200 articles public on arXiv), for one due to its applications in various fields of mathematics. To mention a few: algebraic geometry, mathematical physics, mathematical statistics and graph theory, yet it also has many fruitful applications in more applied settings like biology and genetics.

In this tropical world everything takes a piece-wise linear form. One can already see why this is the case from the two operations on $\mathbb{R}$ we define for the tropical world: $\oplus = \min$ and $\odot = +$. Using these operations one can set up what is called tropical geometry. For instance a tropical line will be the union of three (normal) lines emanating from a certain point. These tropical lines behave as expected: two tropical lines will always intersect in 1 point. In fact one can set up a tropical analogue of *Bézout's Theorem*. Another theorem that also holds in this tropical setting is the *Riemann-Roch theorem*.

1.1. **Tropicalisation.**

One can study this tropical world and its geometry for its own intrinsic properties, which is already rewarding on its own. There is however a deep connection between tropical geometry and geometry. Suppose that we start with a field k. Every such field comes with a so-called valuation. This valuation can be seen as a measuring tool, as it maps an element of the field to an element of $\mathbb{Q}$. Since any object in geometry is a set containing n-tuples of elements from the field k, we can apply this valuation to every individual element. This yields a subset of $\mathbb{Q}^n$, which can be completed (with respect to the basic Euclidean topology) to obtain something in $\mathbb{R}^n$. This is in fact (more or less) the tropicalisation of an algebraic variety.

This tropicalisation can also be obtained in another way for curves over the field of complex numbers (or more generally for the residue field corresponding to the valuation). Take a curve with n coordinates in $\mathbb{C}$. We can apply the usual (real) logarithm on the modulus of every coordinate. This yields a picture in $\mathbb{R}^n$ which is called the *amoeba* of the complex curve. The fact that this picture is called an amoeba stems from the tentacle-shaped portions of the picture leading away from a center body, known as the *eye* of the amoeba. The idea now is to artificially introduce a parameter t to the complex curve so that we can take a limit. This limit will result in reducing the area of the tentacles and the eye to zero. But it can be shown that in this limit case, the logarithm is just equal to the valuation mentioned earlier. This

valuation is however algebraic of nature, whereas the limit process is analytic. Since we're interested in algebraic curves, we proceed with the valuation.

1.2. **Algebraic Geometry and Elliptic Curves.** The algebraic objects in geometry that we alluded to are called algebraic varieties. We won't give a precise definition of algebraic varieties just yet, but basically they are the zero set of a collection of polynomials. The study of these algebraic varieties is called algebraic geometry. This field of mathematics can be seen as a mix of *linear algebra* and *algebra*: linear algebra studies the set of solutions to multiple linear equations and algebra studies the set of solutions to polynomial equations. Rather than finding all the solutions of given equations (which can be hard or even impossible, an example of which is solving the general quintic equation by radicals), one hopes to find more information about the nature of these solutions by considering the geometry of the specific problem. For instance vector spaces naturally arise from solving linear equations as the spaces which are invariant under scaling and addition (a property which linear mappings preserve).

An important problem in algebraic geometry is the classification of curves. A way to do this is by means of the genus of a curve. For a curve over $\mathbb{C}$ the genus represents the amount of "holes" in the curve. So for instance a complex sphere has genus 0 and a complex torus has genus 1. There is in fact a definition for the (geometric) genus of a curve over arbitrary fields, which is harder to apply in practice. It is however still an important classification tool: two isomorphic curves will have the same genus. As a starting point, consider curves of genus 0. Curves of genus 0 are particularly simple, since we can always find a rational parametrisation for these curves given any particular solution. This technique was already known to Diophantus $\pm$200 A.D. In fact, he was the first one to try this technique on a projective curve of genus 1, which is now called an *elliptic curve*. He found that he needed two rational solutions to obtain another rational solution. This latter construction is now known to be equivalent to the group law on elliptic curves. Our focus for the remainder of the paper shall be on these elliptic curves.

As briefly mentioned in the previous paragraph, these elliptic curves have a group law on them. This means that given two points P_1 and P_2, we can construct $P_3 = P_1 + P_2$ such that this operation satisfies all the properties necessary for a group (moreover, we can find an identity element and inverses). This group operation gives the elliptic curve some more algebraic structure which can be exploited in numerous ways.

Given this structure, we can look at the mappings preserving this structure, known as isomorphisms. These isomorphisms relate one elliptic curve to another and basically represent the same elliptic curve (that is, the same structure). It turns out that isomorphic elliptic curves are in fact related by one number: the *j-invariant*.

As the name suggests, this number is invariant under any isomorphism used on the elliptic curve. This also works the other way around: two elliptic curves with the same j-invariant are isomorphic to each other over an algebraically closed field.

Our field of choice still has to be specified. In this paper we shall mainly use the field of formal Puiseux series. This field is an extension of the normal polynomial ring over the field of complex numbers. Instead of allowing only integer powers, one can have rational powers in the indeterminate. This allows one to define a valuation on these series: take the lowest power in the power series. So if we consider algebraic varieties, or in particular elliptic curves, over the field of Puiseux series, we can tropicalise them using this map. This will yield what is known as *tropical elliptic curves*.

These curves can be studied in multiple ways, one of them being the pictorial description as a subset of $\mathbb{R}^2$. This description requires you to solve several linear systems for every curve, which can become cumbersome when dealing with variables (in the coefficients) in your curve. We shall therefore adopt another way of describing tropical curves: by the *Newton subdivision*. This method uses Newton polygons and discrete geometry to quickly give the structure of a tropical curve.

1.3. **Tropical j-invariants and reduction.** The tools mentioned above allow us to study the main subject of this bachelor's thesis: tropical j-invariants. Having seen that every elliptic curve has an invariant quantity called the *j-invariant*, one might wonder if and how this quantity tropicalises. The resulting quantity is known as the tropical j-invariant and may be described as follows. Every smooth elliptic curve with a particular j-invariant has a bounded complex in $\mathbb{R}^2$. This bounded complex is known as a cycle. To every such a cycle one can associate its length. This length will be the tropical j-invariant.

However not all tropicalisations have a cycle. In fact, even taking the normal reduced Weierstrass form of an elliptic curve will yield nothing. The key lies in the xy-term, which is necessary for a tropical elliptic curve to have a cycle. This already shows that the tropical j-invariant is not an invariant connected to the usual isomorphisms. There is however a connection between normal j-invariants and tropical j-invariants. Suppose we have an elliptic curve with valuation of the j-invariant strictly smaller than zero. Assume also that the elliptic curve induces a triangulisation in the Newton subdivision. It can be shown that $-v(j)$ will be equal to the cycle length in this case.

Our main goal in this paper will be showing that we can find a representative of an elliptic curve (with the same j-invariant, valuation smaller than zero) such that its tropicalisation has the correct cycle length. In order to find this curve we will use the method of *reduction*. This method takes the elliptic curve and effectively cancels out all the terms from the indeterminate t, thereby leaving an elliptic curve over $\mathbb{C}$. This cancelling out can also be seen as "filling in $t = 0$". Before we can cancel out

these terms though, we have to make the corresponding equation minimal, which can be seen as making all the powers in the indeterminate greater than zero (something which certainly is necessary if we want to fill in $t = 0$).

Having found this minimal equation, we can apply the reduction mapping to obtain a new elliptic curve over $\mathbb{C}$. This curve may however be singular. The elliptic curve is then said to have *bad reduction*. If it reduces to a non-singular elliptic curve it is said to have *good reduction*. These two cases can be directly linked to the reduced discriminant (in fact $\tilde{\Delta} = 0$ means we have bad reduction). With a little more effort, one can show that these two cases can in fact be related to the valuation of the j-invariant. So for curves with bad reduction we would have $v(j) < 0$. Note that this is exactly the condition that is needed for a tropical elliptic curve to contain a cycle.

With this in mind, we proceed by taking a curve with bad reduction. By chosing the correct isomorphism, we can obtain a new elliptic curve which will have the correct cycle length. This result will be compared to that in [BPR11] and other implications of these theorems will be considered as well.

2. Polynomial rings and Puiseux Series

Given any field or more generally any commutative ring R, its polynomial ring $R[X]$ is defined as

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^n : a_i \in R, n \in \mathbb{N} \right\} \tag{1}$$

That is, it contains all algebraic expressions in the indeterminate X, as long as the expressions used are finite. One of the main features this ring lacks is *multiplicative inverses*. In this section we investigate how we can extend this polynomial ring such that it does have inverses and other useful algebraic properties.

In this bachelor's thesis we shall mainly be considered with objects over the field of complex numbers $\mathbb{C}$. Polynomials over this field have proven to be very useful in all sorts of applications due to the analytic structure $\mathbb{C}$ is endowed with. As motivation for the extensions made in the following sections, we shall quickly highlight the notable features of various polynomials over $\mathbb{C}$. As is known from complex function theory, every holomorphic function on $\mathbb{C}$ can be represented as an infinite series. In contrast, we have that differentiable functions over $\mathbb{R}$ can fail to have such a representation.

There are however more functions that can locally be expanded as an infinite power series. For instance, consider a function that is analytic on a neighbourhood except at a countable amount of points, called *poles*. The set of these functions is called the set of *meromorphic* functions on $\mathbb{C}$. To account for the occuring poles, we have to allow negative exponents in our polynomials. The resulting field is called the field of

Laurent series. Every meromorphic function on $\mathbb{C}$ can then be expanded as follows:

$$f(z) = \sum_{k>-\infty}^{\infty} a_k(z - z_0)^k \tag{2}$$

2.1. **Formal power series.** Infinite sums are not allowed in polynomial rings however (by definition). In order to talk about infinite sums, we have to introduce *formal power series*. Formal power series allow one to work with infinite series without resorting to analysis. A formal power series associates an infinite list of coefficients with an "infinite polynomial". This list can be algebraically manipulated as expected. When using manipulations on infinite series however, we should proceed with caution. For instance, evaluating an infinite series at any point in $\mathbb{C}$ is not allowed when considering these formal power series. Hence we shall mainly use their associated lists.

We begin with describing polynomials with positive powers (hence we are working over $\mathbb{C}[t]$). Take a sequence of elements in $\mathbb{C}$: $\{a_0, a_1...\}$. We set up a one-to-one correspondence between these sequences and infinite polynomials as follows:

$$\{a_0, a_1...\} \longrightarrow \sum_{k=0}^{\infty} a_k t^k \tag{3}$$

We denote the set of all these infinite polynomials by $\mathbb{C}[[t]]$. Such infinite polynomials can be added and multiplied by using the following rules

$$\{a_0, a_1....\} + \{b_0, b_1...\} = \{a_0 + b_0, a_1 + b_1...\} \tag{4}$$

and

$$\{a_0, a_1....\} \cdot \{b_0, b_1...\} = \{a_0 \cdot b_0, ..., \sum_{i=0}^{n} a_i b_{n-i}, ...\} \tag{5}$$

This simple algebraic form of infinite series might be deceiving at first. Normally, infinite series can't be defined without a metric or topology. Some infinite series converge, some diverge and some even converge conditionally. Formal power series however completely ignore these matters of convergence. A formal power series is just an infinite list of elements. Whether it converges or not is considered unimportant for the time being.

Note that every entry contains only a finite amount of normal operations in $\mathbb{C}$, so overall these new operations are well defined (an infinite amount of operations would require some sort of topology). Additive inverses are as usual and all the other ring properties follow as well.

We now investigate whether we can find multiplicative inverses. If the lowest nonzero coefficient of this polynomial is a_i, we say that it has *order* i. Now suppose we take a polynomial of order 0. This means that it has a constant leading term. We now claim any polynomial of order 0 is invertible (with the unitary element being $(1, 0, 0, ...)$). In fact, according to the definition of multiplication, the inverse can be found recursively by the following rules:

- $b_0 = 1/a_0$
- $b_1 = -\frac{a_1}{{a_0}^2}$
- $b_n = -(\sum_{i=1}^{n} a_i b_{n-i})/a_0$

From these formulae we immediately see that the condition "f has order 0" is both a necessary and sufficient condition for invertibility of an element in $\mathbb{C}[[t]]$. Power series in $\mathbb{C}[[t]]$ consequently do not always have inverses, which deprives this ring of the epithet "field". Luckily, this minor difficulty can be overcome. Take any polynomial f of order $m > 0$. Then we can write f as:

$$f = t^m \cdot g \tag{6}$$

where g is of order 0. So g is already invertible. All that is needed now is to find an inverse for t^m, but this is exactly t^{-m} in the field of Laurent series. Hence we have found inverses for every polynomial of order $m > 0$. Analogously we can find inverses for $-m < 0$ with m finite by noting the following:

$$f = t^{-m} \cdot g \tag{7}$$

with g once again having valuation 0. We know that g has an inverse and that the inverse of t^{-m} is t^m. Hence we have found an inverse for every element $\neq 0$ of $\mathbb{C}[[t]]$. The construction above gives the quotient field of $\mathbb{C}[[t]]$: $\mathbb{C}((t))$. In fact, we have shown that $\mathbb{C}[[t]][t^{-1}] = \mathbb{C}((t))$.

2.2. **Puiseux Series.** This field $\mathbb{C}((t))$ is called the field of formal Laurent series, which we will call L for now to avoid cumbersome notation later on. This field is again of characteristic zero (since $\mathbb{C}$ is of characteristic zero), but some properties are not preserved. One of them being algebraic closedness. For instance the polynomial $f = X^2 - t \in L[X]$ is irreducible over $L[X]$. In fact, all nth roots of t are absent in this field. We can add these nth roots by extending the field L. For instance, if we want the square root of t in our new field, we take the following field extension:

$$L \longrightarrow L[X]/(X^2 - t) := L(t^{1/2}) \tag{8}$$

The same procedure can be used for arbitrary nth roots of t. Now consider the following chain of field extensions:

$$L \subset L(t^{1/2}) \subset L(t^{1/6}) \subset ... \subset L(t^{1/n!}) \subset ... \tag{9}$$

Each of these extensions can be naturally embedded in the next extension by means of the identity map. Upon taking the infinite union, we obtain what is called the **field of Puiseux Series**. This infinite union is also known as the direct limit of this system. This new field contains all formal series with fractional powers. That is, it contains $t^{p/q}$ and all combinations of these powers (where $p, q \in \mathbb{Z}$), as long as the denominators occurring in these series are bounded. We can write this field $\mathcal{P}$ as:

$$\mathcal{P} := \cup_{n=1}^{\infty} L((t^{1/n!})) \tag{10}$$

where the double brackets are used to indicate we are still working with formal power series. A word of caution is in order: we do not allow formal power series with unbounded denominators. Consider the following sequence:

$$\{f_n\} = t^{-1} + t^{-1/2} + t^{-1/3} ... + t^{-1/n} \tag{11}$$

If we allow n to go to infinity, we obtain a series with fractional exponents which is *not* a Puiseux series. This might suggest that the field of Puiseux series is not complete (since we found a sequence "converging" to something outside our field). Note however that we cannot discuss convergence because we do not have a metric on our field $\mathcal{P}$ (a particular metric using the valuation can be used to show that this sequence is not a Cauchy sequence)

Having seen what does not constitute a Puiseux series, we now give several examples of proper Puiseux series:

- Any normal polynomial is again a Puiseux series, even when considering infinite series that are bounded below.
- Any Laurent series is a Puiseux series, since we still have negative powers in $\mathcal{P}$.
- $t^{-1/2} + t^{1/3}$ is a Puiseux series, since the powers of t are bounded.
- $e^t := 1 + t + t^2/2 + ...$ is also a Puiseux series

2.3. **Natural valuation.** Any element of $\mathcal{P}$ has a lowest power of t (similar to the case of the Laurent series). We can thus write an element as:

$$f = \sum_{i \in I} c_i t^{p_i/q_i} \tag{12}$$

where q_i is bounded below by some k. Since this k is finite, we can assign a number to every element of the field $\mathcal{P}$ by saying:

$$v(f) := \min\{p_i/q_i\} \tag{13}$$

For $f = 0$ we define $v(f) = \infty$. This mapping $v : \mathcal{P} \longrightarrow \mathbb{Q} \cup \{\infty\}$ is called the *natural valuation* on $\mathcal{P}$. Whenever we use the term "valuation" in the context of Puiseux series, we mean the natural valuation. We defer our discussion of general valuations till chapter 3.

For now, we would like to give several (obvious) properties of this valuation:

- $v(x) = \infty \iff x = 0$
- $v(x \cdot y) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$

In fact, the last property ("triangle inequality") can be made slightly stronger than it is now:

Proposition 2.1. *If $v(x) \neq v(y)$ then $v(x + y) = \min\{v(x), v(y)\}$.*

Proof. Suppose $x = \sum_{i\in I} c_i t^{p_i/q_i}$ and $y = \sum_{i\in I} d_i t^{p_i/q_i}$. Since $v(x) \neq v(y)$, we know that one of them must have lower valuation. Without loss of generality, assume that this is x. By termwise addition, we have that $x + y = \sum_{i\in I}(c_i + d_i)t^{p_i/q_i}$. Now look at the i_0 where $v(x) = p_{i_0}/q_{i_0}$. Then we have that $d_{i_0} = 0$, so that the $c_{i_0} \neq 0$ is the lowest coefficient of $x + y$. Therefore the valuation must be equal to $v(x)$. □

Remark 2.2. When we defined the Puiseux series, we added a certain new polynomial to the old polynomial ring. This old polynomial ring (or field in fact) also has a valuation on it. Consider the ring of polynomial functions on $\mathbb{C}$: $\mathbb{C}[t]$. Once again, we define the valuation of an element as the minimal power of t. We can extend this to the ring of Laurent polynomials. These notions of valuations naturally extend to the formal power series.

Remark 2.3. Let L be the field of formal Laurent series. Now consider the following extension:

$$L \subset L(t^{1/2}) \tag{14}$$

The valuation on L extends to the field $L(t^{1/2})$ by setting $v(t^{1/2}) = 1/2$. In fact, for every $t^{1/n}$, we can set $v(t^{1/n}) = 1/n$. Taking the infinite union leads to the same valuation as the one we defined for the Puiseux series. The difference between these constructions is that with this construction we see that every extension gives a so called *discrete valuation*. This means that the valuation takes values in a subset of $\mathbb{Q}$. In fact, for a given Puiseux series, we have that the valuation of the series can be given by a discrete valuation (since all powers are bounded).

2.4. **Reduction.** In this section we quickly highlight the main ideas of *reduction*. In section (3) these ideas will be made more precise using valuation rings and in section (6.2) these ideas will be used on elliptic curves over $\mathcal{P}$. The technique itself will already be used in the upcoming proof of the algebraic closedness of $\mathcal{P}$, which is the reason we mention the method here.
As an example, consider first the ring $\mathbb{Z}$. This is a principal ideal domain, which means that every ideal can be generated by one element. For every ideal $I = n\mathbb{Z}$, we can define the following quotient ring: $\mathbb{Z}/n\mathbb{Z}$. All multiples of n in this ring are modded out. This means that two elements are equal if and only if they differ a multiple of n.
For any prime p, we have that the ideal $p\mathbb{Z}$ is a maximal ideal; there is no bigger ideal containing this ideal other than the entire ring. Thus we have that the quotient ring is a field. For any element $n \in \mathbb{Z}$ we can use the division algorithm to write:

$$n = pq + r$$

with $r < q$. The map sending an element n in $\mathbb{Z}$ to its remainder is called the **reduction map**:

- $\phi_p : \mathbb{Z} \longrightarrow \mathbb{Z}$
- $n \longmapsto r \in \mathbb{Z}$

This map is a surjective (ring)homomorphism. The kernel is exactly $p\mathbb{Z}$.

Remark 2.4. This idea of reduction on $\mathbb{Z}$ can be generalised to $\mathbb{Q}$. In fact, when we define valuation rings we shall mainly work over fields.

We can repeat the same procedure for the field of complex Puiseux series (and consequently also for the field of formal Laurent series). We know that the field of complex Puiseux series $\mathcal{P}$ has a natural valuation on it. For a polynomial $f \in \mathcal{P}^*$ with

$$f = \sum_{i \in I} c_i t^{p_i/q_i}$$

it is defined as

$$v(f) := \min\{p_i/q_i\}$$

Reducing over this field will be filling in $t = 0$. We shall therefore first need a ring which contains all positive powers of t:

$$\mathcal{P}_+ := \{f \in \mathcal{P} : v(f) \geq 0\}$$

There is only one maximal ideal in this ring, namely all multiples of t:

$$\mathcal{M} = \{f \in \mathcal{P} : v(f) > 0\}$$

We can now define **reduction on** $\mathcal{P}$. As before it just the following mapping:

$$\begin{aligned}\phi: \quad \mathcal{P}_+ &\longrightarrow \mathbb{C} \\ f(t) &\longmapsto f(0)\end{aligned}$$

The same can be done for the field of formal Laurent Series (with exactly the same notation, only with a different valuation).

2.5. **Algebraic Closedness.** The reason we started adding roots of t to our field was to solve new equations. The roots we added were more or less arbitrary, and one might wonder whether we can solve anything a bit more complex, like $X^n + X = t$. The solution of this problem lies in the *algebraic closedness* of $\mathcal{P}$. This means that every polynomial equation with coefficients in $\mathcal{P}$ has at least one solution in $\mathcal{P}$. Or equivalently: the only irreducible elements of $\mathcal{P}[X]$ are of degree 0 or 1. This last characterisation will be used to prove that $\mathcal{P}$ is algebraically closed. Before we can begin the proof however, we will need one result which is primarily known for its use in p-adic analysis: *Hensel's Lemma*.

Lemma 2.5. *(***Hensel's Lemma***) Let F be a monic polynomial in Y with coefficients in $\mathbb{C}[[t]]$. Suppose the associated reduced polynomial $F_0 \in \mathbb{C}[Y]$ factors as*

$$F_0 = g \cdot h$$

for monic polynomials $g, h \in \mathbb{C}[Y]$ that are coprime (that is, they have no common factors). Then F factors as

$$F = G \cdot H$$

where G, H are monic polynomials in y with coefficients in $\mathbb{C}[[t]]$ such that $G_0 = g$ and $H_0 = h$.

Proof. We begin by adopting a special notation for F. Instead of grouping all the coefficients belonging to a certain Y^i, we write F as follows:

$$F = \sum_{i=0}^{\infty} F_i t^i$$

where all the F_i are polynomials in y containing no powers of t. Let the degree of F be m (in other words, m is the highest power of y in all the F_i). Since F is monic, we know that $\deg(F) = \deg(F_0)$. We furthermore have that $\deg(F_i) < m$ by definition. Let $r = \deg(g)$ and $s = \deg(h)$. We want to find

$$G = \sum_{i=0}^{\infty} G_i t^i \qquad \text{and} \qquad H = \sum_{i=0}^{\infty} H_i t^i$$

such that $G_0 = g$, $H_0 = h$ and $G_i, H_i \in \mathbb{C}[Y]$ of degree $< r$ (resp., $< s$) for $i > 0$. And we want F to be factorised by these two, that is, we want $F = GH$.
The condition $F = GH$ leads to a system of equations:

$$F_n = \sum_{i+j=n} G_i H_j.$$

This should be compared to the multiplication of formal series as defined in section (2.1). We shall show how to solve these equations by induction. For $n = 0$ we have $F_0 = gh = G_0 H_0$ (which was in our hypothesis). Now suppose all the G_j and H_i have already been found for $i, j < n$. The nth equation can be written as

$$G_0 H_n + H_0 G_n = F_n - \sum_{i=1}^{n-1} G_i H_{n-i} := U_n$$

The sum in U_n is up to $n-1$, so we know that $\deg(U_n) < m$ (by induction). To complete the induction step, we have to show that we can solve this equation for H_n and G_n such that these polynomials have degree $< r, s$ respectively.
From our hypothesis, we know that G_0 and H_0 are coprime. This means that $\gcd(G_0, H_0) = 1$. We claim that the ideal generated by two coprime polynomials is the entire ring. It is sufficient to prove that $1 \in k[y]$. We know that $k[y]$ is a principal ideal domain, so the ideal $(G_0) + (H_0)$ is generated by a single element of $k[y]$. This element is of course the $\gcd(G_0, H_0)$. Therefore $(G_0) + (H_0) = (1) = k[y]$. But this also means that we can find P and Q such that:

$$PG_0 + QH_0 = U_n$$

We now rewrite P in terms of H_0 by means of the division algorithm:

$$P = H_0 S + R$$

for $R, S \in k[y]$ with $\deg(R) < s$. Set $H_n = R$ and $G_n = Q + G_0 S$. These H_n and G_n solve the equation $G_0 H_n + H_0 G_n = U_n$. We only have to check that they're of the right degree. H_n has the right degree by definition. Now consider the equation $H_0 G_n = U_n - G_0 H_n$. We have that $\deg(H_0 G_n) < m$ (by definition of U_n, G_0 and H_n). But $\deg(H_0) = s$ and $r + s = m$ so $\deg(G_n) < r$ as desired. By induction we can conclude that such a G and H indeed exist. □

Applying this lemma to a pair of polynomials is sometimes referred to as the "lifting" of the factorisation. Note that this result holds only for $\mathbb{C}((t))$, the field of formal Laurent series. The lemma can however also be used on Puiseux series after some modifications. Having proved this lemma, we can now proceed with the proof that $\mathcal{P}$ is algebraically closed.

Theorem 2.6. *The field of complex Puiseux Series, $\mathcal{P}$, is algebraically closed*

Proof. Let $F(Y) = Y^n + \sum_{i=0}^{n-1} A_i Y^i \in \mathcal{P}[Y]$ be irreducible. Suppose that $n \geq 2$. A contradiction will prove the theorem. At the start we will assume that the variable used for the Puiseux series is u. Halfway the proof we will switch back to the original variable t.
By applying the Tschirnhaus transformation $X' = (X - A_{n-1}/n)$ we can make the $n-1$ term zero. So suppose that $A_{n-1} = 0$. Let $a_i u^{r_i}$ be the initial term of every $A_i \neq 0$ and let $r = \min_i\{\frac{r_i}{i}\}$. We then of course have that

$$r_i - ir \geq 0 \tag{15}$$

with equality for at least one of the i. Now perform the following coordinate change:

$$u^r Z = Y$$

We then obtain the following equation:

$$F(Z) = u^{nr}(Z^n + u^{-2r}A_2 Z^{n-2} + ... + u^{-nr}A_n)$$

Thus we have split $F(Z)$ in two parts. If we can find a nontrivial factorisation for $(Z^n + u^{-2r}A_2 Z^{n-2} + ... + u^{-nr}A_n)$ then we're done. Note that every term has positive valuation. To see this, consider the initial term in front of every Z^{n-i}:

$$u^{-ir}u^{r_i} = u^{r_i - ir}$$

But from the definition of r we have that $r_i \geq ir$ (see equation (15)) so all terms will have positive valuation.
We now wish to remove the denominators in every term of every Puiseux series A_i. This can be accomplished by changing coordinates: $u = t^m$ where m is set as follows:

$$m = \text{lcm}\{q_i \in \mathbb{Z} : r_i = \frac{p_i}{q_i}\}$$

The new form $F(Z)$ takes after this transformation is:

$$F(Z,t) = t^{mnr}(Z^n + B_2(t)Z^{n-2} + B_3(t)Z^{n-3} + ... + B_n(t))$$

where all the B_i are polynomials in t. We furthermore have that at least one of the B_i must have valuation 0 by definition of r. That is, one of the B_i must start with a nonzero constant term. Now define

$$D(Z,t) = Z^n + B_2(t)Z^{n-2} + B_3(t)Z^{n-3} + ... + B_n(t)$$

This is a monic polynomial in $\mathbb{C}((t))[Z]$. We can reduce this polynomial to obtain a polynomial in $\mathbb{C}[Z]$:

$$D(Z,0) = Z^n + B_2(0)Z^{n-2} + B_3(0)Z^{n-3} + ... + B_n(0)$$

One of the main properties of $\mathbb{C}$ is its algebraic closedness. That is, every polynomial splits in linear factors. In this case $D(Z,0)$ would split in n factors. These linear factors cannot all be the same. This is because the $n-1$th term is zero and at least one of the B_i is nonzero (because terms with valuation zero reduce to proper complex numbers).
Now take all the linear factors corresponding to one zero as g and the rest as h. This makes g and h coprime (they do not share any linear factors). We therefore have a coprime factorisation over $\mathbb{C}[Z]$ which can be lifted to a factorisation of $F(Z,t)$ using Hensel's Lemma. But this also means that $F(Y)$ is factorised, a contradiction to the irreducibility of $F(Y)$. This completes the proof.

□

3. Valuations

In this section we first give an approach to valuations that is slightly more abstract, yet also more insightful. This approach does not use a mapping, but a ring. Such a ring contains all the information needed for a valuation on general fields. Also, we have that the definitions and notation used in these valuation rings are used later on in this thesis. Afterwards we will relate these valuation rings to the valuations and vice versa.

3.1. **Valuation Rings.** Suppose we have a base field K. We wish to put a measure or valuation on a larger field: L. Every element x of L has an inverse in L. Therefore every element of L divides every other element of L. This does not give any intuition about whatever underlying structure L might have. We shall therefore try to find a subring of L that exposes how the constituents of L fit together. These notions can be made precise as follows:

Definition 3.1. A *valuation ring* is a subring $\mathcal{O}$ of a field L such that

(1) $K \subsetneq \mathcal{O} \subsetneq L$ ($\mathcal{O}$ should not be trivial)
(2) For every $x \in L$, $(x \neq 0)$ we have that either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ (both is also allowed)

Condition (2) ensures that the quotient field of this valuation ring is again the entire field. Creating $\mathcal{O}$ is like having a rule on L: for every element x of L we take either x or the inverse x^{-1}. We cannot however just randomly choose one or the other: we need our choices to be careful enough to allow a ring structure. But in the end, we can be sure that every element of L has left at least a mark on $\mathcal{O}$.

All the properties necessary for this set to be a ring are inherited from the field structure. The only thing missing of course is the presence of an inverse for *every* element of the set. Having found a subring of the field L, we can look for maximal ideals in our subring. The answer turns out to be quite short: there is only one maximal ideal in $\mathcal{O}$.

Proposition 3.2. *For every valuation ring, the set* $\mathcal{M} = \{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$ *has the following properties:*

(1) $\mathcal{M}$ *is an ideal in* $\mathcal{O}$
(2) $\mathcal{M}$ *is a maximal ideal*
(3) $\mathcal{M}$ *is the unique maximal ideal of* $\mathcal{O}$

Proof. 1) First we show that $\mathcal{M}$ is closed under multiplication. Take $m_1 \in \mathcal{M}$ and $x \in \mathcal{O}$. We wish to show that $m_1 x$ is not invertible. Suppose that it is invertible. Then we would have $m_1 xz = zm_1 x = 1$ for some $z \in \mathcal{O}$. Call $zx := y$. Then y is an inverse of m_1 (we use commutativity here), a contradiction.

We now show that $\mathcal{M}$ is closed under addition. Take $x, y \in \mathcal{M}$. We wish to show that $x + y$ is not invertible in $\mathcal{O}$. We know that both x and y are invertible in L, so whenever we use the inverse notation for x and y we mean their inverses in L. Write $x + y = x(1 + x^{-1}y) = y(1 + y^{-1}x)$. We know that for $x^{-1}y$ and $y^{-1}x$ at least one of these must be an element of $\mathcal{O}$. Without loss of generality, suppose that this is $x^{-1}y$. Then we also have $1 + x^{-1}y \in \mathcal{O}$. But $\mathcal{M}$ is closed under multiplication, so $x + y = x(1 + x^{-1}y) \in \mathcal{M}$.
2) Suppose there is an N such that $\mathcal{M} \subset N \subset \mathcal{O}$. Then for every $x \in N - \mathcal{M}$ we have that $x^{-1} \in \mathcal{O}$, because otherwise we would have that $M = N$. Since N is an ideal, we have that $x \cdot x^{-1} \in N$. But this means that $N = \mathcal{O}$. So $\mathcal{M}$ is a maximal ideal of $\mathcal{O}$.
3) Suppose there is another maximal ideal of $\mathcal{O}$, call it N again. Then N must contain an element that $\mathcal{M}$ does not contain (because otherwise N would not be maximal). Suppose $x \in N$ is such an element. By the definition of $\mathcal{M}$, x must have an inverse in $\mathcal{O}$. Because N is an ideal, we have that $x \cdot x^{-1} \in N$ and therefore $N = \mathcal{O}$, contradicting maximality. □

Thus, for every valuation ring we have a unique maximal ideal. An important property of maximal ideals is that their quotient ring is a field (this condition is actually an if and only if). Now quotient out $\mathcal{M}$ as follows: $\mathcal{O}/\mathcal{M} := k$. This k is called the *residue field* of the valuation ring. The field k is sometimes also called the *unit group* of the ring $\mathcal{O}$ (since we deleted all the elements without any inverses in $\mathcal{O}$). Note also that for every valuation ring, we obtain exactly one reduction mapping.

3.2. **Valuations.** As said before, it is possible to give a definition of valuations using these valuation rings. One could also start by defining valuations (as maps) first and afterwards defining the corresponding valuation rings. We shall see how these two definitions are connected shortly.

For any valuation ring, one can show (see [Bo81] for this) that there exists a surjective group homomorphism $v : L^* \longrightarrow G$ (which is called the *valuation*), where G is a totally ordered abelian group G. By totally ordered, we mean that we can order the elements of our group similar to how we order points on a line. For instance $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are totally ordered. The group operation in the valuation ring is multiplication, so we have the identity: $v(xy) = v(x) + v(y)$. If you add the identity $v(0) = \infty$ with $\infty + x = \infty$ for every $x \in G$, then you obtain another definition of valuation:

Definition 3.3 (Valuation)**.** A map $v : L \to G \cup \{\infty\}$ is called a valuation if

- $v(a) = \infty$ if and only if $a = 0$
- $v(ab) = v(a) + v(b)$
- $v(a + b) \geq \min\{v(a), v(b)\}$

Let us prove a couple of very simple properties to get used to these new definitions:

Proposition 3.4. *Let $v : L \longrightarrow G \cup \{\infty\}$ be a valuation. Then we must have:*

- $v(1) = 0$
- $v(a) = v(-a)$
- *if $v(a) < v(b)$, then $v(a + b) = v(a)$*

Proof. 1) For every element x, we know that $v(x) = v(x \cdot 1) = v(x) + v(1)$ which yields $v(1) = 0$.
2) The result will follow from $v(-a) = v(a) + v(-1)$ once we know that $v(-1) = 0$. Consider $0 = v(1) = v(-1) + v(-1) = 2v(-1)$. Now G is a totally ordered group, so it has no points of finite order. To see this for $m = 2$ (which can be extended with induction), note that if $0 < 2a < a$ then $-a < a < 0$, a contradiction. Also if $a < 2a < 0$ then $0 < a < -a$, another contradiction. Therefore $a = 0$. And consequently $v(-1) = 0$.
3) From 2) we know that $v(a) = v((a + b) - b) \geq \min\{v(a + b), -v(b)\} = \min\{v(a + b), v(b)\}$. But $v(a) < v(b)$ so $v(a) \geq v(a + b)$. We also know that $v(a + b) \geq \min\{v(a), v(b)\} = v(a)$. Therefore $v(a + b) = v(a)$. □

Now that we know a little bit about valuations, we can start by finding the connection back to valuation rings. This can be done by defining:

$$\mathcal{O} = \{x \in K : v(x) \geq 0\} \tag{16}$$

You can show that this is a valuation ring by using the following identity: $v(x \cdot x^{-1}) = v(x) + v(x^{-1}) = v(1) = 0$. If x is such that $v(x) < 0$ then $v(x^{-1}) > 0$ so $x^{-1} \in \mathcal{O}$.

3.3. **Examples.** We now give a couple of examples of valuations (which also give the corresponding valuation rings).

Example 3.5. (Trivial Valuation)
For every element $x \in k^*$: define $v(x) = 0$ and for $x = 0$ define $v(x) = \infty$.

Example 3.6. Consider $K = \mathbb{C}((t))$, the field of formal Laurent series over $\mathbb{C}$. Then we can define a valuation as in section 2.3. The corresponding valuation ring $\mathcal{O}$ contains all power series with positive valuation and the maximal ideal contains all power series with zeros at $t = 0$. The residue field $k = \mathcal{O}/\mathcal{M}$ contains all constant functions at $t = 0$.

Example 3.7. The field of Puiseux Series over $\mathbb{C}$ has the natural valuation introduced in section 2.3. For every polynomial $f \in P$, it is defined as the minimum of all the powers in f. So if

$$f = \sum_{k=k_0}^{\infty} c_k t^{\alpha_k} \tag{17}$$

then

$$v(f) := \min_k \{\alpha_k\} \tag{18}$$

We furthermore define $v(0) = \infty$. To see that the first property makes sense here, suppose that $v(f) = k$ for k large. This means that there are no powers of t lower than k. So if we make k higher and higher, we obtain less powers of t. Therefore we have that $v(f) = \infty$ implies $f = 0$ and vice versa. The second and third property follow from the definitions of multiplication and addition on the field of Puiseux series.

4. Affine and Projective Algebraic Varieties

In this section we'll give the definitions and the notation we will use for (normal) affine and projective algebraic varieties. As mentioned before, these affine varieties are basically just the zero set of a collection of polynomials. To study the geometry of a variety, one studies the zero set in an algebraically closed field, like $\mathbb{C}$. For example, taking a polynomial in one variable of degree d, we know that it must have d solutions over $\mathbb{C}$ (with multiplicities of course). We don't always know an explicit expression for these solutions (by Galois theory), but we know they must exist. These types of results are exactly what one aspires to achieve using algebraic geometry. In this section, we shall mainly study zero sets of polynomials in two variables, but everything can be adopted to a more general setting. In section (7), a similar notion will be developed for the *tropical world*. Many of the techniques and ideas from algebraic geometry will have an equivalent form in tropical algebraic geometry.

4.1. **Affine and Projective space.** Suppose we have a fixed algebraically closed field k, like for instance $\mathbf{C}$ or $\mathcal{P}$. We can define *affine n-space* over k as the set of all n-tuples $(a_1, ..., a_n)$ of elements of k. This space is denoted as $\mathbf{A}^n(k)$. The base field k shall occasionally be omitted unless it is deemed necessary.
Similarly we can define *projective n-space* over k: $\mathbf{P}^n(k)$. This time we take the set of equivalence classes of (n+1)-tuples $[a_0, ..., a_n] \in k^{n+1} - \{\bar{0}\}$ where $\bar{0}$ is the zero vector. The equivalence relation is defined as follows: Suppose $x, y \in \mathbf{P}^n(k)$. Then $x \equiv y$ if and only if $x = \lambda y$ for some $\lambda \in k - \{0\}$. Here scalar multiplication is as usual. Note that we use the round bracket notation for affine coordinates and the square brackets for projective coordinates.

Remark 4.1. The beauty of working with equivalence classes is that we have more freedom to look for particular solutions of problems. Suppose that we work over the field $\mathbb{Q}$ (which is not algebraically closed but the same ideas are applicable). Suppose that we want to find a solution of a particular problem in the projective n-space over $\mathbb{Q}$: $\mathbf{P}^n(\mathbb{Q})$. Since we are working in projective space, we can actually clear all the terms in the denominators by choosing the right λ (take λ as the maximum of all the terms in the denominators). This gives us a solution of the same problem (we assume here that our problem is well defined in projective space, see projective varieties) but with coordinates in $\mathbb{Z}$! In fact, the method above leads to a solution $[x_0, ..., x_n]$ with $x_i \in \mathbb{Z}$ and $\gcd(x_i) = 1$. So we see that in solving problems in projective space, one can immediately assume that the solutions are in $\mathbb{Z}$ and have no common terms. In fact, this technique is tacitly already used in most proofs that $\sqrt{2}$ is irrational.

. Having strayed a bit from our original path, we now return to projective space. We give some intuition as to what projective space looks like for the field $\mathbb{R}$. Suppose

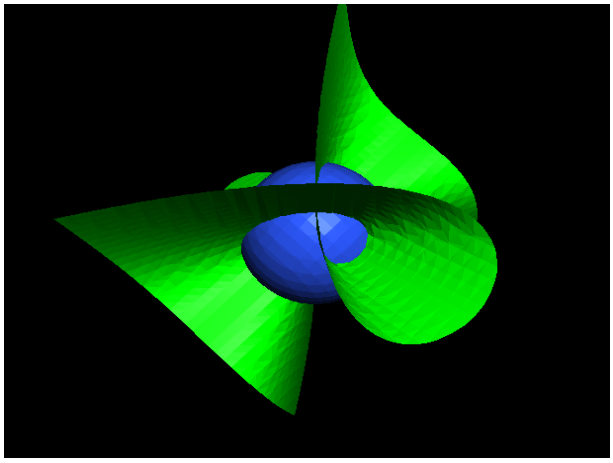


FIGURE 1. The points of a projective singular curve projected on the sphere

we have a set of points in $\mathbf{R}^3$. These can be seen as points in $\mathbf{P}^2_{\mathbf{R}}$ but we have to take into account that certain points might be equivalent. Either way we can now *project* every point (or: equivalence class) to the 1-sphere. This projection can be seen as the act of finding a representative for every point such that this representative has norm 1. Thus we see that points in $\mathbf{P}^2_{\mathbf{R}}$ can be described visually as points on the 1-sphere (this serves merely as a visual example, as this particular equivalence class is completely arbitrary). In fact, we have a bent version of $\mathbf{R}^2$ projected onto the 1-sphere with one additional point: the *point at infinity*. We shall see this point again when we consider elliptic curves.

The method above is a way to switch from projective space to affine space. There is actually a more general way of switching between affine and projective spaces.

Suppose that we start with points in affine space: $\mathbf{A}^n$. We can naturally embed this space in projective space in the following way:

- $\phi_i : \mathbf{A}^n \longrightarrow \mathbf{P}^n$
- $(y_1, ..., y_n) \longmapsto [y_1, y_2, ..., y_{i-1}, 1, y_i, ..., y_n]$

This map is however *not* a bijection since the point $[y_1, ..., y_{i-1}, 0, y_i, ..., y_n]$ (for some $y_j \neq 0$) is not in the image of $\mathbf{A}^n$ under ϕ_i. The map is however bijective on its image, which can be described as follows. Take the hyperplane

$$H_i = \{P = [x_0, ..., x_n] \in \mathbf{P}^n : x_i = 0\} \tag{19}$$

and let U_i be the complement of H_i:

$$U_i = \mathbf{P}^n - H_i \tag{20}$$

.

We can now define the inverse of ϕ_i as follows:

- ${\phi_i}^{-1} : U_i \longrightarrow \mathbf{A}^n$
- $[x_0, ..., x_n] \longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right)$

So we can identify affine space $\mathbf{A}^n$ with U_i by using ϕ_i for some i.
To recapitulate, we have multiple copies of $\mathbf{A}^n$ in $\mathbf{P}^n$ by the embeddings given above.

That is, we can always represent parts of $\mathbf{P}^n$ by $\mathbf{A}^n$ but we need to "glue" these together to get the full picture.

4.2. **Varieties.** Having defined affine and projective space, we can now consider the notion of varieties in these spaces. These varieties will be entirely algebraic of nature, that is, they will be subsets defined as the zero set of one or more polynomial(s). The study of varieties, or *algebraic geometry* bears many resemblances to manifold theory. The latter theory however does not allow any singular points: all manifolds are smooth. In algebraic geometry we do allow singularities, which more or less means that we allow "intersections" to occur in varieties. This will be made precise later on. Throughout this section we will assume that the field k is algebraically closed.

4.3. **Affine Varieties.** As introduced in section (2), we can introduce polynomials in one variable for any commutative ring. Continuing this construction for the polynomial ring, we obtain the polynomial ring in n variables:

$$k[X] := k[X_1, ..., X_n] = k[X_1, ..., X_{n-1}][X_n]...$$

The elements of this ring will be interpreted as functions on the affine n-space by defining $f(P) = f(a_1, ..., a_n) \in \mathbf{A}$ where $P = (a_1, ..., a_n) \in \mathbf{A}^n$.

Since k has a zero element, we can now talk about the set of zeros of a function f: $Z(f) = \{P \in \mathbf{A}^n | f(P) = 0\}$. If we have a set $T \subset k[X]$ of polynomials, then we can also consider the **zero set** of all the polynomials in T:

$$Z(T) = \{P \in \mathbf{A}^n \mid f(P) = 0 \text{ for all } f \in T\}$$

Remark 4.2. If we let τ be the smallest ideal containing T (in other words: the ideal generated by T) then we have that $Z(T) = Z(\tau)$. For "$\supseteq$", suppose that $x \in Z(\tau)$ and $x \notin Z(T)$. Then there exists an $f \in T$ such that $f(x) \neq 0$. But $f \in \tau$ so $x \notin Z(\tau)$, a contradiction.
For the reverse inclusion, we note that the ideal is finitely generated by the Hilbert

basis theorem (see [Gat03] or [Har77] for this theorem) , which tells us that any element $g \in \tau$ can be written as

$$g = h_1 a_1 + ... + h_r a_r$$

where a_i can be chosen to be the elements of T (since τ is the smallest ideal). If $g(x) \neq 0$ then we obtain a contradiction, since $a_i(x) = 0$ from $x \in Z(T)$.

Since ideals play such an important role in algebraic geometry, we want to associate an ideal to an arbitrary subset of $\mathbf{A}^n$. We therefore define the following, known as the **ideal of Y**:

$$I(Y) = \{f \in k[X] \,|\, f(y) = 0 \text{ for every } y \in Y\}$$

One can easily verify that this is indeed an ideal in $k[X]$. We can now start working towards our definition of algebraic variety. We first give a preliminary definition, which consequently has a different name.

Definition 4.3. If there exists a set T (or equivalently an ideal τ) such that $X = Z(T)$, then we call X an **algebraic set**.

Example 4.4. Take $f = y^2 - x^3 - Ax - B$ with $A, B \in \mathcal{P}$. Then the zero set $Z(f)$ is called the affine form of an elliptic curve. We shall return to these particular algebraic sets in section (5).

Example 4.5. Take $f = yx$. Then for $k = \mathbb{C}$ we obtain the following zero set:

$$Z(f) = \{(x, y) \in \mathbb{C}^2 | \, x = 0 \text{ or } y = 0\} \tag{21}$$

This algebraic set can be written as a union of two algebraic subsets. We call an algebraic set that can be written as the union of two interior sets **reducible**. If this is not possible, then we call an algebraic set **irreducible**.

By definition, every algebraic set can be written as a union of these irreducible algebraic sets. Hence these irreducibles can be seen as the building blocks of algebraic sets. The following result should not come as a surprise:

Theorem 4.6. *Suppose X is an algebraic set. Then X is irreducible if and only if $I(X)$ is a prime ideal.*

Proof. The proof isn't lengthy, but we do not include it here. It can be found in [Gat06],[Har77] for instance. □

With this theorem in mind, we define affine varieties:

Definition 4.7. An affine **variety** is an irreducible algebraic set.

Example 4.8. We see that the algebraic set corresponding to $f = yx$ is not an algebraic variety, since it can be written as the union of two algebraic sets.

Example 4.9. For $f(x, y) = y^2 - x^3 - Ax - B$ we note that if we can prove that the f is irreducible, then we automatically have that the set is a variety. This is because $k[X]$ is a unique factorisation domain, which tells us that the notions of prime ideal and irreducibility coincide. We can write the polynomial $x^3 + Ax + B$ in terms of its zeros. For a smooth elliptic curve there are three distinguished zeros. We then apply the Eisenstein criterion with $p = x - \alpha$ where α is one of the roots. Thus f is irreducible and thus (f) is a prime ideal, which makes the variety irreducible.

4.4. **Projective Varieties.** Let us try to do the same with projective varieties. We start with projective n-space and the ring $k[X]$. If we now take the zero set of a polynomial, we are in trouble. Take for instance the polynomial:

$$f = Y^2 - X \tag{22}$$

We have that $[1, 1] \in Z(f)$, yet $[-1, -1] \notin Z(f)$ even though these two points belong to the same equivalence class! The solution to this problem lies in restricting the allowed polynomials. The ones we are looking for are the **homogeneous polynomials**:

Definition 4.10. A polynomial $f \in k[X]$ is **homogeneous** if $f(\lambda X) = \lambda^d f(X)$ for all $\lambda \neq 0$ and some d. The d will be called the degree. Likewise an ideal is called homogeneous if it is generated by homogeneous polynomials.

It is easy to see that the zero set of a homogeneous polynomial is well defined in projective space. If we have $X = \lambda Y$ for some λ then $f(X) = 0 = f(\lambda Y) = \lambda^d f(Y)$ if and only if $f(Y) = 0$ (since $\lambda \neq 0$).

We can now copy the definitions of algebraic sets and varieties:

Definition 4.11. Suppose that I is a homogeneous ideal in $k[X]$. A **projective algebraic set** is then defined as:

$$V_I = \{P \in \mathbf{P}^n \,:\, f(P) = 0 \text{ for all homogeneous } f \in I\}$$

Definition 4.12. A projective algebraic set is a **projective variety** if its homogeneous ideal is a prime ideal.

Example 4.13. Let V be the projective algebraic set in $\mathbf{P}^2$ defined by:

$$X^2 + Y^2 = Z^2$$

This is the equation for Pythagorean triples. Its defining polynomial, $f = X^2 + Y^2 - Z^2$ is homogeneous, since $f(\lambda X, \lambda Y, \lambda Z) = \lambda^2 f(X, Y, Z)$.

Example 4.14. The polynomial $f = Y^2 - X$ is not homogeneous since $f(\lambda X, \lambda Y) = \lambda^2 Y^2 - \lambda X$. We shall shortly see how to make this equation homogeneous though.

We now give a method of switching between affine varieties and projective varieties. The difference between these two is that the first one use general polynomials, whereas the second one uses homogeneous polynomials. Suppose first that we have a projective variety V with homogeneous ideal $I(V)$. We now define the **dehomogenisation** of a polynomial in $k[X]$ with respect to some X_i. We perform a coordinate change as follows:

$$[X_0, ..., X_i, ..., X_n] \longmapsto \left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_i}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right)$$

Instead of $f[X_0, ..., X_i, ...X_n]$ we then have $f(Y_1, ..., Y_{i-1}, 1, Y_{i+1}, ...Y_n)$ where the Y_i are as in the transformation above.

Example 4.15. Let V be the projective variety in $\mathbf{P}^2$ defined by:

$$X^2 + Y^2 = Z^2$$

Then dehomogenising with respect to Z yields:

$$(X')^2 + (Y')^2 = 1$$

Where $X' = X/Z$ and $Y' = Y/Z$. This is the equation of a circle with radius 1. Notice that we have lost the point $Z = 0$ in the process of dehomogenising. If we were working over the field of complex numbers, then $[X : Y : Z] = [1, i, 0]$ would be a point on the variety which would be lost in the process of dehomogenising. We can however recover this point by dehomogenising with respect to another variable, say X. We then obtain:

$$1 + (Y')^2 = (Z')^2$$

where $Y' = Y/X$ and $Z' = Z/X$. Notice that the point $[1, i, 0]$ is sent to $(i, 0)$ by the mapping. This is indeed a point on the affine variety. By choosing the right coordinate one can always recover all the points on the projective variety by glueing all the affine bits together.

We have found a way of getting an affine variety (or in fact multiple, one for every coordinate) from a projective variety. We now construct a projective variety for every affine variety. This is done by changing the defining polynomials of the variety. This change is called the **homogenisation** of f with respect to Y_i. Suppose we have an affine variety V with ideal $I(V)$. For any f, we define a new f' which is homogeneous:

$$f'(Y_0, ..., Y_n) = {Y_i}^d f(\left(\frac{Y_0}{Y_i}, \frac{Y_1}{X_i}, ..., \frac{Y_{i-1}}{Y_i}, \frac{Y_i}{Y_i}, \frac{Y_{i+1}}{Y_i}, ..., \frac{Y_n}{Y_i}\right))$$

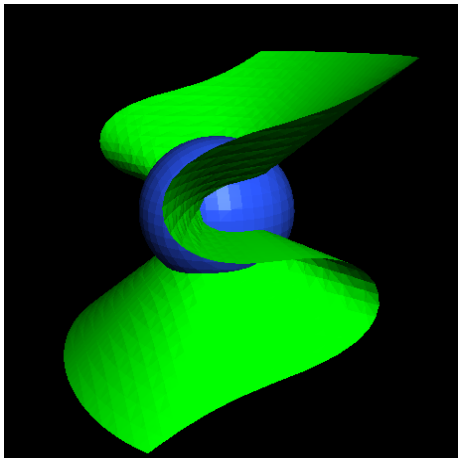


FIGURE 2. A projective version of a nonsingular elliptic curve

where d is the lowest integer such that f' is again a polynomial.

Example 4.16. Earlier on we consider the non-homogeneous variety defined by:

$$Y^2 - X = 0$$

Homogenising yields:

$$Y^2 - XZ = 0$$

Example 4.17. An elliptic curve in (reduced) Weierstrass form is given in affine form as:

$$Y^2 = X^3 + AX + B$$

for some A and B (which satisfy some relation so that we do not obtain a singular curve). This equation is not homogeneous, but we can homogenize it, which yields:

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

We shall see more of these curves in section (5).

4.5. **Nonsingularity.** In this section we quickly define what it means for a point on a (projective) plane curve to be (non)singular. In manifold theory smoothness is characterised by means of the Jacobian matrix. We can do the same for varieties, although we have to be careful with the definition of "dimension", which we will take for granted for now. The field k is once again assumed to be algebraically closed.

Smoothness of an object is usually measured in terms of differentiability. Differentiation is however a notion taken from analysis. We can nonetheless define a derivative for polynomials algebraically: there is no need for a metric. This derivative has exactly the same form as the usual derivative and behaves in the same way as the normal derivative. Hence we can write and manipulate partial derivatives etc. just as we normally would. The following definition mimics that of manifold theory in the sense that we define a point on a curve to be nonsingular if there exists a unique tangent line at that point:

Definition 4.18. Let C be a plane curve, $P \in C$, and $f \in k[X]$ a generator for $I(V)$ (the ideal of the curve C). Then C is **nonsingular** (or smooth) at P if the vector

$$\left(\frac{\partial f}{\partial X_j}(P)\right)$$

has rank 1. If C is nonsingular at every point, we say that C is nonsingular (or smooth).

Remark 4.19. A Jacobian having rank 1 means that for at least one coordinate we have:

$$\frac{\partial f}{\partial X_i}(P) \neq 0$$

Remark 4.20. For projective varieties we adopt the following definition: a point P on a projective variety V is said to be nonsingular if all partial derivatives are nonzero at that point P.

Example 4.21. Let V be the projective variety defined by:

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

As mentioned before, this is an elliptic curve in reduced Weierstrass form. We shall check that the point at infinity, $P = [0, 1, 0]$, is nonsingular for every elliptic curve. To that end, we compute:

$$\frac{\partial f}{\partial Z} = Y^2 - 2AXZ + 3BZ^2$$

which gives us $\dfrac{\partial f}{\partial Z}(P) = 1 \neq 0$ for every elliptic curve. Thus the point at infinity is nonsingular for every elliptic curve.

4.6. **Maps between Varieties.** Having defined what affine and projective varieties are, we should now say what maps we allow between two varieties. In fact, our goal will be to define what an **isomorphism** should be. To that end we first define the coordinate ring and function field of a variety. After that we can say what a regular function is, which will lead to the notion of morphisms and isomorphisms.

Suppose we have an affine variety V. As we saw earlier, we can find an ideal of functions that vanish on V: $I(V)$. Because we defined varieties to be irreducible, we know that the corresponding ideal must be a prime ideal. This also means that the quotient ring $k[X]/(I(V))$ is a domain. This quotient ring is called the **coordinate ring** of the variety V.

Definition 4.22. Let V be an affine variety. We then define the coordinate ring of V to be $K[V] := k[X]/(I(V))$.

Thus we see that two polynomials give rise to the same function on V iff they belong to the same equivalence class of $K[V]$. This also means that for every $f \in K[V]$ we have a well defined function:

$$f : V \longrightarrow k$$

which is defined as evaluating f at the points on V. As mentioned before, this coordinate ring is in fact a domain. This means that we can form its quotient field. This field is known as the **function field** of the variety V:

Definition 4.23. Let V be an affine variety with coordinate ring $K[V]$ Then we define the function field of V to be $K(V)$ (its quotient field).

By definition of quotient field, we can write any element of $K(V)$ as $\frac{f}{g}$ with $f, g \in K[V]$. Thus we see that the function field contains all rational functions on the variety V. If we have two varieties $V_1 \in k^{n_1}$ and $V_2 \in k^{n_2}$, then we can define a **rational map** by taking n_2 of these rational functions. That is, ϕ is **rational** if it can be written as:

$$\phi = [f_1, ..., f_{n_2}]$$

where $f_i \in K(V_1)$. These rational functions may however be ill-defined at some points of V. For every point P on V we can find a ring with functions that are well defined at P, **the local ring at P**:

Definition 4.24. Let V be an affine variety with $P \in V$. We define the local ring of V at P to be:

$$\mathcal{O}_P := \left\{ \frac{f}{g}; f, g \in K[X] \text{ and } g(P) \neq 0 \right\} \subset K(X)$$

This should be thought of as all rational functions that are regular at P. As one can check, this is a valuation ring in $K(X)$. It has a maximal ideal, which is given by:

$$\mathcal{M}_P := \left\{ \frac{f}{g} \in \mathcal{O}_p \, : \, f(P) = 0 \right\}$$

We can also obtain the **ring of regular functions** on V as follows:

$$\mathcal{O}_V := \bigcap_{P \in V} \mathcal{O}_P$$

Every element of this ring defines a proper function $f : \mathcal{O}_V \longrightarrow k$.
Having seen what constitutes a regular function, we can now define what a **morphism** is.

Definition 4.25. Let $V_1 \subset k^{n_1}$ and $V_2 \subset k^{n_2}$ be affine varieties. Let $\phi : V_1 \longrightarrow V_2$ be a rational map. ϕ will be called a **morphism** if for every regular function $f \in K(V_2)$ we have that the map $f \circ \phi$ is regular.

Remark 4.26. Note that if the rational map ϕ is regular everywhere on V_1 then it is automatically a morphism.

For projective varieties we give the following definition.

Definition 4.27. Let V_1 and $V_2 \subset \mathbf{P}^n$ be projective varieties. A rational map

$$\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$$

is regular at P if there is a function $g \in k(V_1)$ such that

- (i) gf_i is regular at P for every i,
- (ii) there is some i for which $(gf_i)(P) \neq 0$.

If ϕ is regular at every point $P \in V_1$ then we call it a **morphism**.

This g allows us to clear the denominators of a map locally. In fact, we have that this projective morphism is a set of affine morphisms glued together. An example of this will be given in the proof of the main theorem. Not surprisingly the definition of a morphism leads to the definition of an **isomorphism**.

Definition 4.28. Suppose that ϕ is a morphism of two varieties V_1 and V_2. Then it is an **isomorphism** if there exists a morphism ξ such that $\phi \circ \xi = \xi \circ \phi = id$.

5. Elliptic Curves

In this section we define what an elliptic curve is. We define it as a smooth curve having certain properties. We can associate an equation to this curve. This equation is known as a Weierstrass equation. A curve with such an equation can have singularities however. We introduce the **discriminant** as a quantity to check whether a Weierstrass equation has a singularity. After this we will consider isomorphisms between two elliptic curves. This will lead to the definition of the **j-invariant**: a single quantity which all isomorphic elliptic curves have in common. The isomorphism also preserves a group operation on it in the usual sense. This group operation takes two points on the elliptic curve and maps these to another point on the elliptic curve. It allows us to talk about concepts like subgroups of the elliptic curve and points of finite order (*torsion points*).

5.1. **Elliptic Curves.** We define an elliptic curve to be a smooth curve of **genus** 1 with a specified basepoint denoted by $\mathcal{O}$. The (geometric) genus is an invariant that is preserved by birational maps. We won't give the exact definition of genus here, but it can be shown using the Riemann-Roch theorem that every such elliptic curve can be written as the zero locus in $\mathbf{P}^2$ of a cubic equation (and one additional condition, see (5.1)).

This equation in $\mathbf{P}^2$ takes the following form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{23}$$

with $\mathcal{O} = [0, 1, 0]$ and $a_1, ..., a_6 \in k$. This equation is usually called the (projective) *Weierstrass equation* of an elliptic curve. We shall however be mainly concerned with elliptic curves given in affine Weierstrass form. The affine form of the equation is obtained by setting $x = X/Z$ and $y = Y/Z$, which yields:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{24}$$

Remark 5.1. Our definition of an elliptic curve assumes it is smooth. In fact, whenever we say "elliptic curve" we shall assume that it is smooth. The corresponding Weierstrass equation however can have singularities. There is a condition on this Weierstrass equation which ensures that it is smooth (and thus an elliptic curve). This condition is given by the **discriminant**. Note the subtle difference between "elliptic curve" and "Weierstrass equation", the first always being smooth, whereas the second can have singularities.

When working over a field of characteristic $\neq 2, 3$, we can greatly simplify this form by applying two isomorphisms. The first one is more commonly known as "completing the square", where we send:

$$y \longmapsto (y + a_1x + a_3)/2$$

Remark 5.2. Note that this is a regular map (since it's a polynomial) on all of E. In fact, it is an invertible affine linear transformation. This also makes the map (and its inverse) regular and therefore it is also an isomorphism. Also note that this transformation would not make any sense in a field of characteristic 2, since we have that $2 = 1 + 1 = 0$ in any such field. Since we will only consider curves of characteristic 0, this will not pose any difficulties.

The new form of the elliptic curve obtained by the isomorphism is:

$$y^2 = x^3 + \frac{b_2}{2}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

where the b_i are as defined in table (1). The c_i's and the other quantities will be explained shortly.

TABLE 1. Several coefficients and other quantities for an elliptic curve

$b_2 = {a_1}^2 + 4a_2$	$c_4 = {b_2}^2 - 24b_4$	$1728\Delta = {c_4}^3 - {c_6}^2$
$b_4 = 2a_4 + a_1a_3$	$c_6 = {b_2}^3 + 36b_2b_4 - 216b_6$	$j = {c_4}^3/\Delta$
$b_6 = {a_3}^2 + 4a_6$		

The last transformation we can apply is the *Tschirnhaus transformation* that we're already familiar with from the proof that $\mathcal{P}$ is algebraically closed. It removes the x^2 term as follows:

$$x \longmapsto (x - \frac{1}{6}b_2)$$

As before, this is also an isomorphism. The curve we obtain after this map is:

$$y^2 = x^3 + (\frac{1}{3}{b_2}^2 + \frac{1}{2}b_4)x + (-\frac{1}{216}{b_2}^3 + \frac{1}{72}{b_2}^2 - \frac{1}{2}b_4b_6 + \frac{1}{4}b_6) \tag{25}$$

which is already in the form $y^2 = x^3 + Ax + B$. One usually doesn't use this form, by convention it is usually given in the following **reduced Weierstrass form**:

$$y^2 = x^3 - 27c_4x - 54c_6$$

This form can be acquired by rescaling equation (25). The c_i's are as in table (1).

5.2. **Singularities and Isomorphisms.** Having seen what a smooth elliptic curve looks like, let us consider the case of a singular Weierstrass equation. There are two possibilities: the singularity can be a **node** or a **cusp**. If we write the Weierstrass equation as $y^2 = f(x)$ then these cases correspond respectively to f having a double zero or a triple zero. To see why this is the case we consider $g = y^2 - f(x)$. Then E

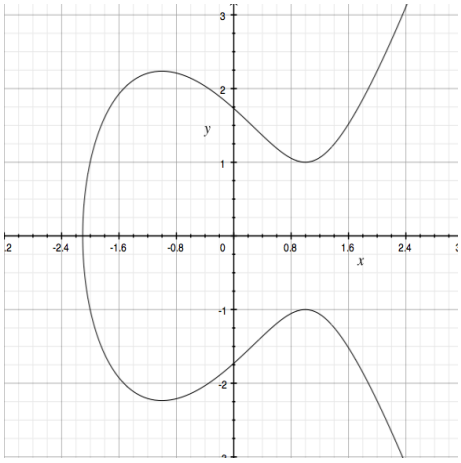


FIGURE 3. A smooth elliptic curve

has a singularity if and only if $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0$. This implies $2y = 0$ or $y = 0$. In other words, a singularity must occur exactly at a zero of f. But we also need $\frac{\partial f}{\partial x} = 0$. This only occurs if we have a repeated zero. Since f is cubic, we have two options: a double or a triple zero.

There are two quantities from table (1) we haven't discussed yet : the **discriminant** and the j**-invariant**. The discriminant Δ is used to determine whether a Weierstrass equation has singularities and the second is a common quantity of isomorphic elliptic curves. This is shown in the following theorem:

Theorem 5.3. *Let E be a curve given by a Weierstrass equation over an algebraically closed field k. Then we have that:*

- *(i) it is nonsingular if and only if $\Delta \neq 0$*
- *(ii) it has a node if and only if $\Delta = 0$ and $c_4 \neq 0$*
- *(iii) it has a cusp if and only if $\Delta = c_4 = 0$.*
- *(iv) two elliptic curves are isomorphic if and only if they have the same j-invariant*

Proof. The proof is in [Silv09] in chapter 3. □

From this theorem we see that the occurrence of singularities in Weierstrass equations is completely determined by the discriminant. The type of singularity is determine by c_4.

Transformation table for Weierstrass equations
$u^1 a_1{}' = a_1 + 2s$
$u^2 a_2{}' = a_2 - sa_1 + 3r - s^2$
$u^3 a_3{}' = a_3 + ra_1 + 2t$
$u^4 a_4{}' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6 a_6{}' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2 b_2{}' = b_2 + 12r$
$u^4 b_4{}' = b_4 + rb_2 + 6r^2$
$u^6 b_6{}' = b_6 + 2rb_4 + r^2 b_2 + 4r^3$
$u^8 b_8{}' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4$
$u^4 c_4{}' = c_4$
$u^6 c_6{}' = c_6$
$u^{12}\Delta' = \Delta$
$j' = j$

TABLE 2

We have yet to discuss isomorphisms. It can be shown that any isomorphism of an elliptic curve preserving the Weierstrass form must be of a special form. These isomorphisms are called **Weierstrass coordinate changes**.

Definition 5.4. A change of variables for an elliptic curve E is called a Weierstrass coordinate change if

- $x = u^2 x' + r$
- $y = u^3 y' + su^2 x' + t$

for some $u \in k^*$ and $r, s, t \in k$.

Note that these transformations are affine linear transformations with determinant $u^6 \neq 0$. Applying such a coordinate change (which preserves the Weierstrass form) induces a set of new coefficients $a_i{}', b_i{}'$ and $c_i{}'$. These are given by Table 2.

5.3. **Group Law.** Let E be an elliptic curve given by a Weierstrass equation. Every point $P = (x, y)$ on this curve in Weierstrass form has a corresponding point in $\mathbf{P}^2$: $[x, y, 1]$. There is one point missing of course, and that is the point at infinity: $[0, 1, 0]$.

If we now take any line L in $\mathbf{P}^2$ (where a line has an equation of the form $aX + bY + cZ = 0$) then we can intersect this line with the curve E. We now use the following theorem:

Theorem 5.5. *(Bézout's Theorem) Let Y, Z be distinct curves in $\mathbf{P}^2$, having degrees d, e. Let $Y \cap Z = \{P_1, ..., P_s\}$. Let $i(Y, Z; P_j)$ be the intersection multiplicity of Y and Z in P_j. Then:*

$$\sum i(Y, Z; P_j) = de$$

Proof. See [Har77] for the proof and for an explanation of the term "intersection multiplicity". We shall not define it rigorously. □

By Bézout's Theorem there are exactly 3 points of intersection (since the curve has degree 3 and the line degree 1, counting multiplicities). If we fix two points $P, Q \in E$ then we obtain another point $R \in E$. If $P = Q$ then L should be taken as the tangent line through P. Either way we obtain a point R. Let L' be the line through $\mathcal{O}$ and R. Then the third intersection point of this line L' with E will define the group operation $P \oplus Q$.
Let us summarise the group operation as follows:

- Take two points $P, Q \in E$
- Take the unique line through P and Q and intersect this line with E to obtain the point R. If $P = Q$ then take the tangent line.
- Take the line through $\mathcal{O}$ and R and intersect this line with E to obtain the point R'.
- Then $P \oplus Q = R'$ or $P \oplus Q \oplus R = \mathcal{O}$.

The fact that $\oplus$ defines a group is contained in the following theorem which we will not prove.

Theorem 5.6. *The operation " $\oplus$ " makes E into an abelian group with identity element $\mathcal{O}$.*

Proof. See [Silv09], [Kna92] or [Cas91]. □

Remark 5.7. From now on we will denote the operation simply by "+". Furthermore we define $[m]P = P + ... + P$ (m times) if $m > 0$ and $[m]P = -P - ... - P$ (m times) if $m < 0$ together with $[0]P = \mathcal{O}$.

We can now consider points of finite order. We call these points **m-torsion points.**

Definition 5.8. Suppose $P \in E$. Then P is an **m-torsion point** if $[m]P = \mathcal{O}$.

For every m we define a subgroup of points on an elliptic curve by only considering points of finite order.

Definition 5.9. Let E be an elliptic curve. The **m-torsion subgroup of** E, denoted by $E[m]$, is the set of points of E of order m,

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}$$

Every such $E[m]$ is isomorphic (as an abstract group) to a particularly easy, cyclic group:

Theorem 5.10. *Let E be an elliptic curve over a field k of char$(k) = 0$. Then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Proof. See [Silv09] chapter 3, paragraph 6. □

We now give explicit equations for the group operation. We only give the equations for adding the same point (also known as the duplication formula). We treat this special case because we want to show the existence of points of order 3.

Example 5.11. (**Group Law Algorithm**) Let E be given by:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

- (a) Let $P_1 = (x_1, y_1)$ with $y_1 \neq 0$. We want to calculate $[2]P_1 = P_2$ where $P_2 = (x_2, y_2)$
- (b) Let $\lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4}{2y_1}$ and $\nu = \dfrac{-{x_1}^3 + a_4x_1 + 2a_6}{2y_1}$
- (c) Then $x_2 = \lambda^2 - a_2 - 2x_1$
- (d) And $y_2 = -\lambda x_2 - \nu$.

  Now let $x_2 = x_1$ and $y_2 = y_1$. Then $y_1 = -\lambda x_1 - \nu$ and $3x_1 = \lambda^2 - a_2$ or $\lambda^2 = 3x_1 + a_2$. Using the equations for λ and ν we obtain a polynomial in x_1 which can always be solved over an algebraically closed field. This also gives the y_1. With a little more effort one can show that there are exactly 9 points of order 3.

As we saw during our discussion of the discriminant, a curve given by a Weierstrass equation can be singular. The good news is that we can still use the group law on these curves of genus 0. We just have to restrict ourselves to a subset of the points on E.

Definition 5.12. Let E be a (possibly singular) curve given by a Weierstrass equation. The **nonsingular part** of E, denoted by E_{ns}, is the set of nonsingular points of E.

This set is actually a group: it is closed under the composition law. This can be proved using Bézout's Theorem. The main argument in the proof is that singular points have multiplicity at least two. If the curve defined by a Weierstrass equation is singular, then we can give an isomorphism from the group E_{ns} to a much easier group. This is the content of the next proposition:

Proposition 5.13. *Let E be a curve given by a Weierstrass equation with $\Delta = 0$, so E has a singular point S. Then the composition law makes E_{ns} into an abelian group. Furthermore, we have that*

- *(a) Suppose that E has a node, so $c_4 \neq 0$. Then $E_{ns} \cong k^*$, the unit group of k*
- *(b) Suppose that E has a cusp, so $c_4 = 0$. Then $E_{ns} \cong k^+$, the additive group of k.*

Proof. For the full proof see [Silv09] chapter 7, paragraph 2. □

The last theorem from the field of elliptic curves we need is known as the "Nagell-Lutz" theorem. It says that if we have a point of finite order (where m is not a prime power) then it must have positive valuation.

Theorem 5.14. *(***Nagell-Lutz***) Let $\mathcal{P}$ be the field of complex Puiseux series and let $E/\mathcal{P}$ be an elliptic curve given by a Weierstrass equation with all coefficients having non-negative valuation. If $P = (x, y)$ is a point of order m where m is not a prime power*

Proof. This can be proven analogous to the argument presented in chapter 8, paragraph 7 of [Silv09] □

So if we take a point of say order 3, then its coordinates must have non-negative valuation.

6. Minimal Weierstrass Equations and Reduction

In this section we discuss the reduction of elliptic curves over $\mathcal{P}$ using valuation rings. We already saw how to reduce elements of $\mathcal{P}_{\geq 0}$ by simply sending an element $(x(t))$ to $(x(0))$. To define the reduction of elliptic curves over $\mathcal{P}$ we need a **minimal Weierstrass equation**. We show how to obtain these and we show how you can find out whether a given Weierstrass equation is minimal.

6.1. **Minimal Weierstrass Equations.** In this section we'll use the following affine form for an elliptic curve E/k:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{26}$$

The following notation shall be used as well:

- k, an algebraically closed field, in this case the field of Puiseux series.
- $\mathcal{R} = \{x \in k : v(x) \geq 0\}$, the ring of integers.
- $\mathcal{R}^* = \{x \in K : v(x) = 0\}$, the unit group of $\mathcal{R}$.
- $\mathcal{M} = \{x \in K : v(x) > 0\}$, the maximal ideal of $\mathcal{R}$.

This equation for an elliptic curve is unique in the sense that all elliptic curves isomorphic to the given elliptic curve are related by Weierstrass coordinate changes. We restate their definition here:

Definition 6.1. A change of variables is called a Weierstrass coordinate change if

- $x = u^2x' + r$
- $y = u^3y' + su^2x' + t$

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

The Weierstrass equation is thus unique up to isomorphisms of the form above. When changing coordinates, the coefficients change according to Table 2. Our goal is now to find a Weierstrass equation such that the valuation of all the coefficients is non-negative. That is, we want $a_i \in \mathcal{R}$. As we shall see, this can be done by chosing a high enough power of t for u. Since the discriminant is a polynomial in the coefficients, the discriminant must then have positive valuation as well. We want this new equation to be unique in some sense, so we demand an extra condition on the discriminant. This is summarized in the following definition:

Definition 6.2. A Weierstrass equation for an elliptic curve is called Weierstrass-minimal if:

- (1) $v(a_i) \geq 0$
- (2) $v(\Delta)$ is minimal under (1)

Let us prove a preliminary result concerning minimal equations first.

Lemma 6.3. *Let E be an elliptic curve given in standard Weierstrass form. Then we can bring this equation to the reduced Weierstrass form E'*

$$y^2 = x^3 - 27c_4x - 54c_6$$

by isomorphisms such that $v(\Delta) = v(\Delta')$.

Proof. The first isomorphism is given by:

- $x \longrightarrow x$
- $y \longrightarrow y + \frac{1}{2}(a_1x + a_3)$

Note that this particular isomorphism has $u = 1 \in \mathcal{R}^*$ so the valuation of the discriminant is unaffected.
The second isomorphism is given by

- $x \longrightarrow (x - 3b_2)/36$
- $y \longrightarrow (y/216)$

We have $v(u) = v(\frac{1}{6}) = 0$ which again leaves the valuation of the discriminant untouched. □

As mentioned before, one now might consider the following question: to what extent is this minimal equation unique? Suppose that we have a minimal equation for an elliptic curve. Isomorphic curves are obtained by considering the Weierstrass coordinate change. These are considered equivalent. However, not all equivalent elliptic curves are minimal with respect to the given valuation. A minimal equation of an elliptic curve is unique up to particular isomorphisms, as is shown in the next Lemma.

Lemma 6.4. *A given minimal Weierstrass equation is unique up to isomorphisms with $u \in \mathcal{R}^*$ and $r, s, t \in \mathcal{R}$*

Proof. We know that the Weierstrass equation is unique up to isomorphisms stemming from the Weierstrass coordinate change. So only the final claims have to be checked. The first one says that u has zero valuation. Now suppose that both the original equation and the new equation are minimal. Because of minimality we have that $v(\Delta) = v(\Delta')$. But the transformation formulas give

$$12v(u) + v(\Delta') = v(\Delta) \tag{27}$$

Combining the preceding two equations yields $v(u) = 0$ or in other words $u \in \mathcal{R}^*$, which proves the first part.
The second part follows analogously by considering Table 2. If a given minimal Weierstrass equation is related to another, then we can bring it to "b_i"-form (The second form in the proof of Lemma 6.3) without changing minimality. Applying a transformation with r would then result in the following change:

$$u^2 b_2{}' = b_2 + 12r$$

We know from the first part that $v(u) = 0$. If the new equation is to be minimal then $v(b_2{}') \geq 0$. This also implies that $r \in \mathcal{R}$ (because $v(b_2) \geq 0$).

The same argument can be used for the equation

$$u a_1{}' = a_1 + 2s$$

to conclude that $s \in \mathcal{R}$. For t we use the following equation:

$$u^3 a_3{}' = a_3 + r a_1 + 2t$$

If $v(t) < 0$ then $v(a_3{}') < 0$ which contradicts the minimality assumption.

□

Since $v(\Delta) \geq 0$, we know that the equation is minimal if the valuation of the discriminant is exactly zero. This corresponds to the presence of a constant, non-zero term in the discriminant. However, we can say more than that. A necessary and sufficient condition for minimality of an elliptic curve over the field of Puiseux series is given in the next theorem.

Theorem 6.5. *A Weierstrass equation is minimal over the field of Puiseux series if and only if* $\min\{v(a_i)\} = 0$

Proof. ($\Longrightarrow$) Suppose that a given equation is minimal. Under any coordinate change we have the following:

$$\Delta' = u^{-12}\Delta \tag{28}$$

Since the equation is assumed to be minimal, we must have that $v(\Delta') \geq v(\Delta)$ if $a_i' \in \mathcal{R}$. Now suppose for a contradiction that $\min\{v(a_i)\} := m > 0$. (Note that m smaller than zero would contradict minimality). If $m > 0$ then surely $m' = \min\{\frac{a_j}{j}\} > 0$. The definition of minimality allows us to use any u we want, as long as that $u \in K^*$. We take $u = t^{m'}$. Using this transformation (along with $r = s = t = 0$), the new coefficients will have $v(a_i{}') \geq 0$ again. To see this, note that from the transformation table we have that

$$u^i a_i{}' = a_i \tag{29}$$

This also means that $iv(u) + v(a_i{}') = v(a_i)$ or $v(a_i{}') = v(a_i) - iv(u)$. But $v(u) = m'$. We can therefore write

$$v(a_i{}') = i(\frac{v(a_i)}{i} - m') \tag{30}$$

But $m' \leq \frac{v(a_i)}{i}$ for every i. Therefore $(\frac{v(a_i)}{i} - m') \geq 0$ and consequently $v(a_i{}') \geq 0$. The new equation therefore satisfies the first condition of minimality. Now our earlier assumption was that $v(\Delta') \geq v(\Delta)$. Combined with a transformation rule, this gives:

$$v(\Delta') = -12v(u) + v(\Delta) \geq v(\Delta) \tag{31}$$

Or in other words: $12v(u) \leq 0$. This clearly contradicts our choice for u, completing the proof of "$\Longrightarrow$".

($\Longleftarrow$) Suppose now that $\min\{v(a_i)\} = 0$. Obviously (1) is satisfied. We once again proceed by assuming the opposite, namely that the Weierstrass equation is *not* minimal. This means that we can find u, r, s and t such that:

$$v(\Delta') < v(\Delta) \tag{32}$$

whenever $v(a_i') \geq 0$. Recall the standard Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{33}$$

We give a small lemma which will help us.

Lemma 6.6. *Let E be an elliptic curve in reduced Weierstrass form. Let E' be an isomorphic elliptic curve also in reduced Weierstrass form. Then the two equations are related by a Weierstrass coordinate change with $r = s = t = 0$.*

Proof. Two isomorphic elliptic curves in reduced Weierstrass form are always related by a Weierstrass coordinate change. If one of the r, s, t is not zero then we would get an equation which is not in reduced Weierstrass form. □

Using Lemma 6.3 we can reduce the standard Weierstrass equation to the reduced Weierstrass form E_{red} without changing the discriminant. We assumed that there is a Weierstrass coordinate change lowering the discriminant, call it ϕ_1. This coordinate change might use r, s, t factors. We can however obtain a coordinate change ϕ lowering the discriminant with $r = s = t = 0$ as follows.

Take the original Weierstrass equation and use ϕ_1 on it to obtain E'. This elliptic curve can be brought to reduced form E'_{red} by Lemma 6.3. So we have that E_{red} and E'_{red} are two elliptic curves in reduced form related by a coordinate change. Then this coordinate change must be have $r = s = t = 0$ acoording to Lemma 6.6. Call this coordinate change ϕ. This ϕ also has $v(\Delta') < v(\Delta)$. We can use this ϕ on the original E. But this would lower the valuation of one of the a_i below zero. But $\phi(E)$ and E' have the same discriminant and have $u \in \mathcal{R}^*$ and $r, s, t \in \mathcal{R}$ which would preserve the minimality of the equation. But one of the a_i in $\phi(E)$ has valuation less than zero, a contradiction. So no such ϕ can exist.

□

Example 6.7.

$$y^2 = x^3 - 27(1+t)x + 54(1-t) \tag{34}$$

Both coefficients have nonnegative valuation, the minimum of which being 0 (which is exactly what is demanded by the theorem). Note that the discriminant is given by

$$\Delta = 6298560t + 2519424t^2 + 1259712t^3 \tag{35}$$

which has valuation 1. So there are elliptic curves which are minimal but have $v(\Delta) > 0$.

Now that we have discussed conditions for minimality, we should investigate whether we can actually obtain a minimal equation for any Weierstrass equation. This boils down to reusing a trick from the first part of the proof of Theorem 6.5.

Lemma 6.8. *(***Existence of minimal models***) Suppose that E is an elliptic curve over $\mathcal{P}$ given by the Weierstrass equation:*

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

Then there exists an isomorphic curve E' such that its Weierstrass equation is minimal.

Proof. Consider the following minimum:

$$m = \min_j \{\frac{a_j}{j}\} \tag{36}$$

Now define u as $u = t^m$. According to the transformation rules we have the following:

- $u^i a_i{}' = a_i$
- $\Delta' = u^{12}\Delta$

In terms of valuations, this can be read as:

- $\mathrm{val}(a_i{}') = \mathrm{val}(a_i) - im = i(\frac{\mathrm{val}(a_i)}{i} - m) \geq 0$

We know however that m is attained for at least one of the a_i. Call that coefficient a_j. Then we have that $\mathrm{val}(a_j{}') = 0$. So at least one of the terms has a constant term and all the new coefficients have positive valuation. These conditions imply minimality of the equation according to theorem 6.5. We therefore have that the equation with the new coefficients is minimal. □

6.2. **Reduction.** We now introduce the concept of reducing an elliptic curve over $\mathcal{P}_{\geq 0} := \mathcal{R}$ to $\mathbb{C}$. This is done by the mapping

$$\begin{aligned} \phi: \quad & \mathcal{P}_{\geq 0} \longrightarrow \mathbb{C} \\ & f \longmapsto f(0) \end{aligned}$$

also known as the *reduction mapping*. It is a surjective homomorphism with the ideal

$$\mathcal{M} = \{f \in \mathcal{R} : v(f) > 0\}$$

in its kernel. We shall denote this map by $\phi(x) = \tilde{x}$. We can apply this reduction mapping to an elliptic curve $E(\mathcal{P})$ in Weierstrass form by applying it to the coefficients. This yields a curve $\tilde{E}(\mathbb{C})$. So if we have that $E(\mathcal{P})$ is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{37}$$

then $\tilde{E}(\mathbb{C})$ is given by:

$$y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6} \tag{38}$$

Suppose now that we transform our curve $E(\mathcal{P})$ by a Weierstrass coordinate change ϕ, with ϕ preserving minimality. This means that $u \in \mathcal{R}^*$ and $r, s, t \in \mathcal{R}$. The new curve, $E'(\mathcal{P})$ is related to the old one by the transformation table. If we reduce this new curve, then we obtain a curve $\tilde{E}'(\mathbb{C})$. This amounts to reducing the factors u, r, s and t. Since $\tilde{u} \neq 0$ we have that the reduced curve $\tilde{E}(\mathbb{C})$ is once again unique up to normal isomorphisms over the field of complex numbers.

Example 6.9. As a simple example, consider the the following elliptic curve:

$$y^2 = x^3 + (1 + t)x \tag{39}$$

This elliptic curve has discriminant $(48(t + 1))^3/1728$ and j-invariant 1728, both having zero valuation (making this elliptic curve minimal!). Reducing this curve yields the following elliptic curve over the field of complex numbers:

$$y^2 = x^3 + x \tag{40}$$

This is an elliptic curve with discriminant $48^3/1728$ and j-invariant 1728. In this case we once again obtain a non-singular curve. This is not always the case however.

After applying the reduction map on an elliptic curve we obtain a curve which is either nonsingular or singular. We designate a name for each case.

Definition 6.10. Let $E/\mathcal{P}$ be an elliptic curve with a minimal Weierstrass equation and let $\tilde{E}$ be the reduced curve.

(a) E has **good reduction** if $\tilde{E}$ is non-singular.
(b) E has **bad, multiplicative reduction** if $\tilde{E}$ is singular, where the singularity is a node.

(c) E has **bad, additive reduction** if $\tilde{E}$ is singular, where the singularity is a cusp.

Recall that $\tilde{E}$ is non-singular if and only if the discriminant $\tilde{\Delta} \neq 0$. This corresponds to $v(\Delta) = 0$. If $v(\Delta) > 0$, we obtain a singular curve because all the powers of t in Δ are removed.

Corollary 6.11. *Suppose that an elliptic curve E over $\mathcal{P}$ is given by a minimal Weierstrass equation. Then it cannot have additive reduction.*

Proof. Suppose that E has bad reduction and that the singularity is a cusp. We then have $\tilde{\Delta} = 0$ and $\tilde{c_4} = 0$. But this means that $\tilde{c_6}^2 = 0$ or $\tilde{c_6} = 0$. This contradicts minimality as we have seen in the proof of theorem 6.5. So we conclude that additive reduction *cannot* occur. □

If we have that the singularity is a node, then $\tilde{\Delta} = 0$ (or equivalently: $v(\Delta) > 0$) and $\tilde{c_4} \neq 0$. This means that $v(c_4) = 0$ and consequently $v(c_6) = 0$ too. In this case the constant terms of the two coefficients exactly cancel in the discriminant, making $v(\Delta)$ bigger than zero.
We now show that the two types of reduction can be read off the valuation of the j-invariant, as is reflected in the following theorem:

Theorem 6.12. *An elliptic curve E over $\mathcal{P}$ has:*

(a) *good reduction if and only if $v(j) \geq 0$*
(b) *bad, multiplicative reduction if and only if $v(j) < 0$*

Proof. (a) ($\Longrightarrow$) If E has good reduction then $v(\Delta) = 0$. Since

$$j = {c_4}^3/\Delta \tag{41}$$

We have that $v(j) = 3v(c_4) - 0 = 3v(c_4) \geq 0$.
($\Longleftarrow$) If $v(j) \geq 0$ then $v(j) = 3v(c_4) - v(\Delta) = 3v(c_4) - v(c_4^3 - {c_6}^2) \geq 0$. Or in other words: $3v(c_4) \geq v(\Delta)$. Suppose that $v(\Delta) > 0$. Then $v(c_4) > 0$ and consequently c_6 must have zero valuation (because we're assuming that our Weierstrass equation is minimal). But this would imply $v(\Delta) = 0$ which is the desired contradiction.
(b) ($\Longrightarrow$) If E has bad, multiplicative reduction then $v(\Delta) > 0$. Then once again we must have $v(c_4) = 0$. This implies $v(j) < 0$.
($\Longleftarrow$) Suppose that $v(j) < 0$. Then $3v(c_4) < v(\Delta)$. But this implies that $v(\Delta) > 0$ which implies bad reduction. This implies multiplicative reduction which completes the proof. □

6.3. **Reduction of Subgroups.** We can now more closely look at the structure in the reduced curve. We know that an elliptic curve over $\mathcal{P}$ can reduce to either a nonsingular or singular curve. We know from proposition (5.13) that the set of all nonsingular points of $\tilde{E}$ forms a group under the ordinary composition law: $\tilde{E}_{ns}$. If E has multiplicative reduction (and thus $v(j) < 0$) then $\tilde{E}_{ns} \cong \mathbb{C}^*$ by the same proposition.

A point on the original curve can now reduce to either $E_{ns} \cong \mathbb{C}^*$ or the set of singular points. We therefore introduce:

$$E_0 = \{P \in E(k) : \tilde{P} \in \tilde{E}_{ns}\}$$

Remark 6.13. This set does not depend on the minimal Weierstrass equation chosen. This follows from Lemma 6.4. To see this again we restate the content of the Lemma slightly differently: if two minimal equations are isomorphic then they are mapped to reduced equations which are also isomorphic.

On the elliptic curve $E(\mathcal{P})$ we have a group law which gives extra structure. One might wonder how this group law is transferred to the reduced curve. The following theorem tells us exactly how.

Theorem 6.14. *Let E be an elliptic curve with a minimal Weierstrass equation. Let E_0 be the set of points with nonsingular reduction. We then have that:*

- *(a) the set E_0 is a subgroup of $E(\mathcal{P})$.*
- *(b) the map $\phi : E_0 \to \tilde{E}_{ns}$ is a surjective homomorphism.*

Proof. The proof boils down to showing that the group law transfers to the reduced curve. The details are in [Silv09] chapter 7 paragraph 2. □

Proposition 6.15. *Let E be an elliptic curve with multiplicative reduction. Then there exists a point $P \in E[3]$ such that $P \notin E_0$*

Proof. Suppose we take an elliptic curve with multiplicative reduction. Then $\tilde{E}_{ns} \cong \mathbb{C}^*$. Suppose $P \in E[3]$. That is, P is of order 3. Suppose for a contradiction that every $P \in E[3]$ reduces to a nonsingular point. Since P is of order 3, its coordinates must have non-negative valuation by Nagell-Lutz. So $P = (x, y)$ is mapped to to $\tilde{P} = (\tilde{x}, \tilde{y})$ which has projective coordinates $\tilde{P} = [\tilde{x}, \tilde{y}, 1] \neq [0, 1, 0]$. This means that P does not reduce to the identity element of $\tilde{E}$.
We can now use Theorem 6.14 which says that the reduction map is a homomorphism. This means that

$$\phi(P + P + P) = \phi(P) + \phi(P) + \phi(P) = \phi(\mathcal{O}) = \tilde{\mathcal{O}}.$$

But this also means that $\phi(P)$ is of order 3 in $\tilde{E}_{ns} \cong \mathbb{C}^*$. But the there are exactly 2 points of order 3 in $\mathbb{C}^*$: the two complex numbers: $x = -\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$ such that

$x^3 = 1$. But the map $\xi : E[3] \to \mathbb{C}^*$ is injective (because P does not reduce to $\mathcal{O}$) and $E[3]$ has 8 points of order 3 because $E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This is the desired contradiction. □

We shall use this proposition in the proof of the main theorem of this thesis.

7. Tropical Geometry

In this section we will give the definitions we use for tropical varieties and other tropical notions. As was briefly mentioned in the introduction, everything in the tropical world takes a piece-wise linear form. This means that locally everything looks linear. In tropical geometry the structure of such piece-wise linear objects, known as *tropical varieties* is studied. The bigger these varieties get, the more and more they look like large honeycombs. Interest for the tropical world arose when people started deforming complex varieties. We shall study this approach as well as the purely algebraic approach.
The first approach uses the Puiseux series we introduced in section 2. Instead of deforming complex varieties using a limiting process, one can apply the valuation map on varieties over $\mathcal{P}$. This process is known as the **tropicalisation**. This is one way of reaching the tropical world.

The other approach starts with two special operations on the field $\mathbb{R}$ (taking a hint from the results of the first approach). These operations lead to a semi-ring. Using these operations one can set up tropical polynomials, which again form a semi-ring. These polynomials are then used to define first tropical curves and afterwards tropical hypersurfaces. These two approaches are linked to each other using Kapranov's theorem, which is often referred to as the "fundamental theorem of tropical geometry".
Having seen several important ideas from the tropical world, we can start working towards our main goal: tropical elliptic curves. One can define elliptic curves over the field $\mathcal{P}$ as usual. This variety can then be tropicalised using the methods given earlier in this section. What you get is called a tropical elliptic curve. Most of these curves have a bounded complex in their honeycomb structure. This bounded complex is called the **cycle** of a tropical elliptic curve. Mikhalkin showed that these cycles behave much like the j-invariant for normal elliptic curves: they are invariants under certain morphisms.
This was confirmed in [KMM00] by Katz, Markwig and Markwig. They showed that every elliptic curve with $v(j) < 0$ inducing a triangulisation in the marked subdivision must have a cycle with length $-v(j)$. Baker, Payne and Rabinoff later showed why some elliptic curves do not tropicalise to a proper tropical elliptic curve. As the main result of this thesis, we show that we can find an explicit equation for every elliptic curve with $v(j) < 0$ such that it tropicalises to the correct cycle length.

Before we can talk about more complex matters like these we first need to lay down some groundwork. We start with the simplest approach to tropical geometry: the purely algebraic one.

7.1. **Tropical Semi-ring.** We start by defining the tropical semi-ring: $\mathcal{R} := \mathbb{R} \cup \{\infty\}$. This is the normal real line together with "infinity". We define the following operations on $\mathcal{R}$:

- $a \oplus b = \min\{a, b\}$
- $a \odot b = a + b$

Let us check that this is indeed a semi-ring. We need $\mathcal{R}$ to be an abelian semi-group with respect to the operation $\oplus$. The identity element is given by ∞. Commutativity and associativity are obvious, the only thing missing is of course additive inverses. In fact, the only element having an additive inverse in this ring is ∞. This accounts for the word "semi" in semi-ring. The other properties needed for this set to be a ring are also easily verified.

Remark 7.1. $\mathcal{R}$ is commutative but it is not a semi-field. The element missing a "multiplicative" inverse is of course ∞. This is because tropical multiplication for ∞ is defined as $\infty \odot a = a \odot \infty = \infty$.

Remark 7.2. Some authors define the tropical semi-ring with the operation "$\oplus = \max$". This ring is isomorphic to the one we defined by the isomorphism $x \mapsto -x$.

Example 7.3. Let us perform some basic arithmetic:

$$2 \oplus 3 = 2$$
$$2 \oplus \infty = 2$$
$$(2 \odot \infty) \oplus 3 = \infty \oplus 3 = 3$$
$$(2 \oplus 3) \odot 5 = 7 = (2 \odot 5) \oplus (3 \odot 5) = 7 \oplus 8$$

Using these operations we can define **tropical polynomials**. We shall first define them for one variable x. We will interpret these as functions from $\mathcal{R} \longrightarrow \mathcal{R}$.

Definition 7.4. A **tropical polynomial** f of the form

$$f(x) = \bigoplus_{i=0}^{n} a_i \odot x^i$$

where x^i should be interpreted as $x \odot x \odot ... \odot x$ (i times).

Remark 7.5. We can rewrite this expression as $f(x) = \min_i\{a_i + ix\}$.

Lemma 7.6. *The set of all tropical polynomials forms a semi-ring when addition and multiplication are defined as:*

- $(f \oplus g)(x) = f(x) \oplus g(x)$
- $(f \odot g)(x) = f(x) \odot g(x)$

Seeing that these operations are well defined (that is, that the sum and product once again yield tropical polynomials) boils down to noting that if we have that

the minimum is attained for a certain term, then that term can be used for a new polynomial. All the other properties follow quite easily as well.
One can define the roots of the tropical polynomials. This definition will be analogous to the definition of general tropical varieties.

Definition 7.7. Let f be a tropical polynomial. Then x is a **tropical root** of f if for at least two terms p, q of f we have that $p(x) = q(x)$.

Example 7.8. Take the polynomial $f = \min\{2x + 1, 3x\}$. Then f has a root exactly where $2x + 1 = 3x$, or $x = 1$. Note that we can write f in tropical form as $f = (1 \odot x^2) \oplus x^3$. This is a polynomial of degree 3, but it only has 1 root.

Example 7.9. Take the polynomial $f = \min\{2x + 1, 3x, 2x\}$. We have as before $2x + 1 = 3x$ with $x = 1$ as a possible candidate for a root of f. But notice that the term $2x$ is smaller at $x = 1$. Therefore $x = 1$ is not a root anymore. Instead we have that $x = 0$ is a root since $0 < 1$.

To see how these tropical polynomials are related to normal polynomials we define the **tropicalisation** of a polynomial over a field k. Every field k comes with a valuation (we always have the trivial valuation). So if $f = \sum_{i=0}^{n} a_i X^i \in k[X]$ then we can apply such a valuation on every coefficient of f.

Definition 7.10. If $f = \sum_{i=0}^{n} a_i X^i$ and $v(\cdot)$ is a valuation on k then we define the **tropicalisation** of f at a point as:

$$\text{Trop}_v(f)(x) = \bigoplus_{i=0}^{n} (v(a_i)) + ix) \tag{42}$$

This allows us to tropicalise a wide range of polynomials on all sorts of fields.

Remark 7.11. Note that for the trivial valuation we have that $v(a_i) = 0$ for all $a_i \neq 0$ so we obtain the tropical polynomial:

$$\text{Trop}(f)(x) = \min_{i:a_i \neq 0} \{ix\}$$

This polynomial only has one root: $x = 0$.

These tropical roots can be related to the original roots of the polynomial. To show this we first need a preliminary result.

Theorem 7.12. *Suppose that f and g are polynomials in $k[X]$. Then*

$$\mathit{Trop}(f \cdot g)(x) = \mathit{Trop}(f)(x) + \mathit{Trop}(g)(x)$$

Proof. Suppose $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{j=0}^{n} b_j X^j$ so that $h = fg = \sum_{k=0} c_k X^k$ where $c_k = \sum_{i+j=k} a_i b_j$. Then $\mathrm{Trop}(fg)(x) = \min_k\{v(c_k) + kx\}$. One of the properties of the valuation then gives us

$$\begin{aligned} \min_k\{v(c_k) + kx\} &\geq \min_k\{\min_{i+j=k}\{v(a_i) + v(b_j)\} + ix + jx\} \\ &= \min_i\{v(a_i) + ix\} + \min_j\{v(b_j) + jx\} \\ &= \mathrm{Trop}(f)(x) + \mathrm{Trop}(g)(x) \end{aligned}$$

Now we need $\mathrm{Trop}(fg)(x) \leq \mathrm{Trop}(f)(x) + \mathrm{Trop}(g)(x)$. To prove this we will need the following inequality:

$$\text{if } v(a) < v(b) \text{ then } v(a+b) = v(a).$$

Now take i_0 and j_0 maximal such that $v(a_{i_0}) + i_0 x = \mathrm{Trop}(f)(x)$ and $v(b_{j_0}) + j_0 x = \mathrm{Trop}(g)(x)$. Define $k_0 = i_0 + j_0$. We will show that

$$v(c_{k_0}) = v(a_{i_0}) + v(b_{j_0})$$

which implies that

$$\min\{v(c_k) + kx\} \leq v(c_{k_0}) + k_0 = v(a_{i_0}) + ix + v(b_{j_0}) + jx$$

as desired.
Let $i > i_0$ then by maximality of i_0 we have that $v(a_i) + ix > v(a_{i_0}) + i_0 x$ or $v(a_{i_0}) < v(a_i) + (i - i_0)x$. For j we then have that $v(b_{i_0}) \leq v(b_i) + i - i_0 x$. Adding these two equations yields:

$$v(a_{i_0}) + v(b_{j_0}) < v(a_i) + v(b_j) + (i + j - i_0 - j_0)x = v(a_i) + v(b_j)$$

We claim that the same holds if $i < i_0$. We know that $j_0 = k_0 - i_0$. But this means $k - i = j > k_0 - i_0 = j_0$. We can therefore repeat the same argument but this time for $j > j_0$. We therefore have

$$v(a_{i_0}) + v(b_{j_0}) < v(a_i) + v(b_j)$$

for all i and j not equal to i_0, j_0. But then according to Lemma 3.4 we must have that $v(c_{k_0}) = v(\sum_{i+j=k_0} a_i b_j) = v(a_{i_0}) + v(b_{j_0})$ which proves the statement. □

So we have that Trop preserves the multiplicative structure of polynomials (where "+" is understood to be tropical multiplication). Using this theorem we can prove the following lemma:

Lemma 7.13. *Suppose f is a monic polynomial in a single variable over an algebraically closed field k. Then for any valuation v, we have that*

$$v\{\textit{roots of } f\} = \{\textit{roots of } \mathit{Trop}(f)\}$$

In other words, v maps the roots of f to the roots of $\mathit{Trop}(f)$ surjectively.

Proof. Write f as $\prod_{i=0}^{n}(X-\alpha_i)$. Then according to Theorem 7.12 we have that $\text{Trop}(f)(x) = \sum_{i=0}^{n}\text{Trop}(x-\alpha_i) = \sum_{i=0}^{n}\min\{x, v(\alpha_i)\}$. But this least minimum can only be attained twice if $x = v(\alpha_i)$. So v maps the roots of f to the roots of $\text{Trop}(f)$. Suppose that y is a root of $\text{Trop}(f)$. Then it must be one of the $v(\alpha_i)$, which proves the claim. □

We defined the $\text{Trop}(f)(x)$ by applying the valuation to every coefficient. What this lemma says it that the valuation preserves the roots of f. This lemma can be used to give a slightly different (tropical) proof of Eisenstein's Criterion for irreducibility.

Theorem 7.14. *(***Eisenstein's Criterion***) Suppose that $f \in R[X]$ of degree $n \geq 2$ for a unique factorisation domain R and that there is an irreducible element p such that $p|a_i$ for $0 \leq i < n$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over $R[X]$.*

Proof. Suppose f is reducible, so that $f = gh$ with g, h having a lower degree than f. Since p is an irreducible element, we can define a valuation on the quotient field of R. Every element of this field can uniquely be written as $y = p^k\frac{l}{m}$, where $k \in \mathbb{Z}$ and $l, m \in R$ such that $p \nmid l, m$. For every nonzero element we define the valuation as $v(y) = k$.
With this valuation we can start tropicalising our polynomial. Note that $v(a_i) \geq 1$ for $0 < i < n$, $v(a_n) = 0$ and that $v(a_0) = 1$. The tropicalisation takes the following form:

$$\text{Trop}(f)(x) = \min\{v(a_i) + ix\}$$

Consider this tropical polynomial for $x \geq 0$. Since $v(a_i) \geq 1$ we have that $v(a_0) = 1 \leq v(a_i) + ix$ for $x \geq 0$ and $0 < i < n$. Thus $\text{Trop}(f)(x)$ will attain the value 1 for some x. The term $v(a_n) + nx = 0 + nx = nx$ will be smaller than 1 for certain x. In fact we have that $\text{Trop}(f)(x)$ has one root exactly at $x = 1/n$. This statement needs some backup from a theorem on valuations:

Theorem 7.15. *Suppose that k is a field with a valuation v. Then v extends uniquely to a valuation on the algebraic closure $\bar{k}$.*

Proof. See [Ser79] for the proof. □

So we can use this extended valuation which allows values like $1/n$. Now remember that the tropical roots correspond to a root of f over the algebraic closure of $\text{Quot}(R)$. These roots must multiply to a_0 which has $v(a_0) = 1$. Therefore any negative tropical roots are not allowed, making $1/n$ the only tropical root. Since $f{=}gh$, we know that $\text{Trop}(f) = \text{Trop}(g) + \text{Trop}(h)$. But this means that $1/n$ is a tropical root of at least one of g or h (in fact of both). But $\deg(g) < n$ and the product of the roots of g must be an element of R. This is impossible, since a product of less than n terms all having valuation $1/n$ will have valuation less than 1 (which is not an element of R by irreducibility of p). □

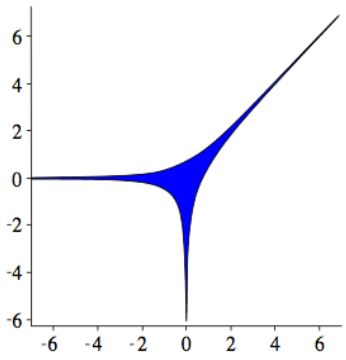


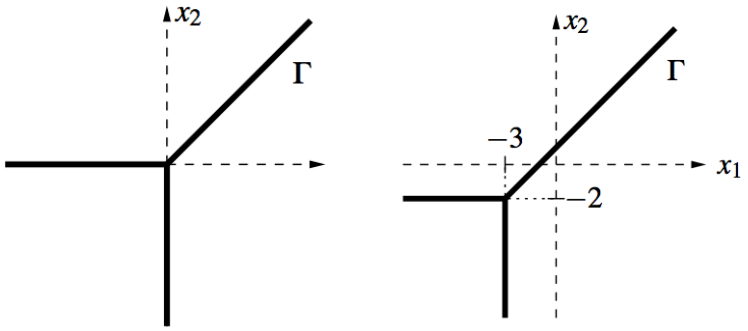
FIGURE 4. The amoeba of $z_1 + z_2 = 1$

7.2. **Amoebas.** In this section we will see the connection between the Puiseux Series defined earlier and the tropical world defined in the section above. We already saw a hint of the connection in the definition of the tropicalisation of a polynomial. We used a valuation to map an element of a field to $\mathbb{R}$. This will exactly be the more general definition of **tropicalisation**. Here we will see how this definition works for a variety. We consider a complex variety V and then take a logarithm map to construct something in $\mathbb{R}^2$. Taking limits will result in the tropical curve, which will be defined using valuations.
We first construct the amoeba of a complex plane curve C. A complex plane curve is something of the form $C = \{(z_1, z_2) : f(z_1, z_2) = 0\}$ for some $f \in \mathbb{C}[X, Y]$. The idea is to restrict to the open subset $(\mathbb{C}^*)^2$ of the complex plane and then to map it to the real plane by the map:

$$\begin{aligned} \text{Log} : \quad & (\mathbb{C}^*)^2 \longrightarrow \mathbb{R}^2 \\ & z = (z_1, z_2) \longmapsto (x_1, x_2) := (\log|z_1|, \log|z_2|). \end{aligned}$$

The resulting subset $A = \text{Log}(C \cap (\mathbb{C}^*)^2)$ is called the **amoeba** of C.

Example 7.16.
- (a) Suppose we take the plane curve $z_1+z_2 = 1$. There are two points with z_i coordinate zero: $(1, 0)$ and $(0, 1)$. Suppose we take $(0, 1)$ first, then points close to this point are mapped to $(-\infty, 0)$ by the Log map. This corresponds to the tentacle going to the left. Similarly we have a tentacle for the point $(1, 0)$. The tentacle going to the upper-right part corresponds to the points $(z, 1 - z)$ for $|z| \to \infty$.
- (b) Now take the slightly different plane curve defined by $e^3 z_1 + e^2 z_2 = 1$. The easy way to find tentacles is to look for the limit behaviour of Log near a zero coordinate. If we set $z_2 = 0$ then we find the point $z_1 = 1/e^3$. This



(A) The first amoeba tropicalised

(B) The second amoeba tropicalised

FIGURE 5. The tropical curves for the amoebas

point is mapped to $\log(z_1) = -3$. Likewise we have that the point $(0, 1/e^2)$ is mapped to the point $(-\infty, -2)$. The other points follow as well. We see that this is the same amoeba as in (a), only we have that this one is translated over $(-3, -2)$.

As can be seen in Figure 4, the resulting figure in $\mathbb{R}^2$ for the plane curve $z_1 + z_2 = 1$ has three tentacles going to infinity and one eye in the middle. Our wish is now to shrink the area of these tentacles and the eye to zero. This can be done using the following modification of the logarithm map:

$$\begin{aligned} \mathrm{Log}_t : \quad & (\mathbb{C}^*)^2 \longrightarrow \mathbb{R}^2 \\ & z = (z_1, z_2) \longmapsto (-\log_t |z_1|, -\log_t |z_2|) = (-\frac{\log |z_1|}{\log t}, -\frac{\log |z_2|}{\log t}). \end{aligned}$$

for $t \in \mathbb{R}$ small. We call the limit of $t \longrightarrow 0$ the **tropical curve** associated to C.

Definition 7.17. Let $C \subseteq \mathbb{C}^2$ be a complex plane curve. We define the **tropical curve** of C as $V = \lim_{t \to 0} \mathrm{Log}_t(C \cap (\mathbb{C}^*)^2)$

Example 7.18. The tropical curve of the first amoeba discussed in Example 7.16 is shown in Figure 5 . If we were to apply the same limit map to the "shifted" amoeba then we would obtain the same tropical curve as for the unshifted curve. This is because the points in the plane are not fixed, in fact we have that the parameter t sends the center to $(0, 0)$

This is obviously not what we want. We therefore introduce a **family of curves**:

$$C_t = t^{-3}z_1 + t^{-2}z_2 = 1$$

Note that for $t = e^{-1}$ we indeed obtain the shifted plane curve. In fact we have that C_t always passes through the points $(0, t^2)$ and $(t^3, 0)$ for all t. Thus we have fixed the points with zero coordinates which are mapped to the tentacles. We now have the proper tropical curve, as can be seen in Figure 5 again.

7.3. **Connection to Puiseux Series.** To actually construct tropical curves using the previous method requires one to use a limiting process for each curve (or family of curves). As was seen in Example 7.18, the tropical curve defined by an amoeba doesn't depend on a particular curve but a **family of curves**. We therefore consider curves defined over a field with a parameter, like for instance the field $\mathcal{P}$. This greatly simplifies the limiting process, as we shall see that the tropical curve of a family of plane curves is defined solely by the **valuations** of the coefficients.
We consider a family of curves C_t. This family is represented by one single curve over $\mathcal{P}$. Thus we have a polynomial $f \in \mathcal{P}[X, Y]$. A coefficient of this polynomial is of the form $a = \sum_k a_k t^k$ with $k \in \mathbb{Q}$. Define $w := v(a)$. Then by complex function theory we have that $|a| \approx |a_w t^w|$ for $t \to 0$. Applying the map Log_t we obtain:

$$\mathrm{Log}_t(|a|) \approx \frac{-\log|a_w t^w|}{\log t} = \frac{-\log|a_w| - w\log|t|}{\log t}$$

The first term vanishes and we are left with the conclusion $\mathrm{Log}_t(|a|) \to -v(a)$. Therefore we have that any limiting process on a curve in $\mathbb{C}^2$ reduces to taking the valuation of the coefficients. We extend the valuation mapping as follows:

$$\begin{aligned} v: \qquad (\mathcal{P}^*)^2 &\longrightarrow \mathbb{R}^2 \\ z = (z_1, z_2) &\longmapsto (x_1, x_2) := (v(z_1), v(z_2)). \end{aligned}$$

Restricting this map to a plane curve C yields the following definition:

Definition 7.19. A **tropical plane curve** is a subset $\mathrm{Trop}(C)$ of $\mathbb{R}^2$ of the form $\mathrm{Trop}(C) = \overline{v(C \cap (\mathcal{P}^*)^2)}$ where C is a plane curve in $\mathcal{P}^2$.

Remark 7.20. The completion is taken to ensure we have values in $\mathbb{R}^2$. This is because the natural valuation maps to $\mathbb{Q}$.

Remark 7.21. It would seem more natural now to define the plane tropical curve using $-v(a)$ instead of $v(a)$. This definition would lead to a necessary change in the definition of our tropical semi-ring. That is, we would have to change the minimum to a maximum for the upcoming alternative description. We used a minimum for our tropical semi-ring (because it makes the tropicalisation easier) and thus we shall

use $v(a)$. Note that these descriptions are the same by the isomorphism given earlier in remark (7.2).

This is our first rigorous definition of a tropical plane curve. It does not involve any limit processes and is entirely algebraic of nature. It is however still quite unhandy as it involves computing the valuation of every point on the curve. We shall remedy this shortly, but first we give an example.

Example 7.22. Let us consider the plane curve defined by $t^{-3}z_1 + t^{-2}z_2 = 1$ with $(z_1, z_2) \in (\mathcal{P})^2$. If we take a point (z_1, z_2) then it depends on the valuation of the coordinates where the point ends up.

- Suppose we take $v(z_1) > 3$. Then we must have $v(z_2) = 2$ or otherwise we wouldn't get $v(1) = 0$. Thus for $x > 3$ we get $y = 2$.
- Suppose that $v(z_2) > 2$. Then we similarly obtain $v(z_1) = 3$ or in other words: for $y > 2$ we have $x = 3$.
- Suppose now that $v(z_1) \leq 3, v(z_2) \leq 2$. Then the leading terms of $t^{-3}z_1$ and $t^{-2}z_2$ must cancel. In order for that to happen they must have the same valuation, so $-3 + v(z_1) = -2 + v(z_2)$ or $v(z_1) = 1 + v(z_2)$. This corresponds to the line $y = 1 - x$ This is the third tentacle we were looking for.

The trick used above to find the tentacles can be quite explicitly described. A way to do this is using the tropical semi-ring.
Suppose we have a polynomial in two variables $f(z_1, z_2) = \sum_{i,j} a_{ij} z_1^i z_2^j$. Then the valuation of an individual summand is as follows:

$$v(a_{ij} z_1^i z_2^j) = v(a_{ij}) + iv(z_1) + jv(z_2)$$

For a point $(z_1, z_2) \in C$ we have that the valuation of all of these summands add up to zero.

Remark 7.23. Note that this should be seen as follows: a condition on the valuation of one coordinate induces a condition on the other. From the equation $f(z_1, z_2) = 0$ one might get the impression that we should impose the condition $v(f(z_1, z_2)) = v(0) = \infty$, but this is definitely not the case since we don't want the function to be identically zero but only locally.

Either way we have that at least two of the valuations must be equal to each other or otherwise we wouldn't have any cancellations. Thus we have the condition that at a point on the tropical curve the minimal valuation should occur at least twice among the summands. We can paraphrase this as follows: at a point on the tropical curve we have that in the tropical polynomial

$$\mathrm{Trop}(f)(x, y) = g(x, y) := \min\{v(a_{ij}) + ix + jy\}$$

the minimum should be attained at least twice. We give this a special name:

Definition 7.24. (**Corner Locus**) The points in $\mathbb{R}^2$ where a tropical polynomial in two variables takes on the minimum at least twice is known as the **Corner locus** of the tropical polynomial.

Thus we have shown that any tropical curve is contained in the corner locus of its tropicalisation. The converse inclusion holds as well and is known as **Kapranov's Theorem** or the "**fundamental theorem of tropical geometry**".

Theorem 7.25. *(A version of Kapranov's Theorem) For any plane curve $C \subset \mathcal{P}^2$ with defining polynomial f we have that the following two sets coincide:*

- *The tropical plane curve Trop(C)*
- *The corner locus of the tropical polynomial Trop$(f)(x, y)$*

Proof. For a proof see [Kap00]. □

This theorem shows an intimate connection between tropical geometry and normal geometry: the object obtained by using the valuation on a variety can be described entirely by tropical polynomials. In fact we shall only use this method from now on to tropicalise plane curves (and in particular elliptic curves).

Example 7.26. Let's use Kapranov's theorem to find the tropicalisation of the plane curve given by:

$$t^{-3}z_1 + t^{-2}z_2 = 1$$

We know that the tropical plane curve is given as the corner locus of the following polynomial:

$$\mathrm{Trop}(f)(x, y) = \min\{x - 3, y - 2, 0\}$$

It is now very easy to find everything we want, we just solve a couple of linear equations. We obtain $x = 3$ for $0 < y - 2$ or $y > 2$. Similarly we find $y = 2$ for $x > 3$ and $y + 1 = x$ for $y \leq 2$ and $x \leq 3$. One can immediately see the benefits of using this theorem : what used to be a tedious limit process has now turned into 3 very simple linear equations.

Remark 7.27. Adding a constant value to all of the $v(a_{ij})$ corresponds to a translation of the tropical curve. This is basically just dividing/multiplying by a certain power of t in the original equation.

7.4. **Newton Subdivision.** Even for such tropical polynomials it can still become quite tedious to solve all of these linear equations (and inequalities) by hand. There is an easy way which is known as the **Newton subdivision** which makes a compact graph from the data available which essentially contains all of the information needed

to draw the corresponding tropical graph. We first give the algorithm and then try to clarify the process.
Let $f = \bigoplus_{i,j} a_{ij}x^i y^j$ be a tropical polynomial. For every $a_{ij} \neq 0$ we associate the following set of points to the tropical polynomial: $(i, j) \in \mathbb{N}^2$. These form a **lattice**. Call this lattice Λ. We give an algorithm to draw a tropical curve using this lattice. The algorithm starts by considering the points $(i, j, a_{ij}) \in \mathbb{R}^3$. We then take the convex hull of these points:

$$W = \text{ConvexHull}\{(i, j, a_{ij})\}$$

Now project the lower part of W back to the lattice Λ to create a subdivision of Λ. Put differently: we get a convex polygon W which has edges. We project the lower edges back onto the lattice Λ. This subdivision is called the **Newton subdivision** of f: $\mathcal{L}$. We then have the following correspondence:

- Every edge of the Newton subdivision $\mathcal{L}$ corresponds to an edge of the tropical curve. These corresponding edges lie in orthogonal subspaces. That is, the edge of $\mathcal{L}$ will be orthogonal to its corresponding edge in the tropical curve.
- Every interior edge of the Newton subdivision corresponds to a bounded edge of the tropical curve.
- Every outer edge of the Newton subdivision corresponds to an unbounded edge (or: ray) of the tropical curve.

We now explain this algorithm by studying the tropical curve locally. Throughout this explanation one should keep an eye on Figure **??**. Suppose we have a tropical curve in $\mathbb{R}^2$. This curve is a union of line segments all emanating from certain points. Suppose we take such a vertex V. If we take this V as a new origin in $\mathbb{R}^2$ then we can locally describe the tropical curve as lines emanating from this origin. We can therefore locally define the tropical curve by a tropical polynomial which takes the following form:

$$g(x, y) = \bigoplus_i {x_1}^{a_1(i)} \odot {x_2}^{a_2(i)}$$

where $a_1(i), a_2(i) \in \mathbb{N}$. Now plot these points $a(i) := (a_1(i), a_2(i))$ in $\mathbb{N}^2$ and let Δ be the **convex hull** of these points. This will be a convex polygon in $\mathbb{R}^2$. Our first claim is that the tropical curve only depends on the outer edges of this convex polygon Δ. This is because it is impossible for an interior point that the expression $a_1(i)x_1 + a_2(i)x_2$ is smaller than the others. We can therefore delete the terms corresponding to interior points.
From the definition of a tropical curve we know that we must now solve linear equations. These are given by:

$$a_1(i)x_1 + a_2(i)x_2 = a_1(j)x_1 + a_2(j)x_2$$

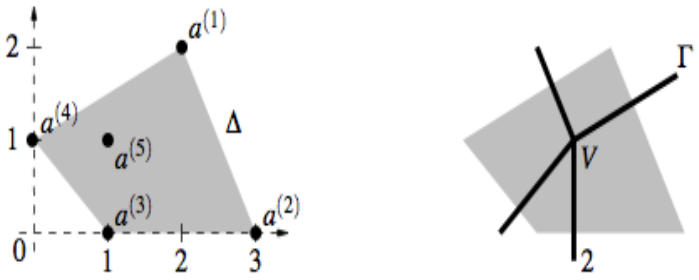


FIGURE 6. The local construction of the Newton subdivision

If any more equations were used then we would obtain an overdetermined system which only yields the solution $(0, 0)$ corresponding to the vertex. The next claim is that we only have to use the equations for **adjacent vertices**. Let us first see why the tropical curve should be orthogonal to the edges defined by adjacent vertices. When solving such a linear equation we can rewrite this expression as an inner product:

$$(a_1(i) - a_1(j))x_1 + (a_2(i) - a_2(j))x_2 = 0$$

but the vector used in this inner product is exactly the direction vector of the edge linking the points $(a_1(i), a_2(i))$ and $(a_1(j), a_2(j))$. So now we know that the points on the tropical curve should be in a subspace of $\mathbb{R}^2$ orthogonal to the edge defining them. Now if the defining points weren't adjacent, then there would be a point $(a_1(k), a_2(k))$ closer to this orthogonal subspace. Consequently the expression $a_1(k)x_1 + a_2(k)x_2$ would be smaller than the ones defining the subspace, which means that the minimum is not attained.

This shows how to construct the Newton subdivision once the local defining equations are known. It is usually hard to immediately see these local equations directly. Computing the convex hull in $\mathbb{R}^3$ boils down to finding these local equations. Locally we have that the terms with the lowest valuation will have the most influence, which gives some idea as to why we take lower part of the convex hull of the points (i, j, a_{ij}).

Remark 7.28. When considering a tropical curve we sometimes only give the Newton subdivision, where it is understood that curves with the same Newton subdivision give rise to the same tropical curve (up to a translation).

The last thing we need from these Newton subdivisions is **direction vectors**. Every edge in the Newton subdivision defines a direction. We formalise this as follows:

Definition 7.29. Let $\mathcal{L}$ be the Newton subdivision of f. Let T be an edge in this subdivision with endpoints (x_1, y_1) and (x_2, y_2). We define the **direction vector** $vec(F) = (y_2 - y_1, x_1 - x_2)$.

Remark 7.30. Note that this direction vector is perpendicular to the edge used to define it. By definition of the Newton subdivision it lies in the same direction as the corresponding tropical edge.

7.5. **Tropical Elliptic Curves.** In this section we shall explain what a tropical elliptic curve is. We start with an elliptic curve over $\mathcal{P}$. In order to have proper tropicalisations we need a more general form for an elliptic curve than the ordinary reduced Weierstrass equation. To that end we quickly explain how we can consider more elliptic curves using the **Newton polygon** and the corresponding **Newton subdivision**. These will tell us whether a given curve has genus 1.

From section (5) we know that an elliptic curve is a curve of genus 1 with a specified base point $\mathcal{O}$. Using the Riemann-Roch Theorem one can always put such an elliptic curve in Weierstrass form. We now seek more general forms however. A way to do this is using Newton polygons. Suppose that we have a plane curve defined by

$$f = \sum_{i,j} a_{ij} x^i y^j \tag{43}$$

where $a_{ij} \in \mathcal{P}$. Now consider the points (i, j) in $\mathbb{N}^2$ for which $a_{ij} \neq 0$. Call the set of these points $\Lambda_f \subset \mathbb{N}^2$.

Definition 7.31. Let Λ_f be as before. Then we define the **Newton polygon** of f to be $\mathcal{N}_f := \text{ConvexHull}(\Lambda_f)$.

The following theorem now tells us how to find the genus of such a curve:

Theorem 7.32. *Let f be as in (43) and $\mathcal{N}_f$ its Newton polygon. Then the genus of the curve defined by f is at most the amount of interior lattice points of $\mathcal{N}_f$. If f is smooth then the genus is equal to the amount of interior lattice points.*

Remark 7.33. For more explanation on Newton polygons, see [Kob84]

Thus we can characterise elliptic curves as being smooth curves with $\mathcal{O}$ and with the Newton polygon having one interior point. This also means that we can restrict to the triangle with vertices $(0, 0), (0, 3)$ and $(3, 0)$. Every elliptic curve can be brought to a form with corresponding Newton polygon in this triangle.

Example 7.34. Suppose we have the curve $E_1 : y^3 = x^3 + 1$. Then its Newton polygon is just the triangle corresponding to the vertices $(0, 0), (0, 3)$ and $(3, 0)$ which has $(1, 1)$ as an interior point. Thus this curve has a maximal genus of 1. The partial

derivatives are zero at $(x, y) = 0$ which is not a point on the curve, making this curve nonsingular. It therefore has genus 1.

Example 7.35. Let E_2 be the curve defined by the equation

$$b + 2\sqrt{a}xy + x^2y + y^2x = 0$$

for $a, b \neq 0$. It has one interior point so it has at most genus 1. The partial derivatives are also never zero, so it indeed defines a smooth elliptic curve. We can actually almost see the Weierstrass form. If we homogenise this equation with z then we obtain:

$$bz^3 + xyz + x^2y + y^2x = 0 \tag{44}$$

Dehomogenising with respect to y now leads to:

$$bz^3 + xz + x^2 + x = 0 \text{ or } x^2 = -bz^3 - xz - x \tag{45}$$

which is in Weierstrass form. We therefore see that the original equation is an affine piece of the entire projective elliptic curve. This particular curve will be used in the main theorem of this thesis.

Definition 7.36. Let E be an elliptic curve over $\mathcal{P}$ defined by the polynomial f. We define the **tropical elliptic curve** corresponding to f as $\mathrm{Trop}(E_f)$

Remark 7.37. (**Important**) Note that this definition relies enormously on the f used for the tropicalisation. In fact we have that two isomorphic elliptic curves can give rise to entirely different tropical elliptic curves. This makes the definition non-intrinsic, but it at least gives a place to start. We give an example to demonstrate this phenomenon.

Example 7.38. Consider the elliptic curve E_3 defined by

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

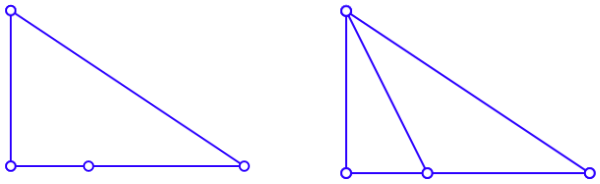
for $A, B \in \mathcal{P}$. Then the tropicalisation depends on the valuation of A and B, but combinatorially we have two possibilities as can be seen in figure (7). The second subdivision gives rise to the tropical curve in figure (8).

Example 7.39. Consider again the elliptic curve E_2 defined by

$$b + 2\sqrt{a}xy + x^2y + y^2x = 0$$

for $a, b \neq 0$ and $v(a) = 0$ and $v(b) > 0$. The tropical elliptic curve has a Newton subdivision and tropical curve as can be seen in figure (9).

What is different in this last elliptic curve is that we have a **bounded complex** in the middle. In fact we have that for a large class of elliptic curves that they contain such a complex. This bounded complex serves as the tropical analogue of the j-invariant. We study this tropical j-invariant in the next section.



(A) Possibility 1 (B) Possibility 2

FIGURE 7. Newton subdivisions for Weierstrass equations

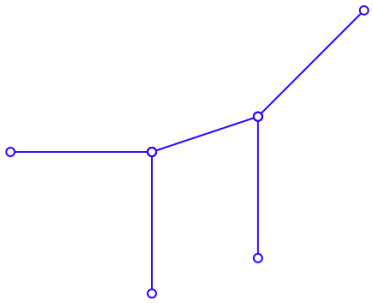
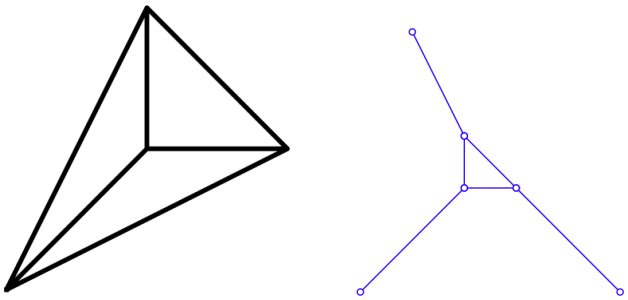


FIGURE 8. Tropical curve for the marked subdivision in fig. (7b)



(A) Subdivision (B) Trop(E_2)

FIGURE 9. The tropical versions of E_2

Remark 7.40. The curves E_2 and E_3 are actually isomorphic, as we will show in our main theorem. Thus we have that two isomorphic elliptic curves have distinct tropicalisations: one doesn't have a bounded complex and the other one does.

7.6. **Cycles and Tropical j-invariants.** In this section we study this bounded complex in more detail. It is more commonly known as the **cycle** of the curve. An important quantity of a tropical elliptic curve is the **cycle length**. This can be used to define a tropical counterpart of the normal j-invariant: the **tropical j-invariant**. This tropical j-invariant is an invariant of tropical morphisms (see [BPR11] or [Mik06]). At the end of this section we shall give the theorem derived by Katz, Markwig and Markwig in [KMM00]. This theorem links the two j-invariants. We begin with a proper definition of a cycle.

Definition 7.41. Let $\mathrm{Trop}(E)$ be a tropical elliptic curve. Suppose that the point $(1,1)$ is visible as a vertex of a polygon $\Delta' \subset \mathcal{N}_f$. By visible we mean that there at least three lines emanating from $(1,1)$ in the Newton subdivision. We then say that $\mathrm{Trop}(E)$ has a **cycle**.

Remark 7.42. Let us give an alternative description of this cycle. The lines emanating from the point $(1,1)$ all lie within the Newton polygon and thus correspond to bounded edges. Since the lines orthogonally correspond to edges, we need at least three lines to "go around a point". These edges thus create a connected bounded complex, a cycle.

Example 7.43. Let E be an elliptic curve with reduced Weierstrass form

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

As we saw in Example 7.38, any elliptic curve given by such a Weierstrass form has **no cycle**. Since every elliptic curve over $\mathcal{P}$ can be brought in this form using the Riemann-Roch Theorem, we have that cycles are not preserved by isomorphisms.

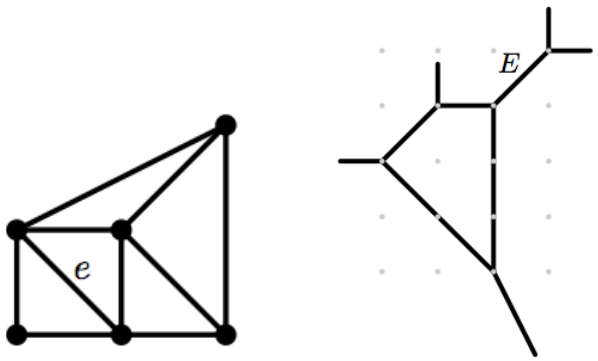
Every edge, G_i, of the **cycle** corresponds to an edge of the Newton subdivision. Thus for every G_i we have a specific **direction vector**: F_i. To every such edge G_i of the cycle we can associate a special length:

$$l(G_i) = \frac{||G_i||}{||F_i||}$$

where $||\cdot||$ is the normal Euclidean length.

Remark 7.44. This weight factor $||F_i||$ is introduced to obtain a value in $\mathbb{Q}$ for $l(G_i)$.

We can now define the **cycle length**:



(A) Newton subdivision (B) Tropical curve

FIGURE 10. Tropical forms of f_4

Definition 7.45. Let E be an elliptic curve over $\mathcal{P}$ with defining equation f and let $\text{Trop}(E)_f$ be the corresponding tropical elliptic curve. If $\text{Trop}(E)_f$ has a cycle, then we define the **cycle length** as:

$$\mathcal{C}(E) := \sum l(G_i)$$

Remark 7.46. This cycle length shall also be referred to as the **tropical j-invariant**:= j_{trop}.

Example 7.47. Let E_4 be the elliptic curve defined by

$$f_4 = xy + t \cdot (y + x + x^2 + x^2y^2) + t^3$$

The tropicalisation of f is:

$$\text{Trop}(f)(x, y) = \min\{x + y, 1 + y, 1 + x, 1 + 2x, 1 + 2x + 2y, 3\}$$

We can also consider the corresponding Newton subdivision $\mathcal{L}$ as is depicted in Figure 10a. To see why this makes sense, note that all the terms have valuation 1 except the ones corresponding to $(0, 0)$ and $(1, 1)$. This also gives the tropical curve as you can see from Figure 10b.

The tropical elliptic curve has a cycle and hence we can calculate its cycle length. To do this we need the length of the direction vectors. Notice that there are two direction vectors of length 1 and two of length $\sqrt{2}$. The Euclidean length of the edges in the tropical curve are as follows:

$$||G_1|| = 1, \quad ||G_2|| = 3 \quad ||G_3|| = \sqrt{2} \cdot 2 \quad ||G_4|| = \sqrt{2} \cdot 1$$

This length is then normalised by the length of the direction vectors which gives:

$$\mathcal{C}(E) = 1 + 3 + 2 + 1 = 7$$

This cycle length can be related to the valuation of the original j-invariant under certain conditions. This is the essence of the next theorem:

Theorem 7.48. [KMM00] *Let E be an elliptic curve defined by the polynomial f. If $Trop(f)$ has a cycle and if it induces a triangulisation in the Newton subdivision then*

$$v(j(E)) = j_{trop}$$

Remark 7.49. A triangulisation of the Newton subdivision is a subdivision of the Newton polygon which consists entirely of triangles.

Note that this is a theorem on a particular equation of the elliptic curve. If $Trop(f)$ has $(1, 1)$ as a visible point in the Newton subdivision and if the subdivision is a triangulisation then we have that the theorem holds. Thus if we take an isomorphic elliptic curve which does not induce a triangulisation then we can get different results.

Example 7.50. Consider the tropical elliptic curves as in Figures 11 and 12. We have that the first curve in Figure 11 does not induce a triangulisation, although it does have a bounded complex. Note however that this curve can be written as the union of three tropical lines! The bounded complex is therefore just a coincidence: it is not a property of the elliptic curve. It can be shown that it does not have the right cycle length.
The second curve in Figure 11 does induce a triangulisation, but it does not contain $(1, 1)$ as a visible point. It therefore does not have a cycle. This curve is actually the tropical equivalent of a biquadratic curve (something with tropical genus 0). It also does not have the right cycle length.
The first curve in Figure 12 is an example of a proper tropical elliptic curve: the subdivision is a triangulisation and $(1, 1)$ is a visible point. The second curve however does not induce a triangulisation.

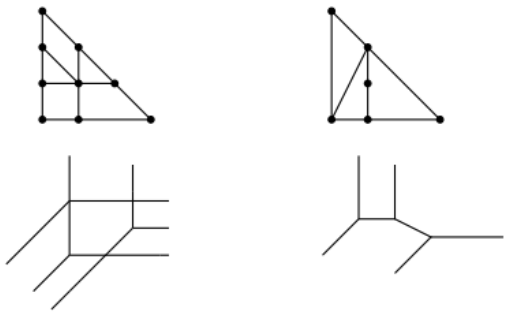


FIGURE 11. Two curves without a triangulisation

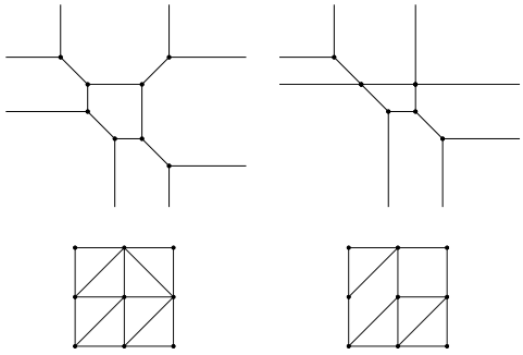


FIGURE 12. One curve with a triangulisation and one without

8. Main Theorem

We conclude this thesis by proving the main theorem. From [KMM00] we know that every elliptic curve over $\mathcal{P}$ with $v(j) < 0$ that induces a triangulation in the Newton subdivision will have a cycle in its corresponding tropical curve with cycle length equal to $-v(j)$. Here we consider another question. Suppose that we are given an elliptic curve with j-invariant j. Can we find an isomorphic elliptic curve such that its tropicalisation has cycle length equal to $-v(j)$? We do this by explicitly giving the isomorphic elliptic curve.
We'll use the following notation in this section:

- If f is the polynomial defining the elliptic curve, then $\text{Trop}(f)$ is its corresponding tropical polynomial

- If C_f is the curve corresponding to f, then $\mathrm{Trop}(C_f)$ is the corresponding tropical variety
- Δ will be the marked subdivision of $\mathrm{Trop}(E)$
- $\mathcal{C}(E)_f$ is the cycle length of a tropical elliptic curve with equation f

The main idea of how to find an isomorphic elliptic curve with the right tropicalisation is as follows. We know that an elliptic curve with $v(j) < 0$ has multiplicative reduction by Theorem 6.12. We take a point of order 3 and then put the equation in a particular Weierstrass form. This Weierstrass form can then be transformed to an elliptic curve not in Weierstrass form such that the tropicalisation has a cycle. We then calculate the cycle length, which will be equal to $-v(j)$. Let us now precisely state the theorem:

Theorem 8.1. *(***Main Theorem***) For every elliptic curve over $\mathcal{P}$ with $v(j) < 0$, we can find an isomorphic elliptic curve E' such that:*

- *Trop(E') has a cycle*
- $\mathcal{C}(E') = -v(j(E))$

Remark 8.2. Several remarks are in order. First of all, since every elliptic curve over a field of characteristic zero can be brought to the form $y^2 = x^3 + Ax + B$, we know that we can always find an elliptic curve such that it has no cycle by Example 7.43. One might wonder if the cycle length found in this particular theorem is not just a coincidence (i.e. can we find an isomorphic elliptic curve with any arbitrary cycle length and thus also with cycle length equal to $-v(j)$?).

Katz, Markwig and Markwig showed that any tropical elliptic curve with a triangulation inducing a cycle must have cycle length equal to $-v(j)$. We can however obtain "elliptic curves" which do not induce a triangulation. This leads to the definition of so-called *faithful representations* of the tropicalisation process (see [BPR11]). These faithful representations require the tropicalisation to map a finite subgraph Γ homeomorphically and isometrically to its image. It can be shown that faithful representations have the correct cycle length. These faithful representations lead to "proper" tropical elliptic curves. The theorem we prove here shows that we can explicitly find an elliptic curve which is faithfully represented by the tropicalisation mapping.

Proof. Let E be an elliptic curve with $v(j) < 0$ over the field $\mathcal{P}$. We can find an isomorphic curve which is minimal according to Lemma 6.8. Then this curve has multiplicative reduction according to Theorem 6.12 . Every elliptic curve can be put in "b_i" form, which amounts to saying that we put it in the following form:

$$y^2 = x^3 + b_2x^2 + b_4x + b_6 \tag{46}$$

This new Weierstrass form has the same discriminant by Lemma 6.3 and it is also minimal. Thus we have that $v(b_i) \geq 0$ for all b_i.
Now take a point P of order 3 on the elliptic curve. Such a point always exists, as was shown in Example 5.11. In fact we can take our point P to reduce to a singular point of $\tilde{E}$ by Theorem 6.15. Suppose that $P = (x_0, y_0)$. Then we can perform a Weierstrass coordinate change ϕ given by

- $x \to x - x_0$
- $y \to y$

such that $P' = \phi(P)$ has coordinates $P' = (0, y_0)$ and such that P' is still of order 3. Note also that $v(y_0) \geq 0$ by Nagell-Lutz. This isomorphic curve is still minimal.
We give a small lemma which shows that this form can be written such that the reduction is immediately apparent.

Lemma 8.3. *Suppose that $P = (0, y_0)$ is a point of order 3 for a Weierstrass equation*

$$y^2 = x^3 + b_2x^2 + b_4x + b_6$$

Then ${b_4}^2 + 4b_2b_6 = 0$ or in other words, the equation can be written as

$$y^2 = x^3 + a(x - b)^2$$

Proof. We check that ${b_4}^2 + 4b_2b_6 = 0$. Let us paraphrase "$P = (0, y_0)$ is a point of order 3" a bit. We know that this is equivalent to $3P = \mathcal{O}$. Such a point P is called a **flex point**. In this case this means that if we take the tangent line through this point, then it must intersect the elliptic curve three times at the point P.
We therefore compute the tangent line at this point. It is given by the equation:

$$(\frac{\partial f}{\partial x}(0), \frac{\partial f}{\partial y}(y_0)) \cdot (x, y - y_0)^T = 0$$

where $y_0 = \sqrt{b_6}$ by virtue of the equation for the elliptic curve. Calculating the partial derivatives yields:

$$b_4x + 2y_0(y - y_0) = 0$$

We can assume that$y_0 \neq 0$ because otherwise we would have a singularity on our curve. We write y in terms of x as:

$$y = \frac{-b_4x + 2{y_0}^2}{2y_0} \Rightarrow y^2 = \frac{b_4^2x^2 - 4{y_0}^2b_4x + 4{y_0}^4}{4{y_0}^2}$$

Equating this to $y^2 = x^3 + b_2x^2 + b_4x + b_6$ yields the following equation for x:

$$x^3 + (b_2 - \frac{{b_4}^2}{4{y_0}^2})x^2 + (b_4 + y_0b_4)x + (b_6 - {y_0}^2)$$

We know that ${y_0}^2 = b_6$. In fact we know that $x = 0$ is a triple root of this equation because we want the tangent line to intersect in $x = 0$ three times. This also means that the coefficient of x^2 is 0. But this means $(b_2 - \frac{{b_4}^2}{4{y_0}^2}) = 0$ which yields the desired result.
The previous quantity is equal to the discriminant of the polynomial $b_2x^2 + b_4x + b_6$ (as can be checked using the high school formula). This means that the discriminant of this polynomial is zero, which means that it has a double root. Consequently we have that for some a and b:

$$y^2 = x^3 + a(x - b)^2$$

as desired. □

Remark 8.4. For our case, we obtain from multiplicative reduction the conditions $v(a) = 0$ and $v(b) > 0$. To see this, note that if $v(a) > 0$ then the reduced curve would be

$$y^2 = x^3$$

which is known as additive reduction, contradicting minimality (because minimal models cannot have additive reduction by Corollary 6.11). Suppose now that $v(b) = 0$. Then the reduced curve would be nonsingular, which contradicts multiplicative reduction.

Using this lemma we can now write our equation in the form

$$y^2 = x^3 + a(x - b)^2 \tag{47}$$

where $v(a) = 0$ and $v(b) > 0$ by Remark 8.4. Now perform the following coordinate change:

- $f = \dfrac{x^2}{y - \sqrt{a}(x - b)}$
- $g = \dfrac{x^2}{y + \sqrt{a}(x - b)}$

This coordinate change is regular except at the points P and $-P$. We can switch to projective space to remedy this problem. In projective space the coordinate change takes the form:

- $x \mapsto \dfrac{x^2}{yz - \sqrt{a}(xz - bz^2)}$
- $y \mapsto \dfrac{x^2}{yz + \sqrt{a}(xz - bz^2)}$

- $z \mapsto \dfrac{zy^2}{x^3 + ax^2z - 2abxz^2 + ab^2z^3}$

Note that on the affine piece defined by $z = 1$ ("piece of affine space in projective space") this indeed gives the previous coordinate change. Our definition of projective morphism now allows us to locally multiply the map by a suitable function h. We need to know exactly what kinds of zeros and poles these functions have.

This is answered as follows: $f = \dfrac{x^2}{y - \sqrt{a}(x-b)}$ has a zero of order 2 at P and a pole of order 1 at $-P$. This can be checked by using divisors (see [Silv09] or [Har77] for an explanation on divisors). Similarly we have that g has a zero of order 2 at $-P$ and a pole of order 1 at P. We want to get rid of these poles locally. This can be done by choosing a function h with a zero at P and then multiplying all the projective coordinates by this function. This makes the function regular at P. Similarly we can make the coordinate change regular at $-P$ by multiplying the coordinates by a function h with a zero at $-P$.

Either way we have that this coordinate change gives a morphism (locally in the affine version) to a yet undetermined variety. Let us first find the inverse of the coordinate change. The coordinate x can be recovered by noticing

$$f \cdot g = x \tag{48}$$

To solve for y, note that $(y - \sqrt{a}(x-b)) \cdot f = x^2$. But we already know x in terms of f and g. We can thus write:

$$y = \frac{x^2}{f} + \sqrt{a}(x-b) = fg^2 + \sqrt{a}(fg - b)$$

Plugging in x and y in the defining equation yields the following equation in terms of f and g:

$$f^2g + 2\sqrt{a}fg + fg^2 + b = 0 \tag{49}$$

Remark 8.5. The maps $f \mapsto f \cdot g$ and $g \mapsto fg^2 + \sqrt{a}(fg - b)$ are polynomials in f and g and thus the inverse coordinate change is also a morphism. Consequently we have that the coordinate change is an isomorphism. This means that the j-invariant is the same for both curves.

Note that we already studied this variety and its tropicalisation in Example 7.39. We have that $v(\sqrt{a}) = 0$ and $v(b) > 0$.

Since the only contributing valuation is the one from the (0,0) coefficient "b", we get a Newton subdivision as in Figure 13. This means that the elliptic curve indeed induces a triangulation with a cycle (due to the (1,1) term). This picture can also be obtained by looking at the (rather simple) tropical polynomial:

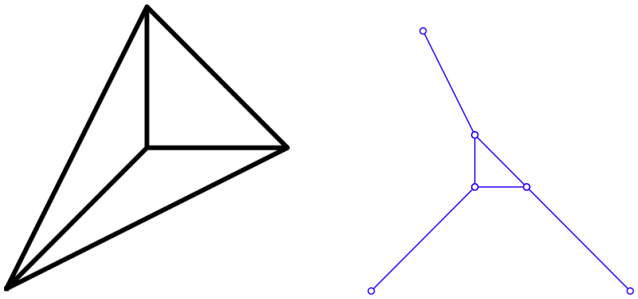


FIGURE 13. The tropical versions of E

$$f = \min\{2x + y, 2y + x, x + y, v(b)\} \tag{50}$$

The corners correspond to the following systems:

- $2x + y = 2y + x = x + y$, or $x = y = 0$
- $2y + x = x + y = v(b)$ or $y = 0$ and $x = v(b)$
- $2x + y = x + y = v(b)$ or $x = 0$ and $y = v(b)$

These corners form a triangle, which incidentally is the cycle we were looking for. Call the two short edges e_1 and e_2. Call the long edge e_3. The two short edges both have length $v(b)$. The long edge has length $\sqrt{2}v(b)$.

In calculating the cycle length we have to compare the Euclidean lengths computed above with the lengths of the corresponding edges in the Newton subdivision. The direction vectors corresponding to these edges (respectively) are:

$$(1, 0), (-1, 0) \text{ and } (1, 1) \tag{51}$$

with lengths 1, 1, and $\sqrt{2}$ respectively. In calculating the cycle length one has to divide the length of the edge in the tropical curve by the corresponding length of the direction vector in the Newton subdivision. One can immediately see that the cycle length will be $3v(b)$.

Now for the j-invariant of the elliptic curve in question. We know that the elliptic curve has multiplicative reduction, so the valuation of the nominator will be zero. So we only need the valuation of the discriminant. We calculate the discriminant of

$$y^2 = x^3 + a(x - b)^2$$

and obtain:

$$\Delta = 884736a^4b^5 + 442368a^4b^4 + 1990656a^3b^4 + 884736a^3b^3 - 746496a^2b^4$$

But $v(a) = 0$ and $v(b) > 0$ so $v(884736a^3b^3) = 3v(b)$ is less than the rest. By Proposition 3.4 this implies that $v(\Delta) = 3v(b)$ and so $v(j) = -3v(b)$. This equals minus the length of the cycle, which concludes our proof.

□

References

[KMM00] E. Katz, H. Markwig, T. Markwig, The j-invariant of a plane tropical cubic, 2008, arXiv:0709.3785

[KMM00-2] E. Katz, H. Markwig, T. Markwig, The tropical j-invariant, 2009, arXiv:0803.4021

[BPR11] M. Baker, S. Payne, J. Rabinoff, Nonarchimedean geometry, tropicalization, and metrics on curves. 2011, arXiv:1104.0320 [math.AG]

[Gat06] A.Gathmann, Tropical Algebraic Geometry, 2006, arXiv:math/0601322v1 [math.AG]

[Stu04] D. Speyer, B. Sturmfels, Tropical Mathematics, arXiv:math/0408099v1 [math.CO], 2004

[Stu03] J. Richter-Gebert, B.Sturmfels, T. Theobald, First Steps in Tropical Geometry, arXiv:math/0306366v2 [math.AG], 2003

[Mum99] D. Mumford, *The Red Book of Varieties and Schemes*, Springer-Verlag, 1999.

[Vol96] H. Volklein, *Groups as Galois Groups, an introduction*. Cambridge University Press, 1996.

[Bo81] N. Bourbaki, *Algebra II*, Springer Verlag, 1981

[Kap00] M.M. Kapranov, Amoebas over non-Archimedian fields, Preprint 2000.

[Kob84] N. Koblitz, *P-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag 1984

[Silv09] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition Springer 2009

[MikTrop09] Ilia Itenberg, Grigory Mikhalkin, Eugenii Shustin, *Tropical Algebraic Geometry*, Second edition, Birkhauser Verlag 2009

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York Inc. 1977

[Stich09] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag Berlin Heidelberg. 2009

[Mat02] J. Matousek, *Lectures on Discrete Geometry*, Springer-Verlag 2002

[Zie95] G.M. Ziegler, *Lectures on Polytopes*, Springer-Verlag 1995

[Ser79] J.P. Serre, *Local Fields*, Springer-Verlag 1979

[Kna92] A.W. Knapp, *Elliptic Curves*, Princeton University Press, 1992.

[Ewa96] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Springer-Verlag 1996.

[Cas91] J.W.S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, 1991.

[Gat03] A.Gathmann, Algebraic Geometry.

[Mik04] Grigory Mikhalkin, Amoebas of Algebraic Varieties and Tropical Geometry, arXiv:math/0403015v1 [math.AG], 2004

[Mik06] Grigory Mikhalkin, Tropical Geometry and its Applications, arXiv:math/0601041v2 [math.AG], 2006

[Mik04-2] Grigory Mikhalkin, Enumerative Tropical Algebraic Geometry in $\mathbb{R}^2$, arXiv:math/0312530v4 [math.AG], 2004