university of groningen

faculty of science
and engineering

mathematics and applied
mathematics

Mordell’s theorem for elliptic curves over rational function fields

Bachelor’s Project Mathematics

July 2019

Student: A. Wouda

First supervisor: Prof. J. Top

Second assessor: Dr. J.S. Müller

Abstract

This thesis considers a generalisation of Mordell's theorem for rational function fields. We prove in an elementary manner that the theorem holds for rational function fields of the form $\mathbb{F}_q(t)$ and we look at where and how the proof needs to be adjusted when we want to consider other rational function fields. We briefly look into some mathematical objects occurring in the proof and we end with the computation of the rank of an elliptic curve over a rational function field.

Contents

1 Introduction

An important branch of number theory is that which studies Diophantine equations. The old Greeks already studied these kind of equations; they are named after the Greek mathematician Diophantus who lived around 200 AD. The theory of Diophantine equations studies the solutions of polynomial equations in either the integers or the rationals. A famous example of such an equation is Fermat's equation

$$X^n + Y^n = Z^n.$$

Fermat asserted in the seventeenth century that such an equation does not have any rational solutions, except the trivial ones, for $n \geqslant 3$. It took 350 years before for someone, Andrew Wiles, was able to find a proof of the theorem. Fermat's last theorem is a great example of how complex the study of Diophantine equations can be. An important tool in the study of Diophantine equations are elliptic curves, they were also used extensively by Wiles in his proof of Fermat's last theorem. An elliptic curve is a curve defined by an equation of the form

$$y^2 = x^3 + ax^2 + bx + c,$$

where a, b, c are elements of some field K with $\operatorname{char}(K) \neq 2$ and where $f(x) := x^3 + ax^2 + bx + c$ does not have any multiple roots.

Elliptic curves turn out to have a lot more structure than one would imagine when just eyeballing the equation that defines them. In fact, the points on an elliptic curve over a field form an abelian group. Most mathematics students are probably familiar with this fact, but again, the group law on those points is not at all that obvious and its construction is completely geometric. Probably even less obvious is the fact that in the case where $K = \mathbb{Q}$, the rational points on an elliptic curve are not only an abelian group, but are in fact finitely generated. This result is due to Mordell who proved it in the beginning of the 20-th century [1]. Mordell's theorem turns out to hold in more generality, as was proved some years later by Weil, Néron and Lang. In particular, the theorem holds for rational function fields which are finitely generated over their prime fields. The main goal of this thesis is to give a proof of this statement for a specific case in an elementary way, that is, using a *height function* and assuming there is a point of order 2 on the curve. We will also discuss where it goes wrong in the more general case.

2 Preliminaries

2.1 Group law on elliptic curves

As mentioned, one can define a group law on the points on an elliptic curve over some field K. It should first be mentioned that we are not considering curves in an affine plane, like the Euclidean plane. Instead, we are considering them in the projective plane, which has some extra points 'at infinity'. One of these points, denoted by O, is on our elliptic curve. This point will play the role of the identity element in the group. Adding these points at infinity has some practical reasons, an important one being that equality holds in Bézout's theorem. This theorem then tells us that the number of intersection points of two curves, which do not have shared components, is the product of their degrees. Hence the number of intersection points of a line with an elliptic curve is equal to 3. This is important as the group law on an elliptic curve is defined using the intersection points of a line and the elliptic curve.

The group law on an elliptic curve is defined as follows; given two points P and Q on the elliptic curve, the point $P + Q := (x, -y)$ is the point where x and y are such that (x, y) is the third intersection point of the line through P and Q and the curve. Hence we obtain $P + Q$ by mirroring the third intersection point of the line through P and Q and the cubic, in the x-axis. In the picture below one can see what the (geometric) process is of finding the point $P + Q$. Note that there are some cases that are a bit different. For example, the third intersection point may be the point at infinity O. In that case we have that $P + Q = O$. Also, if we add the point P to itself, we use the line that is tangent to the curve at that point P to find the third intersection point.

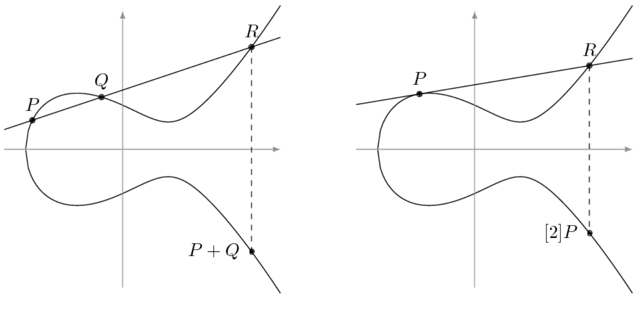

Figure 1: Group law on an elliptic curve

Inverses can be written down explicitly in a simple way; given a point $P = (x, y)$ on the curve, its inverse $-P$ has coordinates $(x, -y)$ as the line going through both these points only meets the curve at O, the identity element. Using this fact it is also easy to see that points $P = (x, y)$ on the curve that have order two, all satisfy $y = 0$, since $P = -P$.

Doing some quite straightforward, but not very pleasant, calculations using the equations for lines through a point and tangent lines, one can find the explicit formulas for the group law. The computations will not be done here as such, but explicit calculations are given in [2]. The formulas for the group law that come out of these computations are as follows; let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $x_1 \neq x_2$, be points on the curve given by the equation $y^2 = x^3 + ax^2 + bx + c$ and denote $P_1 + P_2 = (x_3, -y_3)$. The points x_3 and y_3 are then as follows

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2 \quad \text{and} \quad y_3 = \frac{y_2 - y_1}{x_2 - x_1} x_3 + v, \tag{1}$$

here v is given by

$$v = y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1 = y_2 - \frac{y_2 - y_1}{x_2 - x_1} x_2.$$

Note that the case where $x_1 = x_2$ but the points are distinct corresponds to the case where $P_1 + P_2 = O$. We can also construct an explicit formula for the case where we want to add a point $P = (x, y)$ to itself. This formula, which gives the x-coordinate of $2P = (x', y')$ is called the duplication formula

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{2}$$

These formulas can be used when it is necessary to do explicit computations with points on an elliptic curve.

2.2 Mordell's theorem

Formally, Mordells theorem can be stated as follows.

Theorem 1 (Mordell's theorem)**.** *Let E be an elliptic curve given by an equation*

$$E : y^2 = x^3 + ax^2 + bx + c,$$

where a, b and c are integers. Then the group of rational points on the curve, $E(\mathbb{Q})$, is a finitely generated abelian group.

The most elementary proof of this theorem uses the fact that the index of $2E(\mathbb{Q})$ is finite in $E(\mathbb{Q})$ and that a so called *height function h* exists, which maps $E(\mathbb{Q})$ to $[0, \infty)$ and satisfies some additional properties. The fact that the given index is finite is however no triviality and turns out to be the most difficult part of the proof of Mordell's theorem. In fact, if one wants to prove this finiteness in general, using some algebraic number theory is inevitable. This is why most books that try to steer clear from some more advanced algebra prove this theorem while assuming that there is at least one point of order two on the curve. This is also what will be done in this thesis. The theorem that states that these properties of the rational points on the curve imply that the group they form is finitely generated uses a kind of descent argument. The statement of this theorem and a proof of it will be given in the next subsection.

The fact that there is a point of order 2 on the curve, gives that the curve can be translated in a way such that this point is the origin. The rational points on this new curve are in one-to-one correspondence with the rational points on the original curve, however this new curve has a simpler equation defining it. After some arithmetic with this simpler curve, one is then able to show that the index of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$ is finite.

Another important part of the proof is the introduction of a suitable height function on $E(\mathbb{Q})$. The height function that is used on $\mathbb{Q}$ most often is defined as follows

$$h\left(\frac{m}{n}\right) := \log\max\{|m|, |n|\},$$

where $m/n \in \mathbb{Q}$ is written in lowest terms, i.e. $\gcd(m, n) = 1$. If $P = (x, y)$ is a point in $E(\mathbb{Q})$, then we define: $h(P) := h(x)$. This function on $E(\mathbb{Q})$ turns out to satisfy all properties required by the descent argument.

2.3 Descent Theorem

The theorem used for the proof that the group of rational points on an elliptic curve is finitely generated is stated below. It is worth noting that this theorem itself does not concern elliptic curves, but holds in more generality for abelian groups.

Theorem 2 (Descent). *Let Γ be an abelian group, and suppose that there exists a function*

$$h : \Gamma \to [0, \infty)$$

with the following three properties:

(i) *For every real number M, the set $\{P \in \Gamma : h(P) \leqslant M\}$ is finite.*

(ii) *For every $P_0 \in \Gamma$ there is a constant κ_0 such that*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0$$

for all $P \in \Gamma$.

(iii) *There is a constant κ such that*

$$h(2P) \geqslant 4h(P) - \kappa$$

for all $P \in \Gamma$.

Suppose further that $[\Gamma : 2\Gamma] < \infty$.
Then Γ is finitely generated.

Proof. As the index of 2Γ is finite in Γ, there are finitely many representatives $Q_1, \ldots, Q_n$ for the cosets of 2Γ in Γ. Let $P \in \Gamma$, since P must be in one of the cosets we can write $P = Q_{i_1} + 2P_1$ for some $P_1 \in \Gamma$ and Q_{i_1} the representative of some coset. The same thing can be done for P_1, so we can write $P_1 = Q_{i_2} + 2P_2$. Continuing inductively we have the following

$$\begin{aligned} P_1 &= Q_{i_2} + 2P_2 \\ P_2 &= Q_{i_3} + 2P_3 \\ &\vdots \\ P_{m-1} &= Q_{i_m} + 2P_m. \end{aligned}$$

We have now constructed a sequence of elements P_i in the group Γ. Substituting these P_i into the expression for P eventually gives

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Using the assumptions (ii) and (iii) we will say something useful about the height of a point P_i. First we look at (ii) with $P_0 = -Q_i$, we then get a constant κ_i such that

$$h(P - Q_i) \leqslant 2h(P) + \kappa_i \quad \text{for all } P \in \Gamma.$$

Since there are only finitely many Q_i's, we can take the maximum of all κ_i's, denoted by κ', to obtain the following

$$h(P - Q_i) \leqslant 2h(P) + \kappa' \quad \text{for all } P \in \Gamma \text{ and all } 1 \leqslant i \leqslant n.$$

Next we use the third assumption (iii) and the constant κ that comes from it to obtain the following inequality

$$\begin{aligned} h(P_j) &\leqslant \frac{1}{4}h(2P_j) + \frac{1}{4}\kappa \\ &= \frac{1}{4}h(P_{j-1}) + \frac{1}{4}\kappa \\ &\leqslant \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4}. \end{aligned}$$

Suppose that $h(P_{j-1}) \geqslant \kappa' + \kappa$, then by the above inequality we have that

$$h(P_j) \leqslant 3/4\, h(P_{j-1}).$$

So as long as P_{j-1} is greater than or equal to $\kappa' + \kappa$, we have a sequence of P_i's with height going to zero. This means that there should exist some index m such that $h(P_m) \leqslant \kappa' + \kappa$. So if we take m large enough, we can write for any $P \in \Gamma$

$$P = \alpha_1 Q_1 + \alpha_2 Q_2 + \cdots + \alpha_n Q_n + 2^m R,$$

where $\alpha_1, \ldots, \alpha_n$ are integers and R is some element in Γ with $h(R) \leqslant \kappa' + \kappa$. This means that the set

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leqslant \kappa' + \kappa\}$$

generates Γ. The left set is finite since there are finitely many cosets of 2Γ in Γ and the right is finite by the first property (i), hence we conclude that Γ is finitely generated.

□

3 Generalisation of Mordell's theorem

As mentioned, Mordell's theorem holds in more generality [3]. In this thesis we will look at the elementary proof for Mordell's theorem, i.e. using the descent argument from the previous theorem and the assumption that there is a point of order 2 on the curve, and try to extend it to (some) rational function fields $K(t)$ with $\text{char}(K) \neq 2$. This field $K(t)$ is the field of fractions of the principal ideal domain $K[t]$, which consists of polynomials with coefficients in the field K. Hence elements of the field $K(t)$ can be written as quotients of polynomials with coefficients in K.

Throughout this thesis we will be considering the curve E given by the equation

$$E : y^2 = x^3 + ax^2 + bx + c,$$

where a, b and c are elements of $K[t]$ and $\Delta(f(x)) \neq 0$, i.e. the discriminant of $f(x)$ is nonzero, with $f(x) = x^3 + ax^2 + bx + c$. When we write $E(K(t))$, we are talking about the $K(t)$-rational points on the curve E, i.e. points (x, y) where x and y are in $K(t)$ and satisfy the equation for E.

The analogue of Mordell's theorem for rational function fields $K(t)$ is not true for any field K. For example, if we consider an elliptic curve over the rational function field $\mathbb{C}(t)$, the $\mathbb{C}(t)$-rational points are not finitely generated in general; consider for example a curve E over $\mathbb{C}$. Then $E(\mathbb{C}) \subset E(\mathbb{C}(t))$, but $E(\mathbb{C})$ is clearly not finitely generated as it is an uncountable set and since $E(\mathbb{C}(t))$ is at least as 'large', it is not finitely generated either. We will go through the same steps as the proof for $\mathbb{Q}$ does, but instead considering $K(t)$. This proof will of course not work for general K so when necessary we will mention what adjustments need to be made to K to make the proof work.

We will proceed in approximately two steps, following the same procedure as in [2]. The first step is concerned with finding an appropriate height function h on the $K(t)$-rational points on the curve and proving it satisfies the necessary conditions. The height function that is used a lot on $\mathbb{Q}$ is defined using the absolute value of a number in $\mathbb{Z}$, hence it makes sense to do a similar thing for a rational function field $K(t)$. The second and more difficult part of the proof is concerned with proving the finiteness of the index of the group $2E(K(t))$ in the group $E(K(t))$.

After this we will look in more detail into some parts on the proof and do an example of a calculation of the rank using information gained from the proof.

4 Height

4.1 Height function on $E(K(t))$

The height function generally used on $\mathbb{Q}$ is defined using the absolute value, so it makes sense to do a similar thing for a rational function field $K(t)$. Hence we will want to define an absolute value on $K[t]$, that is, a function $|\cdot|$ from $K[t]$ to the non-negative reals with the following properties

(i) $|f| \geqslant 0$ for all f in $K[t]$;

(ii) $|f| = 0$ if and only if $f = 0$;

(iii) $|fg| = |f||g|$ for all f, g in $K[t]$;

(iv) $|f + g| \leqslant |f| + |g|$ for all f, g in $K[t]$.

Note that a function that satisfies these properties is for example the function $|f| := e^{\deg(f)}$, if we set $\deg(0) = -\infty$. If we are working with $\mathbb{F}_q[t]$ we may also use $|f| := q^{\deg(f)}$. These absolute values actually satisfy a stronger version of the triangle inequality, since $\deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}$, for any f, g in $K[t]$ and hence

$$|f + g| = e^{\deg(f+g)} \leqslant \max\{e^{\deg(f)}, e^{\deg(g)}\} = \max\{|f|, |g|\},$$

for all f, g in $K[t]$. This absolute value will be used to define the height in a similar way to the height defined on $\mathbb{Q}$.

Definition 4.1. Let $x(t) = f(t)/g(t) \in K(t)$ be written in lowest terms. The function h, called the height function, is a function from $K(t)$ to $[0, \infty)$, such that $h(x(t)) = \max\{\deg(f(t)), \deg(g(t))\}$.

Using the absolute value as before, we note that this height is defined analagously to the definition of height we gave on $\mathbb{Q}$ since

$$h\left(\frac{f}{g}\right) := \max\{\deg(f), \deg(g)\} = \max\{\log(|f|), \log(|g|)\} = \log \max\{|f|, |g|\}.$$

This function h is the height function that will be used on $K(t)$. Next we define a height on the points on our curve, we do this in the same way as is done for $E(\mathbb{Q})$.

Definition 4.2. Let $P = (x, y)$ be a point on the given curve. The height of a point on the curve is defined as the height of its first coordinate: $h(P) := h(x)$. The height of the point at infinity is defined as $h(O) := 0$.

In the upcoming sections, we will prove that in some cases this height function satisfies the three conditions needed for the descent argument. We will do this in as much generality as is possible, so using a general rational function field $K(t)$. However whether these conditions hold, depends a lot on the domain of the height function h, therefore it will at some points be necessary to make a more specific choice for the field K.

4.2 Finiteness property

As mentioned we will prove the needed properties of the height in several steps. The first property that will be proved is the finiteness property. However, this property does not hold for a general rational function field $K(t)$, we will elaborate on this later. The version we are going to prove is stated as a lemma below.

Lemma 1. *For every real number M, the set $\{P \in E(\mathbb{F}_q(t)) : h(P) \leqslant M\}$ is finite.*

Proof. We will first prove that there are only finitely many possibilities for the x-coordinate of the point P on the curve when we are given that its height is bounded by some real number M. Since, given an x-coordinate, there are at most two possibilities for the y-coordinate, we will then be able to conclude that also there are finitely many points (x, y) on the curve.

We will first show that for all real numbers M

$$\{x \in \mathbb{F}_q(t) : h(x(t)) \leqslant M\} < \infty.$$

Since the set consisting of the x-coordinates of $\mathbb{F}_q(t)$-rational points on the curve is a subset of $\mathbb{F}_q(t)$, we have then proven the lemma.

We fix $M \in \mathbb{R}$ and let $x \in \mathbb{F}_q(t)$ be such that $h(x) \leqslant M$. If x is written in lowest terms as $x(t) = f(t)/g(t)$, that means that both $\deg(f) \leqslant M$ and $\deg(g) \leqslant M$. However, all the coefficients of both polynomials lie in the finite field $\mathbb{F}_q$, meaning that each of the coefficients can take one of q values, except the leading coefficient, which can have one of the $q - 1$ nonzero values. Therefore there are precisely $(q-1)q^d$ distinct polynomials of degree d in $\mathbb{F}_q[t]$. This implies that the number of polynomials in $\mathbb{F}_q[t]$ with degree lower than or equal to d is equal to

$$\sum_{i=0}^{d} (q-1)q^i,$$

hence there are that many different possibilities for both polynomials f and g. Since x is the quotient of these polynomials, written in lowest terms, there are at most

$$\left(\sum_{i=0}^{d}(q-1)q^{i}\right)^{2}$$

distinct possibilities for x (some terms may not be coprime). This proves that for all real numbers M the set of elements $x \in \mathbb{F}_q(t)$ with $h(x) \leqslant M$ is finite, proving the lemma. □

From this proof it is obvious where it goes wrong when considering a general rational function field $K(t)$. If we fix any degree d and consider polynomials with coefficients in K of degree d, then in general there are infinitely many of those polynomials. This changes only if K is a finite field, i.e. of the form $K = \mathbb{F}_q$. Hence the set that is being considered is not finite in general if we consider $K(t)$ with K a field with infinitely many elements.

As is the case in the proof of Mordell's theorem, this property of the height is the easiest to prove, when considering the rational function field $\mathbb{F}_q(t)$. The other properties will be proved in the upcoming two sections.

4.3 Upper bound when adding points

In this section the second property of the height function h will be proved. Before stating the property as a lemma and proving the lemma, we first note two things about the points on our curve in the upcoming two propositions.

Proposition 1. *If $P = (x, y)$ is a point on the curve E with $x, y \in K(t)$, then x and y have the form*

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3},$$

where $m, n, e \in K[t]$ and $\gcd(m, e) = \gcd(n, e) = 1$.

Proof. First suppose that we write

$$x = \frac{m'}{M} \quad \text{and} \quad y = \frac{n'}{N},$$

in lowest terms. If we can show that $N^2 = uM^3$, where u is a unit, we can define $e = N/M$ and get

$$e^2 = \frac{N^2}{M^2} = \frac{uM^3}{M^2} = uM \quad \text{and} \quad e^3 = \frac{N^3}{M^3} = \frac{N^3}{u^{-1}N^2} = uN.$$

If we then define

$$m := um' \quad \text{and} \quad n := un',$$

we have the expression for x and y that we wanted. So if we show that $N^2 = uM^3$ where M and N are as defined above, we have proven the proposition. We will prove this by showing that both $N^2|M^3$ and $M^3|N^2$, for notational reasons, we will write m and n instead of m' and n'.

First note that substituting x and y into the equation of the curve gives the following relation between m, n, M and N

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

and clearing the denominators gives another equation

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

- Since N^2 occurs in every term on the right-hand side of the equation, we have that $N^2|M^3n^2$. However, we assumed that x and y were written in lowest terms, so $\gcd(n, N) = 1$. Then also $\gcd(n, N^2) = 1$ and we must have that $N^2|M^3$.
- First we note that M divides M^3n^2 and hence it must divide the right side of the equation. Also, since M occurs in the last three terms on the right-hand side, it divides those. These two facts together give us that M must divide N^2m^3. However, $\gcd(M, m) = 1$ by assumption, so we must have that $M|N^2$. By the same reasoning as before this immediately gives us that $M^2|N^2m^3$, so $M|N$. Again using the same reasoning, i.e. $M^3|M^3n^2$ and M^3 divides the last three terms of the equation on the right, we obtain that $M^3|N^2m^3$ so in fact $M^3|N^2$.

By the argument made above, we have now shown that the coordinates x and y can indeed be written as in the proposition. □

This is the first result that will be needed to prove the second property of the height. Note that we hardly need anything else than the fact that the points are on the curve and that there is a unique factorisation in $K[t]$, so this statement really holds for any $K(t)$-rational points. There is one more result that will be needed, which is stated in the next proposition.

Proposition 2. *Let $P = (m/e^2, n/e^3)$ be a point on the curve E, with $m, n, e \in K[t]$ and $\gcd(m, e) = \gcd(n, e) = 1$, then*

$$\deg n \leqslant k + 3/2\, h(P),$$

for some constant k depending on a, b and c.

Proof. We first note that the degree has the following properties: the first is that

$$\deg(fg) = \deg(f) + \deg(g), \text{ for } f, g \in K[t],$$

which holds since f and g are polynomials with coefficients in a field, so there are no zero divisors and multiplying the leading terms will hence never yield zero. The second is that

$$\deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}, \text{ for } f, g \in K[t].$$

Next we note that both $\deg(e^2) \leqslant h(P)$ and $\deg(m) \leqslant h(P)$, so in particular $\deg(e) \leqslant 1/2\ h(P)$. We will use these inequalities to give an upper bound to $\deg(n^2)$.

We know that m/e^2 and n/e^3 satisfy the equation for the curve, substituting them in the equation and clearing the denominators gives

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6,$$

which can be used to obtain the following (in)equalities

$$\begin{aligned}
\deg(n^2) &= \deg(m^3 + ae^2m^2 + be^4m + ce^6)\\
&\leqslant \max\{\deg(m^3), \deg(ae^2m^2), \deg(be^4m), \deg(ce^6)\}\\
&= \max\{3\deg(m), \deg(a) + 2\deg(e) + 2\deg(m), \deg(b) + 4\deg(e) + \deg(m),\\
&\quad \deg(c) + 6\deg(e)\}\\
&\leqslant \max\{3h(P), \deg(a) + 3h(P), \deg(b) + 3h(P), \deg(c) + 3h(P)\}\\
&= \max\{\deg(a), \deg(b), \deg(c)\} + 3h(P).
\end{aligned}$$

We now define $k := 1/2\ \max\{\deg(a), \deg(b), \deg(c)\}$. Then we obtain that

$$\deg(n) = 1/2 \deg(n^2) \leqslant k + 3/2h(P).$$

This proves the proposition. □

We have now proven the two results with which we will be able to prove the second property of the height function. Again, the previous proposition holds in general for a rational function field $K(t)$. The next lemma states that the chosen height function h satisfies the second condition that is needed for the descent argument.

Lemma 2. *If we fix $P_0 \in E(K(t))$, then there exists a constant κ_0, depending only on P_0, a, b and c, such that*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0 \quad \text{for all } P \in E(K(t)).$$

Proof. The proof of this lemma is quite straightforward when using the formulas for the group law. Note that we can exclude any finite set S of points P when proving this, since we can then just take $\kappa_0 = \max_{P \in S} h(P + P_0)$. We can therefore consider $P \notin \{O, P_0, -P_0\}$, this way we can also avoid using the duplication formula. We can also consider $P_0 \neq O$, since the inequality is trivial for all P in that case.

We write $P = (x, y)$ and $P + P_0 = (\xi, \eta)$. We need to calculate $h(P) = h(\xi)$, preferably in terms of $h(P) = h(x)$. The formulas of the group law give us a relation between x and ξ in the following way

$$\xi = \lambda^2 - x - x_0 - a \quad \text{where} \quad \lambda = \frac{y - y_0}{x - x_0}.$$

Substituting the value for λ in the equation for ξ and bringing everything together over one denominator gives

$$\xi = \frac{(-2y_0)y + (2a - x_0)x^2 + (b - 2ax_0 - x_0^2)x + (c + y_0^2 + ax_0^2 + x_0^3)}{x^2 - 2x_0x + x_0^2}.$$

Picking elements A, B, C, D, E, F, G in $K(t)$ depending on $x_0(t), y_0(t), a(t), b(t)$ and $c(t)$ in the proper way, makes that we can write ξ as a quotient of two polynomials in x with coefficients in $K(t)$. We may in fact assume that these coefficients lie in $K[t]$, because we can multiply out the least common multiple of the denominators of the coefficients. We then have

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Dx + G},$$

with $A, B, C, D, E, F, G \in K[t]$. Since we may write $x = m/e^2$ and $y = n/e^3$, we can substitute this into our new expression for ξ and make ξ a quotient of polynomials in $K[t]$

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Note that this expression for ξ may not be written in lowest terms, but in any case we can bound the height of ξ like this

$$h(\xi) \leqslant \max\{\deg(Ane + Bm^2 + Cme^2 + De^4), \deg(Em^2 + Fme^2 + Ge^4)\}.$$

We can now make two case distinctions, the first one is when this maximum equals $\deg(Ane + Bm^2 + Cme^2 + De^4)$ and the second one is when it equals $\deg(Em^2 + Fme^2 + Ge^4)$. In the first case we have the following (in)equalities

$$\begin{aligned}
h(\xi) &\leqslant \deg(Ane + Bm^2 + Cme^2 + De^4) \\
&\leqslant \max\{\deg(Ane), \deg(Bm^2), \deg(Cme^2), \deg(De^4)\} \\
&= \max\{\deg(A) + \deg(ne), \deg(B) + \deg(m^2), \deg(C) + \deg(me^2), \deg(D) + \deg(e^4)\} \\
&\leqslant \max\{\deg(A) + k + 2h(P), \deg(B) + 2h(P), \deg(C) + 2h(P), \deg(D) + 2h(P)\} \\
&= \max\{\deg(A) + k, \deg(B), \deg(C), \deg(D)\} + 2h(P).
\end{aligned}$$

In the second case, we find a similar inequality

$$\begin{aligned}
h(\xi) &\leqslant \deg(Em^2 + Fme^2 + Ge^4) \\
&\leqslant \max\{\deg(Em^2), \deg(Fme^2), \deg(Ge^4)\} \\
&= \max\{\deg(E) + \deg(m^2), \deg(F) + \deg(me^2), \deg(G) + \deg(e^4)\} \\
&\leqslant \max\{\deg(E) + 2h(P), \deg(F) + 2h(P), \deg(G) + 2h(P)\} \\
&= \max\{\deg(E), \deg(F), \deg(G)\} + 2h(P).
\end{aligned}$$

Clearly in both cases we can find a constant so that we can bound $h(\xi)$ in the way we want. If we define

$$\kappa_0 := \max\{\deg(A) + k, \deg(B), \deg(C), \deg(D), \deg(E), \deg(F), \deg(G)\},$$

we have proven the lemma. □

We conclude that this height function h also has the second property that is needed for the descent theorem. In contrast to the finiteness property, this property holds when h is defined on any rational function field $K(t)$. In the next section we will treat the third and final property.

4.4 Lower bound when doubling a point

The proof of this property uses the result of another slightly more general lemma. This lemma says something about how the height of an element changes when a function is applied to it, as we will see shortly this is precisely what we are interested in. We first state the final property as a lemma and then introduce the other lemma that will prove the first one. The proof of the second lemma is very similar to the proof that is given in [4].

Lemma 3. *There is a constant κ depending on a, b and c, such that*

$$h(2P) \geqslant 4h(P) - \kappa \quad \text{for all } P \in E(K(t)).$$

Proof. We first say something about the relation between the x-coordinate of P and the x-coordinate of $2P$. We write $P = (x, y)$ and $2P = (\xi, \eta)$. Note that again we may disregard a finite set of points P, since for this set S we can just take $\kappa = 4 \max_{P \in S} h(P)$. Hence we are allowed to not look at the points P that have order 1 or order 2, which is what we will do. By the duplication formula, we find that

$$\xi = \lambda^2 - 2x - a \quad \text{and} \quad \lambda = \frac{f'(x)}{2y}.$$

Putting this under a common denominator and substituting the equation for $f(x)$ we obtain

$$\begin{aligned}\xi &= \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} \\ &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}.\end{aligned}$$

This shows us that we may write ξ as the quotient of polynomials in x with coefficients in $K(t)$. Since the curve is non-singular by assumption, $f(x)$ and y are not simultaneously zero and hence the polynomial (in x) in the denominator and the polynomial (in x) in the numerator do not have common roots, i.e. their greatest common divisor is equal to 1 in $K(t)[X]$.

One might think that this relation already tells us something about the height of ξ, and it does. However, it only gives us an upper bound for the height of ξ, since we do not know how much 'cancellation' will happen. This is not good enough for the lemma we want to prove, for that proof we will need the result from the lemma stated below.

For notational reasons it is nice to introduce another height function H. Recall that we defined the absolute value on an element from $K[t]$ in the following way

$$|f(t)| := e^{\deg(f(t))} \quad \text{for all } f(t) \in K[t].$$

In the case where K is a finite field $\mathbb{F}_q$ we use q instead of the exponential. We define the absolute value on $K(t)$ as follows

$$\left|\frac{f(t)}{g(t)}\right| := \frac{|f(t)|}{|g(t)|} \quad \text{for all } \frac{f(t)}{g(t)} \in K(t) \text{ written in lowest terms.}$$

We now also define a function $H : K(t) \to [0, \infty)$ by $H(x) = e^{h(x)}$ (or q instead of e when we are considering a finite field). Note that we can also write this as $H(f/g) = \max\{|f|, |g|\}$.

Lemma 4. *Let $\phi(X)$ and $\psi(X)$ be coprime in $K(t)[X]$ and let $d = \max\{\deg(\phi), \deg(\psi)\}$. Then there exists a positive constant C such that*

$$CH(x)^d \leqslant H\left(\frac{\phi(x)}{\psi(x)}\right) \quad \textit{for all } x \in K(t).$$

Proof. Because we are mainly interested in the quotient of the polynomials ϕ and ψ, we can assume that they have coefficients in $K[t]$. This is the case because we can multiply the numerator and denominator by the least common multiple of the denominators of all coefficients, yielding the same fraction, only now the polynomials occuring in it have coefficients in $K[t]$. Hence we will assume $\phi(X), \psi(X) \in K[t][X]$. We define two values

$$\Phi(m,n) := n^d \phi\left(\frac{m}{n}\right),$$
$$\Psi(m,n) := n^d \psi\left(\frac{m}{n}\right),$$

for $m/n \in K(t)$ written in lowest terms.

Without loss of generality we assume that $\deg(\phi) \leqslant \deg(\psi)$. Since the polynomials are coprime in $K(t)[X]$, we can invert $\psi \pmod{\phi}$ in the ring $K(t)[X]/(\phi)$. This means that there exist polynomials $F(X), G(X)$ in $K(t)[X]$ such that

$$F(X)\phi(X) + G(X)\psi(X) = 1. \tag{$\clubsuit$}$$

Next we pick $A \in K[t]$ 'large' enough such that both $AF(X), AG(X) \in K[t]$. We define $F_2(X) := AF(X)$ and $G_2(X) = AG(X)$. We then have

$$F_2(X)\phi(X) + G_2(X)\psi(X) = A. \tag{$\spadesuit$}$$

Now we pick $m/n \in K(t)$ where m and n are coprime and evaluate ($\spadesuit$) in m/n and multiply both sides by n^{2d-1} to obtain

$$\left[n^{d-1}F_2\left(\frac{m}{n}\right)\right]\Phi(m,n) + \left[n^{d-1}G_2\left(\frac{m}{n}\right)\right]\Psi(m,n) = n^{2d-1}A. \tag{$\heartsuit$}$$

First note that the part of $\gcd(\Phi, \Psi)$ that is coprime to n, has to divide A because $n^{2d-1}A$ can be written as a $K[t]$-linear combination of Φ and Ψ.

Next we will consider the absolute value of both sides of this expression. First note that

$$|n|^{d-1} \leqslant H(m/n)^{d-1}.$$

We define $C := \max\{|F_2(m/n)|, |G_2(m/n)|\}$. Now taking the absolute value on both sides of (3) and using the fact that this absolute value is multiplicative and satisfies the strong triangle inequality we see that

$$|n|^{2d-1}|A| \leqslant \max\{|\Phi(m,n)|, |\Psi(m,n)|\} C H \left(\frac{m}{n}\right)^{d-1}.$$

Rewriting this and defining $S = |A|/C$ gives the following inequality

$$\max\{|\Phi|, |\Psi|\} \geqslant S\,|n|^{2d-1}/\,H(m/n)^{d-1}. \tag{◆}$$

We will now do almost the same thing for two other polynomials ϕ^* and ψ^* and obtain similar inequalities. With these we will be able to bound the height of $\phi(x)/\psi(x)$ in the way we want. We define ϕ^* and ψ^* by

$$\phi^*(X) := X^d\,\phi(1/X) \quad \text{and} \quad \psi^*(X) := X^d\,\psi(1/X).$$

Note that ϕ^* and ψ^* are coprime as well. It is quite easy to see, by simply writing out the expression for the polynomials, that

$$m^d\phi^*\left(\frac{m}{n}\right) = \Phi(m,n) \quad \text{and} \quad m^d\psi^*\left(\frac{m}{n}\right) = \Psi(m,n).$$

By the same reasoning as before, we can find $F^*(X), G^*(X) \in K(t)[X]$ such that

$$F^*(X)\phi^*X + G^*(X)\psi^*(X) = 1. \tag{♧}$$

And again we can find an element $A^* \in K[t]$ such that $A^*F(X)$ and $A^*G(X)$ have coefficients in $K[t]$. Defining $F_2^*(X) := A^*F^*(X)$ and $G_2^*(X) := A^*G^*(X)$ we obtain an equation with elements in $K[t][X]$

$$F_2^*(X)\phi^*(X) + G_2^*(X)\psi^*(X) = A^*. \tag{♤}$$

Now we evaluate (♤) in $n/m \in K(t)$, where m and n are as before, and multiply both sides of the equation by m^{2d-1} to obtain

$$\left[m^{d-1}F_2^*\left(\frac{n}{m}\right)\right]\Phi(m,n) + \left[m^{d-1}G_2^*\left(\frac{n}{m}\right)\right]\Psi(m,n) = m^{2d-1}A^*. \tag{♡}$$

Note that the part of $\gcd(\Phi(m,n), \Psi(m,n))$ that is coprime to m has to divide A^*. If we see the similarity between (♥) and (♡) and define $C^* := \max\{F_2^*(n/m), G_2^*(n/m)\}$, we can immediately see

$$|m|^{2d-1}|A^*| \leqslant \max\{|\Phi(m,n)|, |\Psi(m,n)|\} C^* H \left(\frac{m}{n}\right)^{d-1}.$$

If we define, analagously to S, $S^* := |A^*|/C^*$ we obtain

$$\max\{|\Phi|, |\Psi|\} \geqslant S^*|m|^{2d-1}/\, H(m/n)^{d-1}. \tag{$\Diamond$}$$

We are now very close to the completion of the proof of the lemma. We mentioned that the part of $\gcd(\Phi(m,n), \Psi(m,n))$ that is coprime to n divides A and the part that is coprime to m divides A^*. Since m and n are coprime as well, this means that $\gcd(\Phi(m,n), \Psi(m,n))$ divides AA^*. In particular this means that the degree of $\gcd(\Phi(m,n), \Psi(m,n))$ is less than or equal to the degree of AA^*, so also

$$|\gcd(\Phi(m,n), \Psi(m,n))| \leqslant |AA^*|.$$

Note that $H(x)$ is either $|m|$ or $|n|$. Using this and ($\blacklozenge$) and ($\Diamond$) we obtain

$$H\left(\frac{f(x)}{g(x)}\right) = H\left(\frac{\Phi(m,n)}{\Psi(m,n)}\right) = \frac{\max\{|\Phi|, |\Psi|\}}{|\gcd(\Phi, \Psi)|} \geqslant \frac{\min\{S, S^*\}}{|AA^*|} H(x)^d,$$

for all $x = m/n \in K(t)$. This finishes the proof of the lemma.

□

As mentioned the result of this lemma is going to help us prove the original lemma. We want

$$h(\xi) \geqslant 4h(x) - \kappa,$$

where κ is some constant. Since ξ can be written as the quotient of a degree 4 and a degree 3 polynomial, which are coprime, we can apply the previous lemma. So we obtain

$$CH(x)^4 \leqslant H(\xi).$$

Taking the logarithm on both sides of the equation gives us precisely what we are looking for, proving Lemma 3.

□

Like Lemma 2, this lemma also holds for general $K(t)$. We have now treated all three properties the height needs to satisfy for the descent argument, in the next section we will treat the finiteness of the index of the group $2E(K(t))$ in the group $E(K(t))$.

5 Finiteness of the index $[E(K(t)) : 2E(K(t))]$

In the upcoming part we will prove the finiteness of the index $[E(K(t)) : 2E(K(t))]$, for certain K. Out of all four conditions needed for the descent argument, this is by far the hardest to prove to be satisfied. It is a similar to a theorem that is known as the *weak Mordell-Weil theorem*, this theorem states that $[E(K) : mE(K)]$ is finite for any positive integer m where K is a number field. The proof of this theorem requires knowledge of Galois cohomology, which we will not dive into. In this section we will prove the case where $m = 2$, under the additional assumption that there is at least one $K(t)$-rational point of order 2 on the curve. We will first outline some important parts of the proof.

1. The existence of the point of order two makes that we can transform this specific point to the origin, giving an elliptic curve with a simpler description we can henceforth work with.

2. The next step concerns the introduction of another curve $\overline{E}$ and a homomorphism ϕ to it. It turns out that this homomorphism is strongly related to the multiplication-by-two map.

3. Finally we will study a map α from $E(K(t))$ to $K(t)^*/K(t)^{*^2}$ which will provide a way to bound the index.

We will prove that the index of interest is finite for a specific case in the upcoming subsections. In these subsections we will discuss the three steps given above. From here on we will write $L := K(t)$ for notational reasons.

5.1 Translating the curve

As mentioned before, we are assuming that there exists an L-rational point of order 2 on the curve E, we will call this point $(x_0, 0)$. We move this point to the origin by replacing x by $x + x_0$ in $f(x)$. We obtain

$$\begin{aligned} y^2 &= (x + x_0)^3 + a(x + x_0)^2 + b(x + x_0) + c \\ &= x^3 + (3x_0 + a)x^2 + (3x_0^2 + 2ax_0 + b)x + (x_0^3 + ax_0^2 + bx_0) + c \\ &= x^3 + (3x_0 + a)x^2 + (3x_0^2 + 2ax_0 + b)x, \end{aligned}$$

where the last equality follows from the fact that $x_0^3 + ax_0^2 + bx_0 + c = 0$ since $(x_0, 0)$ is a point on the curve. If we rename a as $3x_0 + a$ and b as $3x_0^2 + 2ax_0 + b$ we can write the equation for this curve as $y^2 = x^3 + ax^2 + bx$. We note two things; the first is that now the point $T := (0, 0)$ is a point of order two on the curve. The second is that it does not matter if we study the L-rational points on this new curve or on the previous one, since a rational point (ξ, η) on the original curve corresponds to a rational point $(\xi - x_0, \eta)$ on the new curve and vice versa a rational point (ξ', η') on the new curve corresponds to a rational point $(\xi' + x_0, \eta')$ on the original curve. We will therefore henceforth consider the curve $E : y^2 = x^3 + ax^2 + bx$ instead of the one we had originally.

We can also look at this in a different way. The operation that is applied to the curve is simply a translation, visualising the group law on both the original as well as the translated curve (which can easily be done as its description is geometric) it is easy to see that the L-rational points are in one-to-one correspondence. In fact this holds in some more generality: if ϕ is a map with rational coefficients between elliptic curves and it sends the point at infinity on the first curve to the point at infinity on the second curve, ϕ is a homomorphism. This is clearly what happens when translating the curve and since translating is an invertible operation it is an isomorphism of elliptic curves.

We now introduce a new curve, $\overline{E}$, given by a similar equation. As mentioned before, the curve and the homomorphism ϕ we will introduce are strongly related to the multiplication-by-two map; it is known that the complex points on an elliptic curve can be considered as lying in a parallelogram with two certain periods ω_1 and ω_2, i.e. they are in the set

$$\{\alpha\omega_1 + \beta\omega_2 : 0 \leqslant \alpha, \beta \leqslant 1\} \subset \mathbb{C},$$

for $\omega_1, \omega_2 \in \mathbb{C}\backslash\{0\}$ such that $\omega_1/\omega_2 \notin \mathbb{R}$. The homomorphism ϕ which maps to the new curve will give us the result of slicing this parallelogram in half. If we do this again, we obtain a parallelogram that is very similar to the first and in fact the curve that we get from this, turns out to be isomorphic to the original curve. Moreover, the composition of these two operations will turn out to be the multiplication-by-two map.

Now that we have given some introduction to the new curve $\overline{E}$ and the homomorphism ϕ from E to $\overline{E}$ we will give the explicit equations that define them;

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

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. The map ϕ is defined as

$$\phi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2 - b)}{x^2}\right), & \text{if } P = (x, y) \neq O, T, \\ \overline{O}, & \text{if } P = O \text{ or } P = T. \end{cases}$$

In the next subsection we will prove some properties of this map ϕ, amongst which the fact that it is a homomorphism, as we already claimed.

5.2 Properties of ϕ and $\overline{E}$

The map ϕ as introduced above has some nice properties which will help us study the group $E(L)/2E(L)$. We will prove some of these properties in this section. Throughout the rest of this section the curves E and $\overline{E}$ will be as before. The first property of ϕ will not come as a great surprise and is stated below as a proposition.

Proposition 3. *The map ϕ maps E to $\overline{E}$ and is a homomorphism. Moreover,* $\ker(\phi) = \{O, T\}$.

Proof. It is quite easy to check that indeed $\phi : E \to \overline{E}$. Indeed we only have to check that the image $(\phi((x, y)) = (\bar{x}, \bar{y})$ satisfies the equation for $\overline{E}$:

$$\begin{aligned}
\bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} &= \bar{x}(\bar{x}^2 + \bar{a}\bar{x} + \bar{b}) \\
&= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\right) \\
&= \frac{y^2}{x^6}\left((y^2 - ax^2)^2 - 4bx^4\right) \\
&= \frac{y^2}{x^6}\left((x^3 + bx)^2 - 4bx^4\right) \\
&= \left(\frac{y(x^2 - b)}{x^2}\right)^2 \\
&= \bar{y}^2,
\end{aligned}$$

so indeed ϕ maps E to $\overline{E}$.

The next claim in the proposition is that ϕ is a homomorphism. The proof of this claim mainly consists of considering different cases for points P and Q on the curve and calculating, using the formulas for the group law, that indeed $\phi(P + Q) = \phi(P) + \phi(Q)$ for any points P and Q on the curve. This proof is the same for elliptic curves over any field, therefore I refer to page 85-87 of [2] for the proof, where most of the explicit computations are done and explained at length.

The final thing that needs to be proven for this proposition is that the kernel of ϕ consists solely of O and $T = (0, 0)$. However, it is obvious that both O and T are in the kernel by the definition of ϕ and that no other elements are (since $y^2/x^2 = x + a + b/x$). This finalizes the proof of the proposition.

□

As mentioned we can check that ϕ is a homomorphism by considering some different cases and doing some computations. The map ϕ is constructed such that it maps O to $\overline{O}$. Note however that ϕ, as defined on $(x, y) \notin \{O, T\}$, is a rational function between elliptic curves and if it maps O to $\overline{O}$ 'by itself' (i.e. we do not define it as a piecewise function which maps O and T to $\overline{O}$ as before) then it is a homomorphism of curves, as was mentioned in subsection 5.1. That is, if we define ϕ as

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right),$$

for all (x, y) on the curve and we can show that it maps O to $\overline{O}$, then ϕ is a homomorphism. The x- and y-coordinate of O are such that $1/x = 1/y = 0$, so we want to show that also $1/(y^2/x^2)$ and $1/(y(x^2 - b)/x^2)$ are 0. Note that

$$\frac{y^2}{x^2} = \frac{x^3 + ax^2 + bx}{x^2} = x + a + \frac{b}{x} = x + a,$$

since $1/x = 0$. Hence $x^2/y^2 = 1/(x + a) = 0$, so indeed the image of the x-coordinate is the x-coordinate of $\overline{O}$. For the image of the y-coordinate we have the following

$$\frac{y(x^2 - b)}{x^2} = y - \frac{by}{x^2} = y - \frac{b}{x}\frac{y}{x}.$$

Note that $b/x = 0$ and also $y/x = \sqrt{y^2/x^2} = \sqrt{0} = 0$, hence the image under ϕ of this y-coordinate is the element y which satisfies $1/y = 0$. Hence the image of the y-coordinate of O is the y-coordinate of $\overline{O}$ and we conclude that $\phi(O) = \overline{O}$ and that ϕ is a homomorphism.

There are two more properties of ϕ and the curve $\overline{E}$ that are interesting for this thesis. The next one is stated below.

Proposition 4. *If we define a map $\bar{\phi}$ on $\overline{E}$ in the same way as we defined ϕ on E, we get a map from $\overline{E}$ to $\overline{\overline{E}}$. The curve $\overline{\overline{E}}$ is isomorphic to E via the map $(x, y) \mapsto (x/4, y/8)$ and there is a homomorphism $\psi : \overline{E} \to E$ defined by*

$$\psi(\overline{P}) = \begin{cases} \left(\dfrac{\bar{y}^2}{4\bar{x}^2}, \dfrac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2} \right), & \text{if } \overline{P} = (\bar{x}, \bar{y}) \neq \overline{O}, \overline{T}, \\ O, & \text{if } \overline{P} = \overline{O} \text{ or } \overline{P} = \overline{T}. \end{cases}$$

Proof. It is clear that $\bar{\phi}$ indeed maps $\overline{E}$ to $\overline{\overline{E}}$, since we define it analogously to ϕ. It is also easy to see that the curve $\overline{\overline{E}}$ is given by the equation

$$\overline{\overline{E}} : y^2 = x^3 + 4ax^2 + 16bx.$$

If we define a map $g : \overline{\overline{E}} \to E$ by $(x, y) \mapsto (x/4, y/8)$ it is not hard to see that g has an inverse and that it respects the group structure, hence g defines an isomorphism between $\overline{\overline{E}}$ and E.

Since $\bar{\phi}$ is defined in the exact same way as ϕ, only with domain $\overline{E}$, it is a homomorphism from $\overline{E}$ to $\overline{\overline{E}}$. Moreover, we have an isomorphism g from $\overline{\overline{E}}$ and we can see that the map ψ is precisely the composition of these two maps: $\psi = g \circ \bar{\phi}$. This means that ψ can be written as the composition of two homomorphisms, hence ψ is a homomorphism itself as well (from the curve $\overline{E}$ to the curve E). □

The final property is perhaps the most interesting, because it tells us that the composition of ϕ and ψ is in fact the multiplication-by-2 map, which is interesting when studying the group $2E(L)$. This is stated as a proposition below.

Proposition 5. *The composition $\psi \circ \phi : E \to E$ is the multiplication-by-2 map, i.e.*

$$\psi \circ \phi(P) = 2P$$

Proof. The proof of this proposition merely consists out of computations with the explicit formulas for the group law. It is clear that the statement holds when $P = O$, so we will consider two cases; namely the case where for $P = (x, y)$ both $x \neq 0$ and $y \neq 0$ and the case where P has order two. Note that we have then indeed proven the proposition for all points P on the curve, since when $x = 0$ we have $P = T$ and T has order two, and when $y = 0$, P is also a point of order two.

We first consider the case where P is not a point of order two. Using the formula for the doubling of a point and doing some computations with the y-coordinate, we obtain the following

$$\begin{aligned} 2(x,y) &= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)^2}{4y^2} \left[\frac{(x^2-b)^4}{16y^4} + a\frac{(x^2-b)^2}{4y^2} + b \right] \right) \\ &= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right). \end{aligned}$$

Now we will show that the same expression holds for $\psi \circ \phi((x, y))$. We obtain the following by using the definition of ϕ and ψ and by doing some algebra

$$\begin{aligned}
\psi \circ \phi((x,y)) &= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \\
&= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2-(a^2-4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2} \right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4-x^4(a^2-4b))}{8y^3x^2} \right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^2(x^2+ax+b)^2-x^4(a^2-4b))}{8y^3x^2} \right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2}{8y^3} \right).
\end{aligned}$$

This expression is precisely the same as the expression we found for $2(x,y)$, hence we have shown that $2P = \psi(\phi(P))$ for points P that do not have order 1 or 2.

Now we will consider the case where P is a point of order two, i.e. $y = 0$. This means that we want to prove $\psi(\phi(P)) = O$. If $P = T$, then by definition of ϕ and ψ we have

$$\psi(\phi(T)) = \psi(\overline{O}) = O.$$

If we consider $x \neq 0$, then again by definition of ϕ and ψ we have that

$$\psi(\phi((x,0))) = \psi(T) = O.$$

So indeed it is true that $\psi \circ \phi(P) = 2P$. □

Note that the statement $\phi \circ \psi(P)$ can be proven in the same way. This proposition states that we can break down the multiplication-by-2 map in two parts by going via another curve, namely the curve $\overline{E}$. This will be of interest in the final part of the proof that we can bound the index $[E(L) : 2E(L)]$.

5.3 The image of $E(L)$ under ϕ

In this section we will discuss several properties of the images of $E(L)$ and $\overline{E}(L)$ under ϕ and ψ respectively. Since ϕ and ψ are defined analogously, there is a very obvious relation between the image under ϕ and the image under ψ, therefore we will discuss only one of the two. The properties of the image of ϕ that are of interest are stated below as a proposition.

Proposition 6. *With $\phi : E(L) \to \overline{E}(L)$ as defined before, the following are true about $\phi(E(L))$:*

(i) $\overline{O} \in \phi(E(L))$.

(ii) $\overline{T} = (0,0) \in \phi(E(L))$ *if and only if* $\bar{b} = a^2 - 4b$ *is a perfect square.*

(iii) If $\overline{P} = (\bar{x}, \bar{y}) \in \overline{E}(L)$ *with* $\bar{x} \neq 0$*, then* $\overline{P} \in \phi(E(L))$ *if and only if* $\bar{x}$ *is the square of some L-rational element.*

Proof. We will prove this proposition step by step.

(i) The first claim is quite obvious; since O is defined to be an L-rational point, it is an element of $E(L)$ and since $\phi(O) = \overline{O}$ we immediately have that $\overline{O} \in \phi(E(L))$.

(ii) From the definition of ϕ we can see that $\overline{T}$ is in the image $\phi(E(L))$ if and only if there is some element $(x, y) \in E(L)$ such that $y^2/x^2 = 0$, which is equivalent to having an element $(x, y) \in E(L)$ such that $x \neq 0$ and $y = 0$. If we put $y = 0$ in the equation for the curve, we obtain

$$0 = x(x^2 + ax + b).$$

Since we have that $x \neq 0$, we need that the quadratic polynomial $x^2 + ax + b$ has an L-rational root. Since the abc-formula holds for a general field (with characteristic $\neq 2$), this occurs precisely when the discriminant of this equation is a perfect square. The discriminant is equal to $a^2 - 4b$, which is how $\bar{b}$ is defined.

(iii) Out of the three statements, this statement is hardest to prove. We first note that one side of the implication is obvious: if $(\bar{x}, \bar{y}) \in \phi(E(L))$ and $\bar{x} \neq 0$, we can write that $\bar{x} = y^2/x^2$, by definition of ϕ, and hence $\bar{x}$ is the square of the element $y/x \in L$.
The other side of the implication is more difficult to prove. We first assume that we can write a point $\bar{x}$ as the square of some L-rational number w, i.e. $\bar{x} = w^2$. We now want to show that $(\bar{x}, \bar{y}) \in \phi(E(L))$, to do this we will find a rational point on the curve E that maps to $(\bar{x}, \bar{y})$. Note that since the kernel of ϕ consists of two elements and ϕ is a homomorphism, there will be two elements that map to $(\bar{x}, \bar{y})$ if it really lies in $\phi(E(L))$. We claim that the points (x_1, y_1) and (x_2, y_2) as given below are mapped to our point $(\bar{x}, \bar{y})$.

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right), \qquad y_1 = x_1 w,$$

$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right), \qquad y_2 = -x_2 w.$$

We need to do two things; the first is to show that these points $P_i := (x_i, y_i)$ are really on the curve E and the second is to show that $\phi(P_i) = (\bar{x}, \bar{y})$. We start with showing that the points are on the curve. For this we note that we can simplify the product $x_1 x_2$ in the following way

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\left((w^2 - a)^2 - \frac{\bar{y}^2}{w}\right) \\ &= \frac{1}{4}\left((\bar{x} - a)^2 - \frac{\bar{y}^2}{w}\right) \\ &= \frac{1}{4}\left(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{\bar{x}}\right) \\ &= \frac{1}{4}\left(\frac{4b\bar{x}}{\bar{x}}\right) \\ &= b. \end{aligned}$$

We want to show that the points (x_i, y_i) satisfy $y_i^2 = x_i^3 + ax_i^2 + bx_i$, which is equivalent to showing that they satisfy

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i},$$

and since $b = x_1 x_2$ and $(y_i/x_i)^2 = w^2$, this is in turn equivalent to showing

$$w^2 = x_1 + a + x_2.$$

If we look at the sum $x_1 + x_2 + a$, we see immediately that indeed the outcome is w^2, hence the points P_i are on the curve E. Next we have to check that P_i is actually mapped to $(\bar{x}, \bar{y})$ under ϕ. It is clear from the definition of y_i that

$$\frac{y_i^2}{x_i^2} = \frac{(\pm x_i w)^2}{x_i^2} = w^2 = \bar{x}.$$

Finally we need to show that

$$\frac{y_i(x_i^2 - b)}{x_i^2} = \bar{y},$$

this actually follows from some simple computations

$$\begin{aligned} \frac{y_1(x_1^2 - b)}{x_1^2} &= \frac{x_1 w(x_1^2 - x_1 x_2)}{x_1^2} = w(x_1 - x_2) = w\frac{\bar{y}}{w} = \bar{y}, \\ \frac{y_2(x_2^2 - b)}{x_2^2} &= \frac{x_2 w(x_2^2 - x_1 x_2)}{x_2^2} = w(x_1 - x_2) = w\frac{\bar{y}}{w} = \bar{y}. \end{aligned}$$

We have now proven that both P_i are indeed mapped to $(\bar{x}, \bar{y})$ and hence we are done with the proof of the proposition.

□

We have seen several properties of the image of the L-rational points on the curve E under the homomorphism ϕ. In subsection 5.5 we will see why this is interesting. We will now introduce a new map α which will also come in handy. The map α, which maps $E(L)$ to L^*/L^{*^2} is defined as

$$\begin{aligned}
\alpha(O) &= 1 \bmod L^{*^2}, \\
\alpha(T) &= b \bmod L^{*^2}, \\
\alpha((x, y)) &= x \bmod L^{*^2}, \quad \text{if } x \neq 0.
\end{aligned}$$

In Proposition 6 we saw some relations between elements being a square in $E(L)$ and elements that are in the image of ϕ. Since we will be considering L^*/L^{*^2}, one can imagine that these relations will tell us something about the kernel of α. In the next subsection we will discuss some properties of this map α. At the end of that section, we will have gathered all the information that is needed to prove the final condition for the descent argument.

5.4 Properties of α

We have almost finished discussing all results that we will need, in fact, the only thing we need to establish is that both indices

$$[\bar{E}(L) : \phi(E(L))] < \infty \quad \text{and} \quad [E(L) : \psi(\bar{E}(L))] < \infty.$$

We will discuss why this is sufficient in the section after this one, but for now it is nice to know that this is true since it means that we “only” have to prove the finiteness of these two indices. Because we have already established quite some facts about the images of ϕ and ψ, one can imagine that we are not very far away from proving this. In fact, we will find out that the map α gives us the finiteness of one of these indices (for certain L). Since we can of course also define $\bar{\alpha} : \overline{E}(L) \to L^*/L^{*^2}$ analogously, we then also obtain that the other index $[\overline{E}(L) : \phi(E(L))]$ is finite. We now state some propositions which concern the map α and which will help prove the finiteness of the indices above.

Proposition 7. *The map $\alpha : E(L) \to L^*/L^{*^2}$ as given before is a homomorphism.*

Proof. The proof of this statement is quite elementary, the main things we will be needing are the explicit formulas for the group law. We first make an observation which makes what we want to prove slightly easier, this observation is that α sends inverses to inverses. This is true because

$$\alpha(-P) = (x, -y) = x = \frac{1}{x}x^2 \equiv \frac{1}{x} = \frac{1}{\alpha(P)} = \alpha(P)^{-1} \bmod L^{*^2}$$

for $x \neq 0$. However by the definition of α and Proposition 6 from the previous section this also holds for O and T. The fact that α maps inverses to inverses gives us the following: if we can prove that whenever $P_1 + P_2 + P_3 = O$ then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \bmod L^{*^2}$, we have in fact proven that α is a homomorphism for all points P_1, P_2 and P_3. This is true since in that case

$$\alpha(P_1 + P_2) = \alpha(-P_3) = \alpha(P_3)^{-1} = \alpha(P_1)\alpha(P_2).$$

We will start with the proof of the case where none of the points equals O or T, so they are collinear i.e. lie on a line. We denote the line by: $y = \lambda x + \nu$. This line then intersects the curve in three points, namely P_1, P_2 and P_3, we let the x-coordinates of their intersection be x_1, x_2 and x_3. If we combine $y^2 = \lambda^2 x^2 + 2\lambda\nu x + \nu^2$ with the equation for the curve, we find an equation for which x_1, x_2 and x_3 are the roots

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x - \nu^2 = 0.$$

This gives us that $-x_1x_2x_3 = -\nu^2$, hence

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \bmod L^{*^2},$$

which proves the first case.

We now have to prove the case where P_1, P_2, P_3 are not all distinct from O and T. If we assume that one of the points, let it be P_1, equals O, then $P_2 + P_3 = O$ and hence $P_2 = -P_3$. This gives $\alpha(P_1)\alpha(P_2)\alpha(P_3) = \alpha(-P_3)\alpha(P_3) = 1$. If we assume that two points equal O, the third one must also equal O, and it is easy to see that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$. In the same way: if two points equal T, the third point must equal O and again we are done.

Finally we need to show that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$ also holds if only one of the points equals T, this is of course a specific case of what we showed before. If $T + P_2 + P_3 = O$ then that means that $P_2 + P_3 = T$. Geometrically we can see that this means that P_2 and P_3 are on the same line which goes through $(0,0) = T$. This means that this line will be given by an equation of the form $y = \lambda x$. If we denote the x-coordinates of the points again by $x_1 = 0, x_2$ and x_3, they are the roots of the equation

$$x^3 + (a - \lambda^2)x^2 + bx = 0.$$

We can see that x_2 and x_3 must be the roots of

$$x^2 + (a - \lambda^2)x + b,$$

so that $x_2 x_3 = b$. Then we obtain

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = b^2 \equiv 1 \bmod L^{*^2}.$$

This finishes the proof of this proposition. □

As already mentioned, we know some relations between being in the image of ϕ or ψ and e.g. b being a square in L^* by Proposition 6. The next proposition can easily be proven using results from that previous proposition.

Proposition 8. *The kernel of α is the image $\psi(\overline{E}(L))$. Hence α induces a one-to-one homomorphism*

$$\alpha' : E(L)/\psi(\overline{E}(L)) \hookrightarrow L^*/L^{*^2}.$$

Proof. By Proposition 6 we know some things about the image of ψ, namely that: O is in the image, that T is in the image if and only is b is a perfect square and that (x, y) for $x \neq 0$, is in the image if and only if x is the square of some element. This tells us precisely which elements are in the image of ψ. We know that O is always in there, but O is mapped to 1 by α, hence it is in the kernel of α. If T is in the image of ψ, b is a perfect square (and vice versa), so it is congruent to 1 mod L^{*^2} and since T gets mapped to b, also T is in the kernel of α. In the same way a point (x, y) is in the image of ψ if and only if x is a square. Moreover, then (x, y) gets mapped to $x \bmod L^{*^2} \equiv 1 \bmod L^{*^2}$ and also (x, y) is in the kernel of α. This shows that indeed $\ker(\alpha) = \psi(\overline{E}(L))$. □

The next proposition will give us the result with which it will be very easy to prove the finiteness of the indices we are interested in.

Proposition 9. *Let $p_1, \ldots, p_s$ be the monic irreducible elements that divide b. Then the image of α is contained in the subgroup of L^*/L^{*^2} consisting of the elements*

$$\{up_1^{\epsilon_1} \cdots p_s^{\epsilon_s} : \textit{each } \epsilon_i \textit{ equals } 0 \textit{ or } 1 \textit{ and } u \in K^*/K^{*^2}\}.$$

Proof. It is clear that the image of O is in this subgroup, as O is mapped to the unit element in L^*/L^{*^2} by α, which is in every subgroup. Also if $T \in E(L)$, $\alpha(T) = b \bmod L^{*^2}$. Since $b = u \cdot p_1^{e_1} \cdots p_s^{e_s}$ for certain $e_i > 0$ and $u \in K^*$, also $\alpha(T)$ is in the subgroup mentioned above.

Now we take an element $P = (x, y) \in E(L)$ for which $x \neq 0$ and $P \neq O$. We want to show that $\alpha(P) = x$ can be written as a product of irreducibles dividing b and a unit when we consider it modulo squares. To this end we recall that the L-rational points $P = (x, y)$ on $E(L)$ have coordinates that can be written in the form $x = m/e^2$ and $y = n/e^3$, where $\gcd(m, e) = \gcd(n, e) = 1$ from subsection 4.3. Substituting these expressions into the equation for the curve and clearing the denominators we obtain

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$

Since we are considering a principal ideal domain $K[t]$, the notion of greatest common divisors is well defined and we will look at

$$d := \gcd(m, m^2 + ame^2 + be^4) = \gcd(m, be^4) = \gcd(m, b).$$

Obviously, d divides both m and be^4, but by assumption m and e have no common divisors, hence d must divide b. Now we want to look at the factorisation of m into irreducibles. If we have an irreducible element p dividing m but not dividing b, then it cannot divide be^4 and hence it cannot divide $m^2 + ame^2 + be^4$. Moreover, if $p|m$, then also $p|n^2$, but since the irreducible elements in the factorisation of n^2 occur with even power, we must have that p occurs in some *even* power in n^2. Since $p \nmid m^2 + ame^2 + be^4$, we must then have that p occurs in the factorisation of m to precisely that even power.

This gives us that all irreducibles occuring in the factorisation of m but not in the factorisation of b, occur in m to some even power, so we can write them together as the square of some element $f \in K[t]$. We can write

$$m = uf^2 p_1^{\delta_1} \cdots p_s^{\delta_s},$$

where the δ_i are the powers of the irreducibles that occur in b and u is a unit element. We observe that

$$\alpha(P) = x = \frac{m}{e^2} \equiv m = uf^2 p_1^{\delta_1} \cdots p_s^{\delta_s} \equiv up_1^{\epsilon_1} \cdots p_s^{\epsilon_s} \bmod L^{*^2},$$

where the ϵ_i are either 0 or 1 and we can conclude that $\alpha(P)$ is indeed in the aforementioned subgroup.

□

Next we will see that indeed the finiteness of the field K makes it easy to conclude that the index we are interested in is indeed finite. For this we namely need the subgroup mentioned in the proposition above to have finitely many elements.

Proposition 10. *Suppose $E : y^2 = x^3 + ax^2 + bx$ over $\mathbb{F}_q(t)$ with $a, b \in \mathbb{F}_q[t]$ and $\overline{E}$ as before. Let s be the number of monic irreducible polynomials dividing b. Then the index*

$$[E(\mathbb{F}_q(t)) : \psi(\overline{E}(\mathbb{F}_q(t))] \leqslant 2^{s+1}$$

Proof. The subgroup mentioned in Proposition 9 has precisely 2^{s+1} elements, since the ϵ_i are either 0 or 1 and the number of unit elements in $\mathbb{F}_q[t]$ modulo squares are

$$\#\mathbb{F}_q^*/\#\mathbb{F}_q^{*^2} = \frac{q-1}{\frac{1}{2}(q-1)} = 2$$

as well. By Proposition 8, there exists an injective map from $E(\mathbb{F}_q(t))/\psi(\overline{E}(\mathbb{F}_q(t)))$ into that subgroup. Therefore the index of $\psi(\overline{E}(\mathbb{F}_q(t)))$ in $E(\mathbb{F}_q(t))$ is at most 2^{s+1}, which proves this proposition. □

Of course the fact that there are only finitely many units in $\mathbb{F}_q[t]$ shows that the subgroup mentioned above is finite. However, we do not per se require there to be finitely many units, we just need finitely many units modulo squares, which happens in many more fields than just the finite fields. Note that there are finitely many units modulo squares in any algebraically closed field, since x^2 always has its zeroes in the field, so that every unit is a square. Therefore

$$[E(K(t)) : 2E(K(t))]$$

is also finite whenever K is an algebraically closed field. We can also see that it holds for e.g. $K = \mathbb{R}$ as well, since there are only two units modulo squares in $\mathbb{R}$. However $K = \mathbb{Q}$ for example does not work, since there are infinitely many units modulo squares.

5.5 Bounding the index

We have now established all results that we will need. As mentioned, we were already almost done when we established that both indices $[E(L) : \psi(\overline{E}(L)]$ and $[\overline{E}(L) : \phi(E(L))]$ are finite for for example $L = \mathbb{F}_q(t)$. The next lemma will tell us why it is enough to have the finiteness of these indices.

Lemma 5. *Let A and B be abelian groups and suppose that $\phi : A \to B$ and $\psi : B \to A$ are homomorphisms which satisfy*

$$\psi \circ \phi(a) = 2a \quad \text{for all } a \in A \qquad \text{and} \qquad \phi \circ \psi(b) = 2b \quad \text{for all } b \in B.$$

Suppose further that $\phi(A)$ has finite index in B and that $\psi(B)$ has finite index in A. Then

$$[A : 2A] \leqslant [A : \psi(B)][B : \phi(A)],$$

in particular we can conclude that $2A$ has finite index in A.

Proof. The fact that $\psi(B)$ has finite index in A, gives that there exist only finitely many representatives, let's say n, of the cosets of $\psi(B)$ in A. We denote those representatives by $a_1, \ldots, a_n$. In the same way there exist finitely many representatives of the cosets of $\phi(A)$ in B, we denote those by $b_1, \ldots, b_m$. We claim the following: the cosets of $2A$ in A can all be represented by an element from the following set:

$$\mathscr{X} := \{a_i + \psi(b_j) : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}.$$

If this holds, then, since $[A : 2A]$ equals the number of distinct cosets of $2A$ in A, it follows that $[A : 2A] \leqslant mn$, since mn is an upper bound for the number of elements in the set $\mathscr{X}$. Since $m = [B : \phi(A)]$ and $n = [A : \psi(B)]$, this would prove the lemma.

By the above argument, it suffices to prove that the set $\mathscr{X}$ contains a complete set of representatives of the cosets of $2A$ in A. This is equivalent to showing that if we take an arbitrary element a from A, this a can be written as an element in some coset $\alpha + 2A$, where $\alpha \in \mathscr{X}$, i.e. $a = \alpha + 2a'$, for some $a' \in A$. Since a must be in one of the cosets of $\psi(B)$ which are represented by $a_1, \ldots, a_n$, we can write $a = a_i + \psi(b)$ for some representative a_i and some $b \in B$. In the same way, since b must be in one of the cosets of $\phi(A)$, we can write $b = b_j + \phi(a')$ for some representative b_j and some $a' \in A$. We now have the following

$$\begin{aligned} a &= a_i + \psi(b) \\ &= a_i + \psi(b_j + \phi(a')) \\ &= a_i + \psi(b_j) + \psi(\phi(a')) \\ &= a_i + \psi(b_j) + 2a'. \end{aligned}$$

Since $a_i + \psi(b_j) \in \mathscr{X}$ we have proven the lemma. □

We conclude that if we have a field $K(t)$ that satisfies the properties from the proposition above, we can show in this way that the index $[E(K(t)) : 2E(K(t))]$

is finite. As mentioned before, the finiteness of the indices of the images of ϕ and ψ in $\overline{E}(K(t)))$ and $E(K(t))$ respectively does not come for free. If we are considering a rational function field $K(t)$ and we want to prove the finiteness of these indices in the way we did in the previous section, we really require there to be only finitely many unit elements in $K[t]^*$ modulo the squares in $K[t]^*$. This is easily satisfied when $K = \mathbb{F}_q$, but other cases are more difficult or even untrue. Therefore we cannot conclude from our argument that $2E(K(t))$ has finite index in $E(K(t))$ for any rational function field K. We may however conclude that it does hold for the case where $K = \mathbb{F}_q$ or K is an algebraically closed field. So we have proven that

$$[E(K(t)) : 2E(K(t))] < \infty,$$

if $K = \mathbb{F}_q$ or K is algebraically closed.

6 The curve $\overline{E}$ and the homomorphism ϕ

In subsection 5.1 we introduced a new curve $\overline{E}$ and a homomorphism ϕ to it. Recall that $\phi : E(K(t)) \to \overline{E}(K(t)))$ was defined as

$$\phi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2}\right), & \text{if } P = (x,y) \neq O, T, \\ \overline{O}, & \text{if } P = O \text{ or } P = T. \end{cases}$$

This map turned out to help when studying the multiplication-by-two map after doing some arithmetic, but it is at first sight not obvious why one would choose this map. It is slightly more obvious why this map is chosen when studying some field different than $L := K(t)$, namely the function field of E over L, denoted by $L(E)$. This consists of the rational functions over L on E and is formed by taking the field of fractions of $L[x,y]/(y^2 - (x^3 + ax^2 + bx))$, it is not hard to show that this is the field $L(x)[y]$ where y satisfies $y^2 = x^3 + ax^2 + bx$. Again it might not be obvious why we would study this function field, but if one is familiar with some category theory we can remark that the category of function fields over a field is categorically equivalent to the category of irreducible curves over that same field. In essence this means that studying the function field gives us information about the elliptic curve as well.

Next we consider the translation map τ that adds the point $T = (0,0)$ to a point $P = (x,y)$ on the curve. Using the duplication formulas it is easy to calculate that $\tau(P) = (b/x, -by/x^2)$. Now we consider what this map does on the function field of E over L, of course τ is not defined on $L(E)$, but since x and y are in the function field we can define $\tau^* : L(E) \to L(E)$ in almost the same way. We let τ^* be such that

$$\tau^*(x) = \frac{b}{x} \quad \text{and} \quad \tau^*(y) = \frac{-by}{x^2}.$$

It is not hard to see that τ^* is an automorphism of order 2 (this also follows from the fact that τ is a translation over a point of order 2). Consider the elements in $L(E)$ that are invariant under this map τ^*, i.e. the elements in $L(E)^{\langle\tau^*\rangle}$. In fact those are the rational functions that do the same at the point P as at the point $P + (0,0)$, i.e. the rational functions on $E/\langle(0,0)\rangle$. This $E/\langle(0,0)\rangle$ will turn out to 'be' $\overline{E}$, by showing that their function fields are the same (note that we don't know yet if $E/\langle(0,0)\rangle$ is an elliptic curve).

Let $\xi := y^2/x^2 = x + b/x + a$, which is an element from $L(E)^{\langle\tau^*\rangle}$. This means that the field $L(\xi)$ is a subset of all elements that are invariant under τ^* since both L and ξ are. We have the following inclusion of fields

$$L(\xi) \subset L(x) \subset L(x)[y] = L(E),$$

where y is such that it satisfies $y^2 = x^3 + ax^2 + bx$. We know that the second field extension has degree 2 since y is the zero of some quadratic polynomial, but is not contained in $L(x)$. We know that x is not invariant under τ^*, hence the degree of the first extension is at least 2. Also we know that x is a zero of the polynomial $X^2 + (a - \xi)X + b$, by definition of ξ, so that the degree of the first extension is maximally two. This gives that also $L(\xi) \subset L(x)$ has degree two and hence $L(E)$ has degree 4 as a vector space over $L(\xi)$.

As mentioned we are interested in the subfield of $L(x)[y]$ that is invariant under the map τ^*, by Galois theory and the fact that τ^* has order 2, we know that the second extension of

$$L(\xi) \subset L(E)^{\langle\tau^*\rangle} \subset L(E),$$

has degree 2. The first inclusion follows from the fact that both L and ξ are invariant under τ^*, this extension must have degree 2, since the total extension has degree 4. We took ξ to be an element that is invariant under the map τ^*, but there is another quite obvious element that is also invariant under τ^*, since it has degree 2, namely the element

$$\eta := y + \tau^*(y) = y - by/x^2.$$

Hence we have

$$L(\xi, \eta) \subset L(E)^{\langle\tau^*\rangle} \subset L(E).$$

We can say something more about $L(\xi, \eta)$ if we determine a relation between ξ and η, by looking at η^2.

$$\begin{aligned}
\eta^2 &= \left(y - \frac{by}{x^2}\right)^2 \\
&= y^2 - \frac{2by}{x^2} + \frac{b^2y^2}{x^4} \\
&= \frac{y^2}{x^2}\left(x^2 - 2b + \frac{b^2}{x^2}\right) \\
&= \xi\left(\left(x + \frac{b}{x}\right)^2 - 4b\right) \\
&= \xi((\xi - a)^2 - 4b) \\
&= \xi(\xi^2 - 2a\xi + a^2 - 4b).
\end{aligned}$$

Hence we see that $L(\xi, \eta)$ is precisely the function field of the elliptic curve $\overline{E}$ that is given by the equation

$$\overline{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

It is clear from the expression above that $\eta \notin L(\xi)$, so that the degree of the extension

$$L(\xi) \subset L(\xi, \eta),$$

is at least two. We also have the following field extensions

$$L(\xi) \subset L(\xi, \eta) \subset L(E)^{\langle \tau^* \rangle},$$

and we know that the degree of $L(\xi) \subset L(E)^{\langle \tau^* \rangle}$ is 2. This means that the degree of $L(\xi, \eta) \subset L(E)^{\langle \tau^* \rangle}$ equals 1 and hence

$$L(E)^{\langle \tau^* \rangle} = L(\xi, \eta) = L(\overline{E}).$$

This is one way we can 'find' the curve $\overline{E}$ and the homormorphism ϕ, which is just an element from $L(E)^{\langle \tau^* \rangle}$.

7 Computation of the rank of $E(K(t))$

In this section we consider $E(K(t))$ where $L := K(t)$ is such that $E(L)$ is finitely generated (e.g. $K = \mathbb{F}_q$). We will show how we can (sometimes) calculate the rank of the group $E(L)$. The following proposition is useful for the calculation of the rank.

Proposition 11. *The rank r of the group $E(L)$ can be calculated as*

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4},$$

where α and $\overline{\alpha}$ are as defined before and $\Gamma := E(L)$ and $\overline{\Gamma} := \overline{E}(L)$.

Proof. We first observe a relation between the rank and the index $[\Gamma : 2\Gamma]$. Since Γ is a finitely generated group, it can be written as

$$\Gamma \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{\nu_s}\mathbb{Z},$$

where $r \geqslant 0$ is the rank of Γ, the p_i's are primes and the ν_i's are positive integers. Using this expression for Γ, we see that we can write

$$\Gamma/2\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_{p_1^{\nu_1}}/2\mathbb{Z}_{p_1^{\nu_1}} \times \cdots \times \mathbb{Z}_{p_s^{\nu_s}}/2\mathbb{Z}_{p_s^{\nu_s}}. \tag{3}$$

We know the following about $2(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})$. If $p_i \neq 2$, then $2(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}) = \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$, hence their quotient is the trivial group. If $p_i = 2$, then

$$\#2(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}) = (1/2)\#\mathbb{Z}/p_i^{\nu_i}\mathbb{Z},$$

so their quotient has two elements, meaning it must be isomorphic to the cyclic group of order 2. If we look at (3) we see that

$$[\Gamma : 2\Gamma] = 2^r 2^{\#\{j \text{ such that } p_j = 2\}}.$$

Defining $\Gamma[2]$ to be the subgroup of Γ consisting of all elements Q such that $2Q = O$, we claim that $\#\Gamma[2] = \#\{j \text{ such that } p_j = 2\}$. For $Q \in \Gamma$, we can write

$$Q = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_2Q_s,$$

for $P_i \in \mathbb{Z}$ and $Q_i \in \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$. So if we require $2Q = O$, that means that all n_i must be zero and all m_i satisfy $2m_i \equiv 0 \bmod p_i^{\nu_i}$. If p_i is odd that means that m_i must be zero modulo $p_i^{\nu_i}$. This is not the case for $p_i = 2$, since then $m_i \equiv 0 \bmod 2^{\nu_i - 1}$, so we get two possibilities for m_i, namely $m_i \equiv 0$ or $m_i \equiv 2^{\nu_i - 1} \bmod \nu_i$. So whenever $p_j = 2$ this gives two elements m_j that satisfy $m_j \equiv 0 \bmod 2^{\nu_j - 1}$, i.e. indeed the number of elements in $\Gamma[2]$ is the same as 2 to the power of the number of p_i's that equal 2. We now have

$$[\Gamma : 2\Gamma] = 2^r \cdot \#\Gamma[2]. \tag{4}$$

Note that this a result concerning abelian groups in general. In our specific case we know something about $\#\Gamma[2]$, the elements in this group namely correspond to the element O and elements with y-coordinate equal to zero. From the equation of our curve we see that there are at most three points with y-coordinate equal to zero. There is one point, namely $T = (0,0)$, if $x^2 + ax + b$ does not have any solutions i.e. when $a^2 - 4b$ is not a square. And there are three points when $x^2 + ax + b$ does have solutions i.e. when $a^2 - 4b$ is a square (recall that $a^2 - 4b$ was nonzero because the curve is non-singular). Hence

$$\#\Gamma[2] = \begin{cases} 2, & \text{if } a^2 - 4b \text{ is not a square,} \\ 4, & \text{if } a^2 - 4b \text{ is a square.} \end{cases}$$

We can also say something about $[\Gamma : 2\Gamma]$ in our case. Note that the following holds, using the fact that $2\Gamma \subset \psi(\overline{\Gamma}) \subset \Gamma$:

$$[\Gamma : 2\Gamma] = [\Gamma : \psi \circ \phi(\Gamma)] = [\Gamma : \psi(\overline{\Gamma})] \cdot [\psi(\overline{\Gamma}) : \psi \circ \phi(\Gamma)].$$

Now we consider an abelian group A and a subgroup B of A, where B has finite index in A. If we consider the following maps

$$A \xrightarrow{\psi} \psi(A) \xrightarrow{\pi} \psi(A)/\psi(B),$$

where π is the canonical map, we see that $\pi \circ \psi$ is a surjective map with kernel equal to $B + \ker(\psi)$, so we have

$$\psi(A)/\psi(B) \cong A/(B + \ker(\psi)).$$

Moreover, since B is a normal subgroup of both A and $B + \ker(\psi)$, we have, by the third isomorphism theorem, that

$$\frac{A}{B + \ker(\psi)} \cong \frac{A/B}{(B + \ker(\psi))/B}.$$

Finally, since B and $\ker(\psi)$ are both normal subgroups of A, we have by the second isomorphism theorem

$$\frac{\psi(A)}{\psi(B)} \cong \frac{A/B}{(B + \ker(\psi))/B} \cong \frac{A/B}{\ker(\psi)/(\ker(\psi) \cap B)}.$$

Applying this to $[\psi(\overline{\Gamma}) : \psi \circ \phi(\Gamma)]$ gives

$$[\Gamma : 2\Gamma] = \frac{[\Gamma : \psi(\overline{\Gamma})] \cdot [\overline{\Gamma} : \phi(\Gamma)]}{[\ker(\psi) : \ker(\psi) \cap \phi(\Gamma)]}.$$

We can make this more precise by looking at the elements in the kernel of ψ and in the image of ϕ. We know that $\ker(\psi) = \{O, T\}$ and that O is always in the image of ϕ, but T only is when $a^2 - 4b = \overline{b}$ is a square. Hence

$$[\ker(\psi) : \ker(\psi) \cap \phi(\Gamma)] = \begin{cases} 2, & \text{if } \overline{b} \text{ is not a square,} \\ 1, & \text{if } \overline{b} \text{ is a square.} \end{cases}$$

Also by the first isomorphism theorem and the fact that $\ker(\alpha) = \psi(\overline{\Gamma})$, we have that

$$\alpha(\Gamma) \cong \Gamma / \ker(\alpha) = \Gamma / \psi(\overline{\Gamma}).$$

Combining the above and substituting it into (4) we obtain the result we wanted.

□

This gives a way to compute the rank r, given that we have enough information about the images of α and $\overline{\alpha}$. There are some things that can be said about the images of these maps. If a point $(x, y) \neq (0, 0)$ is on the curve, it can be written as

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3},$$

where $\gcd(m, e) = \gcd(n, e) = 1$. We pick b_1 such that it equals the greatest common divisor of m and b multiplied by the unit that occurs as the leading coefficient of m. This gives that when we write

$$m = m_1 b_1 \quad \text{and} \quad b = b_1 b_2,$$

where $\gcd(m_1, b_2) = 1$, then m_1 has a factorisation with only the unit element occuring in it as a unit. Since m/e^2 and n/e^3 satisfy the equation of the curve we have

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$

Substituting the expressions we have for m and b we obtain

$$n^2 = b_1^2 m_1 (b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

This implies that b_1 divides n so we can write $n = b_1 n_1$. Using this information gives us the following about n_1^2

$$n_1^2 = m_1 (b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

Note that $\gcd(m_1, b_2) = \gcd(m_1, e) = 1$ so that m_1 and $b_1 m_1^2 + a m_1 e^2 + b_2 e^4$ are relatively prime. Since their product is a square and the leading coefficient of m_1 is a square, this means that both of these must be a square. We write

$$M^2 = m_1 \quad \text{and} \quad N^2 = b_1 m_1^2 + a m_1 e^2 + b_2 e^4.$$

Substituting m_1 into the second part of the expression above we obtain the useful equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4. \tag{5}$$

In particular we can also see that the x-coordinate can be written as b_1 times a square

$$x = \frac{b_1 M^2}{e^2}, \tag{6}$$

meaning that its image under α will be b_1 (modulo squares).

Example 7.1. Consider the elliptic curve E over $K(t)$, where we choose K so that $E(K(t))$ is finitely generated, given by the equation

$$E : y^2 = x^3 - tx.$$

The rank of this curve can be computed using Proposition 11 and (5) and (6). First note that O gets mapped to the unit element by α, T gets mapped to $-t \bmod K(t)^{*^2}$ and (x, y) with $x \neq 0$ gets mapped to $b_1 \bmod K(t)^{*^2}$.

We look at the possible factorisations of $b = -t$. Note that b can only be factored as $b = ut \cdot -u^{-1}$, where u is a unit. We need to consider both $b_1 = ut$, $b_2 = -u^{-1}$ and $b_1 = -u^{-1}$, $b_2 = ut$.

- Consider the first factorisation. From (5) we have that $N^2 = utM^4 - u^{-1}e^4$, for some $N, M, e \in K[t]$, where M and N are coprime. Considering the degrees of both sides of the equation we see something interesting, namely the degree of N^2 is even, whereas the degree of utM^4 is odd. This means that $-u^{-1}e^4$ must have the larger degree, so its leading coefficient has to be a square. In particular this means that $-u^{-1}$ must be a square. This means that

  $$b_1 = ut \equiv -(-u^{-1})t \equiv -t \bmod K(t)^{*^2}.$$

  Hence a point on the curve which has x-coordinate ut times some square gives the same image under α as T, namely $-t$.

- Now consider the second factorisation. We make an argument that is almost the same as the previous since we now have $N^2 = -u^{-1}M^4 + ute^4$, hence by a similar reasoning $-u^{-1}$ must be a square again. So we have

  $$b_1 = -u^{-1} \equiv 1 \bmod K(t)^{*^2}.$$

So again the image of such a point is already in the image of α since O is also mapped to it by α.

Since both factorisations give elements that are already in the image of α we obtain that

$$\mathrm{Im}(\alpha) = \{1, -t\}.$$

Next we want to know what the image of $\overline{\alpha}$ is. The curve $\overline{E}$ is given by the equation

$$\overline{E} : y^2 = x^3 + 4tx.$$

Note that the image of $\overline{\alpha}$ at least consists of the elements 1 and t. The possible factorisations of $b = b_1 b_2$ are $b_1 = ut$, $b_2 = 4u^{-1}$ and $b_1 = 4u^{-1}$, $b_2 = ut$. Note that $b_1 = 2ut$, $b_2 = 2u^{-1}$ is not a different factorisation as it only actually changes the unit in it. If we reason in exactly the same way as before using the degrees of the expression, in the first case we obtain that u^{-1} is a square, so

$$b_1 = ut \equiv t \bmod K(t)^{*^2}.$$

In the second case we get that $4u^{-1}$ is a square so again u^{-1} is a square. This gives

$$b_1 = 4u^{-1} \equiv 1 \bmod K(t)^{*^2}.$$

So we obtain

$$\mathrm{Im}(\overline{\alpha}) = \{1, t\}.$$

Now we know what the rank of this curve must be using the result of Proposition 11, since we know how many elements are in the images of α and $\overline{\alpha}$. We have

$$2^r = \frac{\#\mathrm{Im}(\alpha) \cdot \#\mathrm{Im}(\overline{\alpha})}{4} = \frac{2 \cdot 2}{4} = 1,$$

therefore the rank of this curve is 0.

This example illustrates how a rank computation might go, however in this case we have been quite lucky and in general it is a lot more difficult to compute the rank. There are also some ways to compute the torsion subgroup of the curve, using for example Nagell-Lutz theorem. For this I would like to refer to e.g. chapter 8 of [5].

8 Discussion

We have considered a proof of Mordell's theorem and tried to generalise this proof to rational function fields $K(t)$. As was known, the theorem does not hold for general rational function fields, so we expected problems during the proof when wanting to consider an arbitrary rational function field, which is what happened. We also looked in some more detail at some of the mathematical objects occurring in the proof and explicitly computed the rank of a specific elliptic curve.

The first property the height needs to satisfy for the descent argument is not satisfied for general K. Using this height we need K to be a finite field. The other two properties of the height are satisfied for this height function for any $K(t)$, although the proof has some minor differences with the proof for $\mathbb{Q}$.

Most of the proof of the finiteness of the group $2E(K(t))$ in $E(K(t))$ goes in the same way as for $\mathbb{Q}$ because it mainly uses the group law on the curve, which has the same description for any curve. However the image of the map α as introduced in subsection 5.3 does not map into a finite set for every $K(t)$, but it does do so for example for $\mathbb{F}_q(t)$ and rational function fields $K(t)$ with K algebraically closed.

Lang-Néron's theorem tells us that Mordell's theorem holds for any fields that are finitely generated over their prime field, hence it might be interesting to study height functions on this type of rational function fields that do satisfy the finiteness property. It is also interesting to study the image of the map α for different rational function fields. The finiteness of its image is easy to see for a finite field $K = \mathbb{F}_q$ or algebraically closed field K, but since the theorem holds in more generality than for $\mathbb{F}_q(t)$, we might be able to see the finiteness of the image for other $K(t)$ as well by doing some more work.

References

[1] J.L. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21, 1922.

[2] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015.

[3] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *American journal of Mathematics*, 81(1):95 – 118, 1959.

[4] P. Stevenhagen and B. de Smit. Lecture notes: *Kernvak Algebra*, Universiteit van Amsterdam, 1997.

[5] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer International Publishing, 2009.