Elliptic Curves, Divisors and Lines

Lars A. Wallenborn

21. Jun - 19. Jul 2010

Contents

1 Notation and Global Definition 2

2 Elliptic Curves 3

3 Polynomial and Rational Functions 6

4 Zeros and Poles 10

5 Divisors and Lines 18

Abstract

This Script is basis for a seminar talk given in the seminar “Algebraic methods in computational complexity” by Prof. Nitin Saxena in summer term 2010. Its heavily based on a paper by Leonard S. Charlap and David P. Robbins from 1988 [CRD]. We will give all common definitions, results and proofs for this results on elliptic curves over finite fields.

1 Notation and Global Definition

For a field K, $n \in \mathbb{N}$ and $k \in K$ we define

$$n \cdot k := \underbrace{k + \ldots + k}_{n-\text{times}}$$

The characteristic of a field K is defined by

$$\operatorname{char}(K) := \begin{cases} 0 & \text{for } C_k = \varnothing \\ \min(C_K) & \text{else} \end{cases}$$

with $C_k := \{p \in \mathbb{N}_{>0} \mid p \cdot 1 = 0,\ 1 \in K \text{ additive neutral } \}$.

Proposition 1.1. $\operatorname{char}(K)$ *is either* 0 *or prime.*

Global Definition / Notation 1.2. *From now an let*

- K *be an algebraically closed field with* $\operatorname{char}(K) \notin \{2, 3\}$
- *the letters* X *and* Y *be variables*
- $K[X]$ *and* $K[X, Y]$ *be the polynomial ring in one respective two variables*
- $K(X)$ *and* $K(X, Y)$ *be the field of rational functions in one respective two variables*

2 Elliptic Curves

Definition 2.1 (Vanishing Set)**.** *For $f \in K[X,Y]$ we define*

$$V(f) \coloneqq \{(a,b) \in K^2 \mid f(a,b) = 0\}$$

Definition 2.2 (Elliptic Curve)**.** *For $A, B \in K$ the set*

$$E \coloneqq E_{A,B} \coloneqq V(Y^2 - X^3 - AX - B) \cup \{\mathcal{O}\}$$

is called an <u>*elliptic curve over K*</u> *if $s(x) \coloneqq s_{A,B}(x) \coloneqq x^3 + Ax + B$ has three distinct roots. The element $\mathcal{O} \in E$ is called* <u>*identity*</u> *or* <u>*point at infinity*</u> *and element of $\in E \setminus \{\mathcal{O}\}$* <u>*finite*</u>*. For a finite point $P = (a,b) \in E$ we abbriviate $(a,-b)$ by $-P$. The term*

$$\Delta(E_{A,B}) \coloneqq -4A^3 - 27B^2$$

is called <u>*discriminant*</u>*.*

Remark 2.3. *Sometime one defines the set $E_{A,B}$ as elliptic curve and call it non-singular iff $s_{A,B}$ has three distinct roots. Otherwise it is called singular. We will include non-singularity in the definition of elliptic curve because we only want to deal with non-singular ones.*

Definition 2.4 (Points of order two)**.** *Let $E_{A,B}$ be an elliptic curve and $\omega_1, \omega_2, \omega_3$ the three distinct roots of $s_{A,B}(x)$. The three points $\Omega_i \coloneqq (\omega_i, 0) \in E_{A,B}$ are called* <u>*points of order two*</u>*.*

Proposition 2.5. *For an arbitrary $f(x) = x^3 + Ax + B$ with $A, B \in K$ with roots ω_1, ω_2 and ω_3 it holds that:*

1. $0 = \omega_1 + \omega_2 + \omega_3$
2. $A = \omega_2\omega_3 + \omega_1\omega_3 + \omega_1\omega_2$
3. $B = -\omega_1\omega_2\omega_3$

<u>Proof.</u> Since K is algebraically closed we can write

$$\begin{aligned} f(x) &= (x-\omega_1)(x-\omega_2)(x-\omega_3) \\ &= x^3 + x^2(-\omega_1 - \omega_2 - \omega_3) + x(\omega_2\omega_3 + \omega_1\omega_3 + \omega_1\omega_2) - \omega_1\omega_2\omega_3 \end{aligned}$$

comparing coefficients with $x^3 + Ax + B$ gives the result. □

Proposition 2.6 (Elliptic curve criterion)**.** *The set $E_{A,B}$ is an elliptic curve iff $\Delta(E_{A,B}) \neq 0$.*

<u>Proof.</u> We will show that if $E_{A,B}$ is not an elliptic curve (which, by Def. 2.2, means that $s_{A,B}$ has a double or a tripple root) iff $\Delta(E_{A,B}) = 0$.

Suppose $s_{A,B}$ has a double root w.l.o.g. let this root be ω_1. From Prop. 2.5 we get the three relations

$$\begin{aligned} 0 &= 2\omega_1 + \omega_2 \\ A &= 2\omega_1\omega_2 + \omega_1^2 \\ B &= -\omega_1^2\omega_2 \end{aligned}$$

from the first one we get $\omega_2 = -2\omega_1$. Plugging that into the second and third relation yield

$$\begin{aligned} A &= 2\omega_1(-2\omega_1) + \omega_1^2 = -4\omega_1^2 + \omega_1^2 = -3\omega_1^2 \\ B &= -\omega_1^2(-2\omega_1) = 2\omega_1^3 \end{aligned}$$

and finally we get

$$\Delta(E_{A,B}) = -27B^2 - 4A^3 = -27\left(2\omega_1^3\right)^2 - 4\left(-3\omega_1^2\right)^3 = -108\omega_1^6 + 108\omega_1^6 = 0$$

Suppose $s_{A,B}$ has a tripple root then the preceeding proof will do it too.

Suppose $\Delta(E_{A,B}) = 0$:

$$\begin{aligned} & 0 = \Delta(E) = -27B^2 - 4A^3 \\ \Leftrightarrow\quad & \tfrac{-27B^2}{8A^3} = \tfrac{1}{2} \\ \Leftrightarrow\quad & 0 = \tfrac{-27B^2}{8A^3} - \tfrac{1}{2} \\ \Rightarrow\quad & 0 = \left(\tfrac{-27B^2}{8A^3} - \tfrac{1}{2}\right)B = \tfrac{-27B^3}{8A^3} - \tfrac{3B}{2} + B = s_{A,B}\left(\tfrac{-3B}{2A}\right) \end{aligned}$$

So we know that $x_1 := \frac{-3B}{2A}$ is a root of $s_{A,B}$ and polynomial division yields

$$(x^3 + Ax + B) : (x + \frac{3B}{2A}) = x^2 - \frac{3B}{2A}x + \left(A + \frac{9B^2}{4A^2}\right)$$

p-q-formula yield the two other roots:

$$\begin{aligned} x_{2,3} &= -\frac{-\frac{3B}{2A}}{2} \pm \sqrt{\frac{\left(\frac{3B}{2A}\right)^2}{4} - \left(A + \frac{9B^2}{4A^2}\right)} \\ &= -\frac{3B}{4A} \pm \sqrt{\frac{9B^2}{16A^2} - A - \frac{36B^2}{16A^2}} \\ &= -\frac{3B}{4A} \pm \sqrt{\frac{-27B^2}{16A^2} - A} \end{aligned}$$

Now suppose that $s_{A,B}$ has a double root. Then

- $x_2 = x_3$ or
- $x_1 = x_2$ or $x_1 = x_3$

The first case means that the term under the root is zero:

$$\frac{-27B^2}{16A^2} - A = 0 \;\Leftrightarrow\; -27B^2 - 16A^3 = 0$$

together with $-27B^2 - 4A^3 = 0$ that implies $A = B = 0$.

For the second two cases we calculate:

$$\begin{aligned}
-\frac{3B}{2A} &= -\frac{3B}{4A} \pm \sqrt{\frac{-27B^2}{16A^2} - A} \\
-\frac{3B}{4A} &= \pm\sqrt{\frac{-27B^2}{16A^2} - A} \\
\frac{9B^2}{16A^2} &= \frac{-27B^2}{16A^2} - A \\
9B^2 &= -27B^2 - 16A^3 \\
0 &= -36B^2 - 16A^3 \\
0 &= -9B^2 - 4A^3
\end{aligned}$$

Which together with $-27B^2 - 4A^3 = 0$ again implies $A = B = 0$. □

Proposition 2.7. *Elliptic curves are inifinite.*

Proof. Suppose $E_{A,B}$ is finite. Since K, which is as an algebraically closed field, infinite, we can find $a \in K$ s.t. $\forall b \in K : (a,b) \notin E_{A,B}$, hence $\nexists b \in K : b^2 = c$ for $c = a^3 + Aa + B$. But since K is algebraically closed, the polynomial $X^2 - c$ needs to have a root. □

Definition 2.8. *For a subfield $k \subseteq K$ and $A, B \in k$*

$$E(k) := \{(a,b) \in E_{A,B} \mid a, b \in k\} \cup \{\mathcal{O}\}$$

are called k-rational points.

Remark 2.9. *When* $\operatorname{char}(K) \in \{2,3\}$ *the defining equation of an elliptic curve can be more general:*

$$k^2 + a_1 hk + a_3 k = h^3 + a_2 h^2 + a_4 h + a_6$$

but in our case ($\operatorname{char}(K) \notin \{2,3\}$*) it can be shown that our equation can define every elliptic curve that can be defined by this more general seeming one. [WER, Prop. 2.3.2]*

3 Polynomial and Rational Functions

Definition 3.1 (Polynomials on elliptic curve)**.** *For an elliptic curve $E = E_{A,B}$ we denote the set of polynomials on E by*

$$K[E] := {}^{K[X,Y]}/\langle Y^2 - X^3 - AX - B\rangle$$

Global Definition / Notation 3.2. *From now an let the small letters x and y be the coordinat functions, defined by $x(a,b) := a$ and $y(a,b) := b$ on an elliptic curve E, which therefore fullfill the equation $y^2 = s(x)$. With this notation, we can also say that $K[E] = K[x,y]$.*

Remark 3.3. *Passing to the quotient means that we can replace every Y^2 in a polynomial $f \in K[X,Y]$ by the term $X^3 + AX + B$ without changing the equivalence class of f. So f can be written as $f(x,y) = v(x) + yw(x)$ with $v, w \in K[X]$ i.e. polynomials in one variable.*

Notation 3.4 (Canonical form)**.** *A polynomial $f \in K[E]$ is said to be written in canonical form when we write $f(x,y) = v(x) + yw(x)$.*

Remark 3.5. *The canonical form is unique.*

Proof. Let $f(x,y) = \tilde{\tilde{v}}(x) + y\tilde{\tilde{w}}(x) = \tilde{v}(x) + y\tilde{w}(x)$ be two canonical forms. We get $\tilde{\tilde{v}}(x) - \tilde{v}(x)) + y(\tilde{\tilde{w}}(x) - \tilde{w}(x)) = 0$ so after setting $v(x) = \tilde{\tilde{v}}(x) - \tilde{v}(x)$ and $w(x) = \tilde{\tilde{w}}(x) - \tilde{w}(x)$ it suffices to show that from $v(x) + yw(x) = 0$ follows that $v(x) = w(x) = 0$. We calculate

$$\begin{aligned} 0 &= 0 \cdot (v(x) - yw(x)) \\ &= (v(x) + yw(x)) \cdot (v(x) - yw(x)) \\ &= v^2(x) - y^2 w^2(x) \\ &= v^2(x) + (-s(x))w^2(x) \end{aligned}$$

Since $\deg_x(s)$ is odd and $\deg_x(v^2)$ and $\deg_x(w^2)$ are even the polynomial w has to be zero, hence the polynomial v. □

Definition 3.6 (Conjugate and norm)**.** *Write $f \in K[E]$ in canonical form $f(x,y) = v(x) + yw(x)$. The conjugate of f is defined as $\overline{f}(x,y) := v(x) - yw(x)$. The norm of f is defined by $N_f := f \cdot \overline{f}$.*

Remark 3.7.

1. *One can calculate $N_f = v^2(x) - s(x)w^2(x)$ so $N_f \in K[X]$ i.e. a polynomial in only one variable.*
2. *Because we easily see that $\overline{fg} = \overline{f}\,\overline{g}$ it follows that $N_{fg} = N_f N_g$.*

Definition 3.8 (Rational functions on elliptic curve)**.** *For an elliptic curve E we denote the set of rational functions on E by*

$$K(E) := {}^{K[E]^2}/_{\sim}$$

with the following equivalence relation: For $(f,g),(h,k) \in K[E]^2$*:*

$$(f,g) \sim (h,k) :\Leftrightarrow f \cdot k = g \cdot h$$

(to check the equality one can write both $f \cdot k$ *and* $g \cdot h$ *in canonical form and compare coefficients). We denote the equivalence class of* $(f,g) \in K(E)$ *by* $\frac{f}{g}$*. For* $r \in K(E)$ *and a finite point* $P \in E$ *we say* r is finite at P *iff there exists a representation* $r = \frac{f}{g}$ *with* $f,g \in K[E]$ *and* $g(P) \neq 0$ *in this case we define* $r(P) := \frac{f(P)}{g(P)}$*. If* r *is not finite at a point* P *we write* $r(P) = \infty$*.*

Remark 3.9 (Canonical form for rational functions)**.** *One can calculate for* $r = \frac{f}{g} \in K(E)$*:*

$$\frac{f}{g} = \frac{f\overline{g}}{g\overline{g}} = \frac{f\overline{g}}{N_g}$$

writing $(f\overline{g})(x,y) = v(x) + yw(x)$ *in canonical form yields*

$$\frac{f}{g} = \frac{v(x) + yw(x)}{N_g} = \frac{v(x)}{N_g} + y\frac{w(x)}{N_g}$$

so every rational function can be written in canonical form too.

Proposition 3.10. *The rational functions that are finite at* $P \in E$ *form a ring.*

Proof. We want to show that

$$R_P := \{r \in K(E) \mid r \text{ is finite at } P\}$$

together with the pointwise addition and multiplication is a ring. Associativity and commativity of the addition and multiplication and distributivity is inhertied from the underlying field. The elements $\frac{0}{1}, \frac{1}{1} \in R_P$ are the neutral elements, which are clearly finite at P. And we can give additive inverse elements by $-\frac{f}{g} = \frac{-f}{g}$. □

In the following we want to define the value of a rational function at $\mathcal{O}$. In calculus and in the situation of only one variable (i.e. $f \in K(X)$) one normaly compares the degrees of nominator and denominator to obtain a value at ∞, but in our case we have two variables. The relation $y^2 = x^3 + Ax + B$ suggests that the degree of y should be $\frac{2}{3}$ of the degree of x. Since we want to avoid fractional degrees, we assign the degree 3 to y and the degree 2 to x. The classical degree of a polynomial $f \in K[X]$ will be denoted by $\deg_x(f)$.

Definition 3.11 (Degree of a polynomial)**.** *Let* $f \in K[E]$ *and write it in canonical form* $f(x,y) = v(x) + yw(x)$*. The* degree of f *is defined by:*

$$\deg(f) := \max\{2 \cdot \deg_x(v), 3 + 2 \cdot \deg_x(w)\}$$

Remark 3.12. *Recall that* $\deg_x(0) = -\infty$ *and* $\deg_x(c) = 0 \ \forall \ c \in K \setminus \{0\}$

The classical degree of a polynomial and the degree of a polynomial on E are connected via the norm:

Lemma 3.13 (Connection of degree to classical degree)**.** *For $f \in K[E]$:*

$$deg(f) = deg_x(N_f)$$

Proof. Write f in canonical form $f(x,y) = v(x) + yw(x)$ then $N_f = v^2(x) - s(x)w^2(x)$. Since $\deg_x(v^2)$ and $\deg_x(w^2)$ are even and $\deg_x(s)$ is odd, it follows that

$$\begin{aligned}\deg_x(N_f) &= \deg_x(v^2(x) - s(x)w^2(x)) \\ &= \max\left\{\deg_x(v^2), \deg_x(s) + \deg_x(w^2)\right\} \\ &= \max\left\{2 \cdot \deg_x(v), 3 + 2 \cdot \deg_x(w)\right\} \\ &= \deg(f)\end{aligned}$$

□

Furthermore the degree defined at 3.11 has the fundamental property that we expect of degrees:

Proposition 3.14 (Property of degree of polynomials)**.** *For $f, g \in K[E]$:*

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Proof. We easily calculate:

$$\begin{aligned}\deg(fg) &\overset{\text{Lemma 3.13}}{=} deg_x(N_{fg}) \\ &\overset{\text{Rem. 3.7}}{=} \deg_x(N_f N_g) \\ &\overset{\text{property of } \deg_x}{=} \deg_x(N_f) + \deg_x(N_g) \\ &\overset{\text{Lemma 3.13}}{=} \deg(f) + \deg(g)\end{aligned}$$

□

It makes no sense to talk about the ”degree of the nominator (or denominator) of a rational function on E“ since it may change when the representant is changed:

$$\frac{x+1}{xy-2} = \frac{x^2+x}{x^2y-2x}$$

but by Prop. 3.14 we get that for $r = \frac{f}{g} = \frac{h}{k} \in K(E)$ it always holds that $\deg(f) - \deg(g) = \deg(h) - \deg(k)$ since $fk = gh$. Therefore we can make the following definition concerning the value of a rational function at $\mathcal{O}$:

Definition 3.15 (Evaluating a rational function at $\mathcal{O}$)**.** *Let $r = \frac{f}{g} \in K(E)$ and distinguish the following cases:*

$\deg(f) < \deg(g)$**:** *set $r(\mathcal{O}) = 0$*

$\deg(f) > \deg(g)$**:** *say that r is not finte at $\mathcal{O}$.*

$\deg(f) = \deg(g)$ **and** $\deg(f)$ **is even:** *write both f and g in canonical form, they both have a leadings terms ax^d and bx^d (for some $a, b \in K$ and $d = \frac{\deg(f)}{2}$) and we set $r(\mathcal{O}) = \frac{a}{b}$.*

$\deg(f) = \deg(g)$ **and** $\deg(f)$ **is odd:** *write both f and g in canonical form, they both have a leadings terms ayx^d and byx^d (for some $a, b \in K$ and $d = \frac{\deg(f)-3}{2}$) and we again set $r(\mathcal{O}) = \frac{a}{b}$.*

Remark 3.16. *It might seem natural to define the degree of a rational function $r = \frac{f}{g}$ as $\deg(f) - \deg(g)$. Then the value at $\mathcal{O}$ depends on the sign of this degree. But this differes from the usual definition of degree of a rational function in algebraic geometry. So we dont define the degree of a rational function at all.*

Example 3.17. *For*

$$r(x,y) = \frac{x^3 + 2x + y + 2x^4 y}{x + x^2 + 5xy^3}$$

one can write

$$r(x,y) = \frac{x^3 + 2x + y + 2x^4 y}{x + x^2 + 5xy(x^3 + Ax + B)} = \frac{(x^3 + 2x) + y(1 + 2x^4)}{(x + x^2) + y(5x^4 + 5Ax^2 + 5Bx)}$$

This representant has a nominator degree of $\max\{2 \cdot 3, 3 + 2 \cdot 4\} = 11$ *and a denominator degree of* $\max\{2 \cdot 2, 3 + 2 \cdot 4\} = 11$ *which are both odd. So* $r(\mathcal{O}) = \frac{2}{5}$.

Proposition 3.18. *For $r, s \in K(E)$ s.t. $r(\mathcal{O})$ and $s(\mathcal{O})$ are finite then it holds that:*

$$(r \cdot s)(\mathcal{O}) = r(\mathcal{O}) s(\mathcal{O})$$

and

$$(r + s)(\mathcal{O}) = r(\mathcal{O}) + s(\mathcal{O})$$

4 Zeros and Poles

Definition 4.1 (Zero and Poles)**.** *Let $r \in K(E)$. We say that r has a zero at $P \in E$ if $r(P) = 0$ and that it has a pole at P if $r(P)$ is not finite.*

In the following we will define the multiplicity of a zero and a pole. It is motivated by multiplicities of zeros in analysis of functions in one variable: Consider the elliptic curve $E = E_{1,0}$ which therefore is given by the equation

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

then $P = (0,0) \in E$. First notice, that P is a zero of the functions x and y. But between this two functions, there is the relation $x = y^2 - x^3$. In the analytic sense, when $x \to 0$ the term x^3 can be neglected so we whould say something like "the function x has a zero at P whose multiplicity is twice that of the zero of y at P". So lets formalize:

"f f&nz" $:\Leftrightarrow$ f is finite and non-zero

Definition 4.2 (Uniformizer)**.** *For an elliptic curve E let $P \in E$ be a point. $u \in K(E)$ with $u(P) = 0$ is called a uniformizer at P if it has the following property: $\forall r \in K(E) \setminus \{0\} : \exists d \in \mathbb{Z}, s \in K(E)$ finite at P with $s(P) \neq 0$ s.t.*

$$r = u^d \cdot s$$

Stehen lassen

Lemma 4.3 (Uniformizer in generic case)**.** *Let E be an elliptic curve and $P \in E$ be finite and not of order two. Then for $P = (a,b)$ the function $u(x,y) := x - a$ is a uniformizer at P.*

Proof. First note that $u(a,b) = 0$. Now let $r \in K(E) \setminus \{0\}$ be arbitrary. If r has neither a zero nor a pole at P we can take $d = 0$ and $s = r$ and see that u is immaterial. So first let $r(P) = 0$. We now can write $r = \frac{f}{g}$ with $f(P) = 0$ and $g(P) \neq 0$. If we can decompose $f = u^d s$ as above then we can calculate

$$r = \frac{f}{g} = \frac{u^d s}{g} = u^d \frac{s}{g} = u^d \tilde{s}(x)$$

and we found $\tilde{s} := \frac{s}{g} \in K(E)$ as needed.

Put $s_0(x,y) := f(x,y)$ and repeat the following process (beginning with $i = 0$) while $s_i(P) = 0$: write $s_i(x,y) = v_i(x) + y w_i(x)$ in canonical form. Distinguish the cases $\overline{s_i}(P) = 0$ and $\overline{s_i}(P) \neq 0$:

Case $\overline{s_i}(P) = 0$: Since $y(P) = b \neq 0$ the system of linear equations

$$\begin{array}{rcrcl} v_i(a) & + & b w_i(a) & = & 0 \\ v_i(a) & - & b w_i(a) & = & 0 \end{array}$$

has rank 2 (which is less then the characteristic) and therefore yields $v_i(a) = w_i(a) = 0$. Now we can write

$$s_i(x,y) = v_i(x) + y w_i(x) = (x-a) v_{i+1}(x) + (x-a) y w_{i+1}(x) = (x-a) s_{i+1}(x,y)$$

for $s_{i+1}(x,y) = v_{i+1}(x) + y w_{i+1}(x)$ and feasible polynomials $v_{i+1}, w_{i+1} \in K[E]$.

Case $\overline{s_i}(P) \neq 0$**:** Multiply s_i by $1 = \frac{\overline{s_i}}{\overline{s_i}}$ to get

$$s_i(x,y) = \frac{N_{s_i}(x)}{\overline{s_i}(x,y)}$$

Now $s_i(P) = 0$ and $\overline{s_i}(P) \neq 0$ implies that $N_{s_i}(a) = 0$ so we can write $N_{s_i}(x) = (x-a)n(x)$ and with $s_{i+1}(x,y) := \frac{n(x)}{\overline{s_i}(x,y)}$ (which is finite at P) we again get

$$s_i(x,y) = \frac{N_{s_i}(x)}{\overline{s_i}(x,y)} = \frac{(x-a)n_{i+1}(x)}{\overline{s_i}(x,y)} = (x-a)s_{i+1}(x,y)$$

If this process terminates, we end up with

$$f(x,y) = (x-a)^i s_i(x,y)$$

where $s := s_i$ is finite and nonzero. With $x - a = u(x,y)$ and $d := i$ this is the desired decomposition: $f = u^d s$.

Since s_i is a rational function, not a polynomial, its not clear that this process terminates. To show it anyhow calculate:

$$\begin{aligned} N_f(x) &= N_{u^i s_i}(x) \\ &= \left((x-a)^i v_i(x)\right)^2 - s(x)\left((x-a)^i w_i(x)\right)^2 \\ &= (x-a)^{2i}\left(v_i^2(x) - s(x)w_i^2(x)\right) \\ &= (x-a)^{2i} N_{s_i}(x) \end{aligned}$$

so we have that $\deg_x(N_f) = 2i + \deg_x(N_{s_i})$ and since $\deg_x(N_{s_i}) > 0$ this implies that $\deg_x(N_f) > 2i$, so $2i$ is bound by a finite number.

Thus if r has a zero at P we are done. If r has no zero and no pole we are done too and in the case where r has a pole at P, $\frac{1}{r}$ has a zero and we can take the same u with a negative d and are done too. □

Lemma 4.4 (Uniformizer at points of order two)**.** *Let E be an elliptic curve and $P := \Omega_i \in E$ be of order two, then $u(x,y) := y$ is a uniformizer at Ω_i.*

Proof. W.l.o.g. we can take $i = 1$. Then note that $u(P) = 0$ and let $r \in K(E) \setminus \{0\}$ be arbitrary with $r(P) = 0$ so it has the form $r = \frac{f}{g}$ with $f(P) = 0$ which implies $v(\omega_1) = 0$ where $f(x,y) = v(x) + yw(x)$ is in canonical form. Hence v has a linear factor: $v(x) = (x-\omega_1)v_1(x)$ for some polynomial v_1. Since the three roots of s are different we can write

$$\begin{aligned} f(x,y) &= (x-\omega_1)v_1(x) + yw(x) \\ &= \tfrac{(x-\omega_1)(x-\omega_2)(x-\omega_3)v_1(x) + yw_1(x)}{(x-\omega_2)(x-\omega_3)} \\ &= \tfrac{y^2 v_1(x) + yw_1(x)}{(x-\omega_2)(x-\omega_3)} \\ &= y \cdot \tfrac{yv_1(x) + w_1(x)}{(x-\omega_2)(x-\omega_3)} \\ &= u(x,y) \cdot W(x,y) \end{aligned}$$

where $w_1(x) := w(x)(x-\omega_2)(x-\omega_3)$ and $W(x,y) := \frac{yv_1(x)+w_1(x)}{(x-\omega_2)(x-\omega_3)}$. If $W(P) \neq 0$ we are done, otherwise we can repeat the process with W, but this is only neccessary finitle many times since v can only contain finitly many factors. □

Lemma 4.5 (Uniformizer at $\mathcal{O}$)**.** *Let E be an elliptic curve then the function $u(x,y) := \frac{x}{y}$ is a uniformizer at $\mathcal{O} \in E$.*

Proof. Since $\deg(y) = 3 > 2 = \deg(x)$ it follows that $u(\mathcal{O}) = 0$. Now let $r = \frac{f}{g} \in K(E) \setminus \{0\}$ be arbitrary with $r(\mathcal{O}) = 0$ or not finite at $\mathcal{O}$, which means that $d := \deg(g) - \deg(f) \neq 0$. We want to take $s(x,y) = \left(\frac{y}{x}\right)^d r(x,y)$ which now needs to be finite and non-zero at $\mathcal{O}$ because then we see

$$r(x,y) = \left(\frac{x}{y}\right)^d \left(\left(\frac{y}{x}\right)^d r(x,y)\right) = u^d(x,y)s(x,y)$$

But because

$$\begin{aligned} & \deg(y^d f(x,y)) - \deg(x^d g(x,y)) \\ \overset{\text{Prop. 3.14}}{=} & (\deg(y^d) + \deg(f)) - (\deg(x^d) + \deg(g)) \\ \overset{\text{Def. 3.11}}{=} & 3d + \deg(f) - 2d - \deg(g) \\ = & d + (\deg(f) - \deg(g)) = 0 \end{aligned}$$

which implies that $s(x,y) = \frac{y^d f(x,y)}{x^d g(x,y)}$ is indeed finite and non-zero. □

Theorem 4.6 (Uniformizer theorem)**.** *Every point on an elliptic curve has a uniformizer and the number d in Def. 4.2 does not depend on it's choice.*

Proof. Lemma 4.3, 4.4 and 4.5 together yield the existence of a uniformizer for every point. So its only left to show that d does not depend on it's choice: Let u and $\tilde{u}$ be uniformizers at P then we can write especially $u = \tilde{u}^a q$ and $\tilde{u} = u^b p$ for $a, b \in \mathbb{Z}$ and $q, p \in K(E)$ are both finite and non-zero at P. After calculating

$$u = \tilde{u}^a q = \left(u^b p\right)^a q = u^{ab}(p^a q)$$

we assume $ab \neq 1$, divide by u and get $1 = u^{ab-1}(p^a q)$ which, evaluated at P leads to $1 = 0$, so $ab = 1$ and $a = b = \pm 1$. If $a = b = -1$ we get

$$u = \tilde{u}^{-1} q \iff u\tilde{u} = q$$

which, evaluated at P yields $0 = u(P)\tilde{u}(P) = q(P) \neq 0$. So it holds that $a = b = 1$. Now let $r \in K(E) \setminus \{0\}$ be arbitrary, because u and $\tilde{u}$ are uniformizers, there exists $d, \tilde{d} \in \mathbb{Z}$ and $s, t \in K(E)$ finite an non-zero at P with $r = u^d s$ and $r = \tilde{u}^{\tilde{d}} t$. Now we calculate

$$u^d s = \tilde{u}^{\tilde{d}} t = (up)^{\tilde{d}} t = u^{\tilde{d}}(p^{\tilde{d}} t)$$

which yields

$$u^{d-\tilde{d}} = \frac{p^{\tilde{d}} t}{s}$$

On the right side are only rational functions which are finite and non-zero at P but if $d - \tilde{d} \neq 0$ the left side is zero at P. So $d = \tilde{d}$. □

Now that we know that uniformizers at a point always yield the same d we can make the following definition:

Definition 4.7 (Order of a rational function)**.** *For an elliptic curve E let $P \in E$ be a point and u an uniformizer at P. For $r \in K(E) \setminus \{0\}$ with $r = u^d \cdot s$ we call d the order of r at P and write*

$$\mathrm{ord}_P(r) =: d$$

The multiplicity of a zero is the order at that point and the multiplicity of a pole is the negative of the order.

machen!

Remark 4.8. *This definition of order at a zero agress with the well known definition of order of a zero of a polynomial in one variable in the case that the zero does not corresponde to a point of order two: Let $f \in K[X]$ with*

$$f(x) = g(x) \cdot (x - a)^k$$

for $g \in K[X]$ with $g(a) \neq 0$, $k \in \mathbb{N}_{>0}$ and $a \in K$. We whould now say that f has a zero of order k at a. Now see f as a polynomial $f \in K[E]$ and pick a uniformizer u at $P = (a, s(a))$ (which is a point on E, by assumption not of ordet two and a root of f), for instance $u(x,y) = x - a$, and write f as:

$$f(x,y) = u^d(x,y) \cdot s(x,y) = (x-a)^d \cdot g(x)$$

which implies $k = d = \mathrm{ord}_P(f)$.

However, when $a = \omega_i$ (w.l.o.g. $i = 1$) we see that $P = (a, s(a)) = (a, 0)$ is a zero of order $2k$ of f since with the uniformizer $u(x,y) = y$ at P and the rational function $s(x,y) := \frac{g(x)}{(x-\omega_2)^k (x-\omega_3)^k}$ we write:

$$\begin{aligned} f(x,y) &= u^d(x,y) \cdot s(x,y) \\ &= y^d \cdot \tfrac{g(x)}{(x-\omega_2)^k (x-\omega_3)^k} \\ &= y^d \cdot \tfrac{(x-a)^k g(x)}{(x-\omega_1)^k (x-\omega_2)^k (x-\omega_3)^k} \\ &= y^d \cdot \tfrac{(x-a)^k g(x)}{y^{2k}} \end{aligned}$$

so $(x-a)^k \cdot g(x) = f(x,y) = y^d \cdot \frac{(x-a)^k g(x)}{y^{2k}}$ which implies $d = 2k$.

Proposition 4.9 (Order at finite non-root)**.** *Let $r \in K(E)$ and $P \in E$ s.t. $r(P) \neq 0$ and r is finite at P then:*

$$\mathrm{ord}_P(r) = 0$$

Proof. Pick a uniformizer at P, take $s(x,y) = r(x,y)$ (which is finite and non-zero at P) and write

$$r(x,y) = u^0(x,y) r(x,y) = u^d(x,y) s(x,y)$$

i.e. $\mathrm{ord}_P(f) = d = 0$. □

Proposition 4.10 (Order of polynomials at non-root)**.** *Let $f \in K[E]$ and $P \in E \setminus \{\mathcal{O}\}$ s.t. $f(P) \neq 0$ then:*

$$\mathrm{ord}_P(f) = 0$$

Proof. Since polynomials dont have finite roots, this follows from Prop. 4.9. □

Proposition 4.11 (Order of polynomials at $\mathcal{O}$)**.** *For $f \in K[E] \setminus \{0\}$:*

$$\mathrm{ord}_{\mathcal{O}}(f) = -\deg(f)$$

Proof. $u(x,y) = \frac{x}{y}$ is a uniformizer at $\mathcal{O}$ by Lemma 4.5. With $k := \deg(f)$ we take $s(x,y) = \frac{x^k}{y^k} f(x,y)$. Because $\deg(x^k \cdot f(x,y)) \overset{\text{Prop. 3.14}}{=} 2k + \deg(f) = 3k$ and $\deg(y^k) = 3k$ we know that s is finite and non-zero and can write

$$f(x,y) = u^d(x,y)s(x,y) = \left(\frac{x}{y}\right)^d \frac{x^k}{y^k} f(x,y)$$

which implies that $d = -k = -\deg(f)$. □

Proposition 4.12 (Property of order of rational functions)**.** *For $r_1, r_2 \in K(E)$ and $P \in E$:*

$$\mathrm{ord}_P(r_1 \cdot r_2) = \mathrm{ord}_P(r_1) + \mathrm{ord}_P(r_2)$$

Proof. Let $P \in E$ and pick a unformizer u at P. We now get numbers $d, d_1, d_2 \in \mathbb{Z}$ and at P finite and non-zero rational functions $s, s_1, s_2 \in K(E)$ s.t.

$$\begin{aligned} r_1 \cdot r_2 &= u^d \cdot s \\ r_1 &= u^{d_1} \cdot s_1 \\ r_2 &= u^{d_2} \cdot s_2 \end{aligned}$$

and can calculate

$$u^d \cdot s = r_1 \cdot r_2 = \left(u^{d_1} \cdot s_1\right) \cdot \left(u^{d_2} \cdot s_2\right) = u^{d_1 + d_2} \cdot s_1 \cdot s_2$$

and since Thm. 4.6 it follows that

$$\mathrm{ord}_P(r_1 \cdot r_2) = d = d_1 + d_2 = \mathrm{ord}_P(r_1) + \mathrm{ord}_P(r_2)$$

□

Example 4.13. *Let $P = (a,b) \in E$ with $b \neq 0$ i.e. P finite and not of order two. We now want to calculate the orders of $r(x,y) = x - a$ at all points $Q \in E$ where $r(Q)$ is not finite or zero (at all other points it holds that $\mathrm{ord}_Q(r) = 0$):*

$Q = P$ **or** $Q = P' := (a, -b) \neq P$**:** *Take a uniformizer u at Q, since r itself is a uniformizer it follows that $r = u^d \cdot s = r^1 \cdot 1$ and $\mathrm{ord}_Q(r) = d = 1$.*

$Q = \mathcal{O}$**:** *Take a uniformizer $u(x,y) = \frac{x}{y}$ at Q and $s(x,y) = \frac{x^3 - ax^2}{y^2}$ (note $s(Q) = 1$)*

$$u^d(x,y) \cdot s(x,y) = \left(\frac{x}{y}\right)^{-2} s(x,y) = \frac{y^2}{x^2} \frac{x^3 - ax^2}{y^2} = x - a = r(x,y)$$

and $\mathrm{ord}_Q(r) = d = -2$.

Summing up we see that r has two simple zeros and a single double pole.

Example 4.14. *Now consider $r(x,y) := y$ since $u(x,y) = y$ is a uniformizer at the three points of order two we have $\operatorname{ord}_{\Omega_i}(r) = 1$. At every other finite point r has order zero. In $\mathcal{O}$ we can take $u(x,y) = \frac{x}{y}$ as a uniformizer and with $s(x,y) = \frac{x^3 y}{y^3}$ (which is finite at $\mathcal{O}$) it follows that:*

$$u^d(x,y) \cdot s(x,y) = \left(\frac{x}{y}\right)^{-3} \cdot s(x,y) = \frac{y^3}{x^3} \cdot \frac{x^3 y}{y^3} = y = r(x,y)$$

and $\operatorname{ord}_{\mathcal{O}}(r) = d = -3$. Summing up we see that r has three simple zeros and a single tripple pole.

Example 4.15. *What about $r(x,y) = \frac{x}{y}$? Since $\deg(x) = 2 < 3 = \deg(y)$ it holds that $r(\mathcal{O}) = 0$ to obtain the order we take $u(x,y) = \frac{x}{y}$ as a uniformizer at $\mathcal{O}$ and calculate for $s(x,y) = 1$ that*

$$u^d(x,y) \cdot s(x,y) = \left(\frac{x}{y}\right)^1 \cdot 1 = r(x,y)$$

and get $\operatorname{ord}_{\mathcal{O}}(r) = 1$. Now distinguish the two cases:

$B \neq 0$: *The two points $P_\pm := (0, \pm\sqrt{B})$ are zeros of r. To calculate the multiplicity we take $u(x,y) = x$ as a uniformizer at $P_\pm$, $s(x,y) := \frac{1}{y}$ (which is finite and nonzero for $y = \pm\sqrt{B}$ and calculate*

$$\frac{x}{y} = r(x,y) = u^d(x,y)s(x,y) = x^d \frac{1}{y}$$

to optain $\operatorname{ord}_{P_\pm}(r) = d = 1$. Furthermore r is not finite at all points of order two Ω_i: We take a uniformizer $u(x,y) = y$ at Ω_i, $s(x,y) := x$ (which is finite and nonzero at Ω_i since $B \neq 0$ and Prop. 2.5 implies that $\omega_i \neq 0$) and calculate

$$\frac{x}{y} = r(x,y) = u^d(x,y)s(x,y) = y^d x$$

to get $\operatorname{ord}_{\Omega_i}(r) = d = -1$. So summing up, we get three zeros of order one and three poles of order one.

$B = 0$: *An elliptic curve $E_{A,0}$ is given by*

$$y^2 = x^3 + Ax = x\left(x - \sqrt{-A}\right)\left(x + \sqrt{-A}\right)$$

so we get $\omega_1 = 0$, $\omega_2 = \sqrt{-A}$ and $\omega_3 = \sqrt{A}$ as the three points of order two. First note, that Ω_2 and Ω_3 are poles of r, since $\omega_2 \neq 0$ and $\omega_3 \neq 0$. To optain the order, we take $u(x,y) = y$ as a uniformizer, $s(x,y) = x$ (which is finite and nonzero) and calculate:

$$\frac{x}{y} = r(x,y) = u^d(x,y)s(x,y) = y^d x$$

to optain $\mathrm{ord}_{\Omega_2}(r) = \mathrm{ord}_{\Omega_3}(r) = d = -1$*. Furthermore we calculate*

$$r(x,y) = \frac{x}{y} = \frac{xy}{y^2} = \frac{xy}{x\left(x-\sqrt{-A}\right)\left(x+\sqrt{-A}\right)} = \frac{y}{\left(x-\sqrt{-A}\right)\left(x+\sqrt{-A}\right)}$$

and therefore get, that $(0,0)$ *is a zero of* r*. To optain the order at* $(0,0)$ *we take the uniformizer* $u(x,y) = y$ *and calculate*

$$\frac{y}{\left(x-\sqrt{-A}\right)\left(x+\sqrt{-A}\right)} = r(x,y) = u^d(x,y)s(x,y) = y^d \frac{1}{\left(x-\sqrt{-A}\right)\left(x+\sqrt{-A}\right)}$$

with $s(x,y) = \frac{1}{\left(x-\sqrt{-A}\right)\left(x+\sqrt{-A}\right)}$ *and get* $\mathrm{ord}_{(0,0)}(r) = d = 1$*. So summing up, we get two simple zeros and two simple poles.*

The three examples 4.13, 4.14 and 4.15 suggest that the sum of orders over all points is zero, which is sort of a baby Riemann-Roch Theorem. To prove this, we need the following lemma:

Lemma 4.16 (Sum of multiplicities of roots equal degree)**.** *For* $f \in K[E]$*:*

$$\deg(f) = \sum_{\substack{P\in E\\ f(P)=0}} \mathrm{ord}_P(f)$$

Proof. Define $n \coloneqq \deg(f)$. By Lemma 3.13 it follows that $n = \deg_x(N_f)$. We can write

$$\left(f\overline{f}\right)(x) = N_f(x) = \prod_{i=1}^{n}(x-a_i)$$

with not necessarily different a_is. By Rem. 4.8 it follows that dependent on whether $(a_i,0)$ is of order two or not the factor $(x-a_i)$ has two distinct roots on E (namely $(a_i, \pm\sqrt{s_{A,B}(a_i)})$) or one double one. So, counting multiplicities, we get that $f\overline{f}$ has exactly $2n$ roots on E. Since f and $\overline{f}$ have the same number of roots on E, f has exactcle n roots (again counting multiplicities), which is a synonym for the right side of the above equation. □

Theorem 4.17 (Sum of orders is zero)**.** *For* $r \in K(E)$*:*

$$\sum_{P\in E} \mathrm{ord}_P(r) = 0$$

Proof. Since for $r = \frac{h}{g} \in K(E)$ it holds that

$$\sum_{P\in E} \mathrm{ord}_P(r) = \sum_{P\in E} \mathrm{ord}_P(h) - \sum_{P\in E} \mathrm{ord}_P(g)$$

for any $P \in E$, it suffices to show the result for a polynomial $f \in K[E]$. One can calculate

$$\sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(f) \overset{\text{Prop. 4.10}}{=} \sum_{\substack{P\in E\\ f(P)=0}} \mathrm{ord}_P(f) \overset{\text{Lemma 4.16}}{=} \deg(f)$$

On the other hand by Prop. 4.11 the order of f at $\mathcal{O}$ is $-\deg(f)$ which yields the result. □

Lemma 4.18. *Let f be a nonconstant polynomial on E, then f must have at least two simple zeros or one double zero at finite points of E.*

Proof. Since f is not constant, it contains an x or a y. Since $\deg(x) = 2$ and $\deg(y) = 3$ the result follows from Lemma 4.16. □

Lemma 4.19. *If two rational function agree on an infinite number of points of E (which is possible since E is infinite by Prop. 2.7), they are equal.*

Proof. Let $f, g \in K(E)$ with $f(P) = g(P)$ for infinitely many $P \in E$ and define $h := f - g$, which therefore has infinitely many zeros. Since $\operatorname{ord}_P(h) > 0$ for a zero $P \in E$ the sum

$$\sum_{\substack{P \in E \\ f(P)=0}} \operatorname{ord}_P(f)$$

is not finite. But if h is not the zero-polynomial $\deg(h)$ is finite which whould contradict Lemma 4.16. □

Lemma 4.20. *A rational function without a finite pole is a polynomial.*

Proof. Write an $r \in K(E)$ without poles in canonical form $r(x, y) = a(x) + yb(x)$ with $a, b \in K(x)$ (Rem. 3.9).

$$\begin{aligned}
& r \text{ has no finite pole} \\
\Rightarrow\ & \bar{r} = a - yb \text{ has no finite pole} \\
\Rightarrow\ & r + \bar{r} = 2a \text{ has no finite pole} \\
\Rightarrow\ & yb = r - a \text{ has no finite pole} \\
\Rightarrow\ & (yb)^2 = sb^2 \text{ has no finite pole}
\end{aligned}$$

If b has a pole, b^2 has a double pole. But sb^2 has no finite pole, hence s has a double zero which contradicts the definition of elliptic curve 2.2. □

Definition 4.21 (Rational map)**.** *A pair of rational functions $(u, v) \in K(E_{A,B})$ is called rational map if*

$$v^2 = u^3 + Au + B$$

Remark 4.22. *Because of the relation between u and v of a rational map $F = (u, v)$ it holds for every $P \in E$:*

$$u(P) \text{ is (not) finite} \Leftrightarrow v(P) \text{ is (not) finite}$$

When we make the convention that $F(P) = \mathcal{O}$ if u and v are not finite at P we see that F defines a map $E \to E$ by $P \mapsto (u(P), v(P))$.

Remark 4.23. *Given a field K, form the elliptic curve E using the equation from Def. 2.2:*

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

and consider the field of rational funtions over E, namely $K(E)$ and use the same equation to define an elliptic curve over that field, denoted by $E(K(E))$. Since $K(E)$ may not be algebraically closed, the points of $E(K(E))$ may have coordinates in the algebraic closure of $K(E)$. The $K(E)$-rational points (Def. 2.8) of $E(K(E))$ are exactly the rational maps. We think of the identity of this curve, call it $\mathcal{O}_M$, as the map with constant value $\mathcal{O}$.

5 Divisors and Lines

nearly every result from the last lecture only holds for non-zero functions

To store the zeros and poles of a rational function (together with their degree), we will use a formal sum. For this we recall the definition of a free abelian group:

Definition 5.1 (Free abelian group)**.** *Let S be a set. The free abelian group $\mathscr{F}_S$ generated by S is the set of formal linear combinations*

$$\sum_{s \in S} \lambda(s) \cdot \langle s \rangle$$

where $\lambda : S \to \mathbb{Z}$ and $\lambda(s) = 0$ for almost all $s \in S$ (i.e. for all $s \in S$ except of finitely many) together with the formal addition of two such formal linear combinations.

Definition 5.2 (Divisor)**.** *For a elliptic curve E we definie the group of divisors of E by*

$$\operatorname{Div}(E) := \mathscr{F}_E$$

For a divisor $\Delta = \sum_{P \in E} \lambda(P) \cdot \langle P \rangle \in \operatorname{Div}(E)$ we define the degree of Δ as

$$\deg(\Delta) := \sum_{P \in E} \lambda(P)$$

and the norm of Δ as

$$|\Delta| := \sum_{P \in E \setminus \{\mathcal{O}\}} |\lambda(P)|$$

Fact 5.3. *A Divisor of norm 1 has the form $\pm\langle P \rangle + n\langle \mathcal{O} \rangle$ for $n \in Z$.*

Proposition 5.4 (Property of divisor degree)**.** *For $\Delta_1, \Delta_2 \in \operatorname{Div}(E)$:*

nicht machen

$$\deg(\Delta_1 + \Delta_2) = \deg(\Delta_1) + \deg(\Delta_2)$$

Proof. Note that for $\Delta_i = \sum_{P \in E} \lambda_i(P)\langle P \rangle$ the sum $\Delta_1 + \Delta_2$ is again a formal sum, hence a divisor and one can calculate:

$$\begin{aligned} \deg(\Delta_1 + \Delta_2) &= \deg\left(\textstyle\sum_{P \in E} \lambda_1(P)\langle P \rangle + \sum_{P \in E} \lambda_2(P)\langle P \rangle\right) \\ &\overset{\text{finite sums}}{=} \deg\left(\textstyle\sum_{P \in E} (\lambda_1(P) + \lambda_2(P))\langle P \rangle\right) \\ &\overset{\text{Def. 5.2}}{=} \textstyle\sum_{P \in E} (\lambda_1(P) + \lambda_2(P)) \\ &\overset{\text{finite sums}}{=} \textstyle\sum_{P \in E} \lambda_1(P) + \sum_{P \in E} \lambda_2(P) \\ &\overset{\text{Def. 5.2}}{=} \deg(\Delta_1) + \deg(\Delta_2) \end{aligned}$$

□

Definition 5.5 (Associated divisor)**.** *For a rational function $r \in K(E) \setminus \{0\}$ we define the associated divisor by*

$$\operatorname{div}(r) = \sum_{P \in E} \operatorname{ord}_P(r) \cdot \langle P \rangle$$

Remark 5.6. *A rational function has a finite number of zeros and poles by Lemma 4.16 so the associated divisor is well-defined.*

Fact 5.7. *Constant non-zero functions have divisor* 0.

The Divisor of a rational function is a possibility to write down all information about poles and zeros of a rational functions i.e. the positions and multiplicities.

Fact 5.8. *For* $f \in K[E]$*:*

$$|\operatorname{div}(f)| \overset{\text{Def. 5.2}}{=} \sum_{P \in E \setminus \{\mathcal{O}\}} \operatorname{ord}_P(f) \overset{\text{Prop. 4.10}}{=} \sum_{\substack{P \in E \\ f(P)=0}} \operatorname{ord}_P(f) \overset{\text{Lemma 4.16}}{=} \deg(f)$$

Definition 5.9. *Let* $r \in K(E)$*, then the* <u>*leading coefficient*</u> *is defined by* **weg lassen**

$$\operatorname{lc}(r) := \left[\left(\frac{x}{y} \right)^{\operatorname{ord}_{\mathcal{O}}(r)} \cdot r \right] (\mathcal{O})$$

Example 5.10. *Let* $r(x,y) = \frac{2x^2+7x}{3yx+2}$*. With the uniformizer* $\frac{x}{y}$ *at* $\mathcal{O}$ *(Lemma 4.5) and*

$$\left(\frac{x}{y} \right)^{-1} r(x,y) = \frac{2yx^2 + 7yx}{3yx^2 + 2x}$$

we get $\deg_{\mathcal{O}}(r) = -1$*. Evaluating at* $\mathcal{O}$ *yields* $\operatorname{lc}(r) = \frac{2}{3}$ *which makes perfect sense with our intuition of what a leading coefficient should be.*

Proposition 5.11. *If two rational functions have the same divisor, their quotient is constant.*

<u>Proof.</u> Let $r_1, r_2 \in K(E)$ with $\operatorname{div}(r_1) = \operatorname{div}(r_2)$, so they have the same roots and the same poles (with same multiplicities). If $\operatorname{div}(r_1)$ (and hence $\operatorname{div}(r_2)$) has no finite poles, Lemma 4.20 implies that r_1 and r_2 are polynomials, which additionally have same degree (by Lemma 4.16) and the same roots, which implies that they are equal und the quotient is 1 which is constant. Now assume that $\operatorname{div}(r_1)$ has a finite pole, say $P \in E$ of order m. Pick a uniformizer u at P and write

$$\frac{r_1}{r_2} = \frac{u^m s_1}{u^m s_2} = \frac{s_1}{s_2}$$

for $s_1, s_2 \in K(X,Y)$ finite and non-zero at P. So $\frac{s_1}{s_2}$ is finite and non-zero at P, hence is$\frac{r_1}{r_2}$. Since this works for every finite pole P by Lemma 4.20 again $\frac{r_1}{r_2}$ is a polynomial, which is possible only if r_1 is a multiple of r_2. ☐

Thus we can check if two rational functions are equal if they have the same divisor and agree at any point on E for example $\mathcal{O}$. If the two functions have a pole at $\mathcal{O}$ we can compare their leading coefficients:

Lemma 5.12. *Two rational functions with the same divisor and leading coefficient are equal.*

Proof. Let $r_1, r_2 \in K(E)$ be two rational function with the same divisor and leading coefficient. We know that

$$\begin{aligned}
0 &= \mathrm{lc}(r_1) - \mathrm{lc}(r_2) \\
&\overset{\text{Def. 5.9}}{=} \left[\left(\frac{x}{y}\right)^{\mathrm{ord}_{\mathcal{O}}(r_1)} r_1\right](\mathcal{O}) - \left[\left(\frac{x}{y}\right)^{\mathrm{ord}_{\mathcal{O}}(r_2)} r_2\right](\mathcal{O}) \\
&\overset{d:=\mathrm{ord}_{\mathcal{O}}(r_1)=\mathrm{ord}_{\mathcal{O}}(r_2)}{=} \left[\left(\frac{x}{y}\right)^{d} r_1\right](\mathcal{O}) - \left[\left(\frac{x}{y}\right)^{d} r_2\right](\mathcal{O}) \\
&\overset{\text{Prop. 3.18}}{=} \left[\left(\frac{x}{y}\right)^{d} r_1 - \left(\frac{x}{y}\right)^{d} r_2\right](\mathcal{O}) \\
&= \left[\left(\frac{x}{y}\right)^{d} (r_1 - r_2)\right](\mathcal{O})
\end{aligned}$$

Since Prop. 5.11 we have $r_1 = c \cdot r_2$ which implies

$$\begin{aligned}
0 &= \left[\left(\frac{x}{y}\right)^{d} (c \cdot r_2 - r_2)\right](\mathcal{O}) \\
&= \left[\left(\frac{x}{y}\right)^{d} (c-1) \cdot r_2\right](\mathcal{O}) \\
&\overset{\text{Prop. 3.18}}{=} (c-1)\left[\left(\frac{x}{y}\right)^{d} \cdot r_2\right](\mathcal{O})
\end{aligned}$$

which implies $c = 1$ and therefore $r_1 = r_2$. □

Example 5.13. *1. Let $P = (a,b), P' = (a,-b) \in E$ with $b \neq 0$ and $r(x,y) = x - a$. With Exa. 4.13 we see that*

$$\mathrm{div}\,(r) = \langle P \rangle + \langle P' \rangle - 2\langle \mathcal{O} \rangle$$

2. Let $P_i = (\omega_i, 0) \in E$ and $r(x,y) = y$. With Exa. 4.14 we see that

$$\mathrm{div}\,(r) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \mathcal{O} \rangle$$

3. Let $Q = (0, \sqrt{B}), Q' = (0, -\sqrt{B}) \in E_{A,B}$ and $r = \frac{x}{y}$. With Exa. 4.15 we see that for $B \neq 0$:

$$\mathrm{div}\,(r) = \langle Q \rangle + \langle Q' \rangle - \langle P_1 \rangle - \langle P_2 \rangle - \langle P_3 \rangle + \langle \mathcal{O} \rangle$$

Definition 5.14 (Principal divisors)**.** *$\Delta \in \mathrm{Div}\,(E)$ is called principal if:*

$$\exists r \in K(E): \ \Delta = \mathrm{div}\,(r)$$

Furthermore we say that $\Delta_1, \Delta_2 \in \mathrm{Div}\,(E)$ are linearly equivalent or in the same divisor class if $\Delta_1 - \Delta_2$ is principal. We then write $\Delta_1 \sim \Delta_2$.

The following Proposition and Corrolar yield that $\sim$ is indeed an equivalents relation and that the set of principal divisors is a subgroup of $\mathrm{Div}\,(E)$:

Fact 5.15. *For $r_1, r_2 \in K(E)$ it holds:*

$$\mathrm{div}\,(r_1 \cdot r_2) = \mathrm{div}\,(r_1) + \mathrm{div}\,(r_2)$$

Proof. With Prop. 4.12 it directly follows from the Def. 5.2. □

Corrolar 5.16. *For $r \in K(E)$:*

1. $\operatorname{div}(-r) = \operatorname{div}(r)$
2. $-\operatorname{div}(r) = \operatorname{div}(\frac{1}{r})$

Proof.

1. $\operatorname{div}(-r) = \operatorname{div}((-1)\cdot r) \overset{\text{Fact 5.15}}{=} \operatorname{div}(-1) + \operatorname{div}(r) \overset{\text{Fact 5.7}}{=} \operatorname{div}(r)$
2. $0 \overset{\text{Fact 5.7}}{=} \operatorname{div}(1) = \operatorname{div}(\frac{r}{r}) = \operatorname{div}(\frac{1}{r}\cdot r) \overset{\text{Fact 5.15}}{=} \operatorname{div}(\frac{1}{r}) + \operatorname{div}(r)$

□

Definition 5.17. *We define the following two subgroups of* $\operatorname{Div}(E)$*:*

$$\operatorname{Prin}(E) := \{\Delta \in \operatorname{Div}(E) \mid \Delta \textit{ is principal }\}$$

and

$$\operatorname{Div}_0(E) := \{\Delta \in \operatorname{Div}(E) \mid \deg \Delta = 0\}$$

and the so called Picard group of E or divisor class group of E:

$$\operatorname{Pic}(E) := {}^{\operatorname{Div}(E)}/_{\operatorname{Prin}(E)}$$

Since Thm. 4.17 we know that $\operatorname{Prin}(E) \subseteq \operatorname{Div}_0(E)$ *and are able to define the degree zero part of the Picard group:*

$$\operatorname{Pic}_0(E) := {}^{\operatorname{Div}_0(E)}/_{\operatorname{Prin}(E)}$$

The goal of this chapter will be to show that $\operatorname{Pic}_0(E)$ and E itself are one-to-one.

Definition 5.18 (Line)**.** *A line on E is a polynomials of the form*

$$l(x,y) = \alpha x + \beta y + \gamma$$

with $\alpha, \beta, \gamma \in K$ and $\alpha \neq 0$ or $\beta \neq 0$. If $P \in E$ is a zero of l we say l goes through P and P is on l.

Proposition 5.19. *For $P_1, P_2 \in E$ finite with $P_1 \neq P_2$ there is a line through P_1 and P_2.*

Proof. With $P_i = (a_i, b_i)$ we find that

$$l(x,y) = \begin{cases} \frac{b_2-b_1}{a_2-a_1}(x-a_1) - (y-b_1) & \text{if } a_1 \neq a_2 \\ x - a_1 & \text{else} \end{cases}$$

defines a line with roots P_1 and P_2. □

The following special line through an arbitrary point will be very usefull:

Proposition 5.20. *For $P = (a, b) \in E$ finite and not of order two, the line*

$$l(x, y) = m(x - a) - (y - b)$$

with $m = \frac{3a^2+A}{2b}$ has a double zero at P and one other finite zero. In other words:

$$\exists Q \in E : \operatorname{div}(l) = 2\langle P\rangle + \langle Q\rangle - 3\langle \mathcal{O}\rangle$$

Proof. We clearly see, that $l(P) = 0$, we now want to show, that the order at P is 2: Let $u(x, y) = x - a$ be a uniformizer at P and write:

$$l(x, y) = (x - a)^2 s(x, y)$$

and $s(x, y) = \frac{l(x,y)}{(x-a)^2}$ has to be finite and non-zero at P. Let $g(x, y) := \frac{y-b}{x-a}$. Polynomial division and the fact that $b^2 = a^3 + Aa + B$ yield:

$$\begin{aligned} g(x, y) = \frac{y - b}{x - a} &= \frac{y^2 - b^2}{(x - a)(y + b)} \\ &= \frac{x^3 + Ax + B - b^2}{(x - a)(y + b)} \\ &= \frac{x^2 + ax + A + a^2}{y + b} \\ g(a, b) &= \frac{3a^2 + A}{2b} = m \end{aligned}$$

Now we calculate with $2mb = 3a^2 + A$:

$$\begin{aligned} s(x, y) &= \frac{m(x - a) - (y - b)}{(x - a)^2} \\ &= \frac{m}{x - a} - \frac{g(x, y)}{x - a} \\ &= \frac{m}{x - a} - \frac{\frac{x^2+ax+A+a^2}{x-a}}{y + b} \\ &= \frac{m\frac{y+b}{x-a}}{y + b} - \frac{x + 2a + \frac{A+3a^2}{x-a}}{y + b} \\ &= \frac{m\frac{y+b}{x-a} - x - 2a - \frac{2mb}{x-a}}{y + b} \\ &= \frac{m\frac{y-b}{x-a} - x - 2a}{y + b} \\ &= \frac{m \cdot g(x, y) - x - 2a}{y + b} \end{aligned}$$

Which, evaluated at P yields: $s(a, b) = \frac{m^2-3a}{2b}$ which is finite and non-zero at P.
□

Lemma 5.21 (Divisor of Line)**.** *Let l be a line:*

$$|\operatorname{div}(l)| \in \{2,3\}$$

Proof. $l(x,y) = \alpha x + \beta y + \gamma$ is a polynomial of degree 2 (if $\beta = 0$) or 3 (if $\beta \neq 0$). Hence by Lemma 4.16, the sum of multiplicities of the zeros of l is 2 or 3, which by Fact 5.8 is $|\operatorname{div}(l)|$. □

Proposition 5.22. *Let l be a line and $P_1, P_2, P_3 \in E$ pairwise distinct points on l, then one of the following holds:*

1. $\operatorname{div}(l) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \mathcal{O} \rangle$
2. $\operatorname{div}(l) = 2\langle P_1 \rangle + \langle P_2 \rangle - 3\langle \mathcal{O} \rangle$
3. $\operatorname{div}(l) = 3\langle P_1 \rangle - 3\langle \mathcal{O} \rangle$
4. $\operatorname{div}(l) = \langle P_1 \rangle + \langle P_2 \rangle - 2\langle \mathcal{O} \rangle$
5. $\operatorname{div}(l) = 2\langle P_1 \rangle - 2\langle \mathcal{O} \rangle$

In the contrary, there is a line for each of this divisors.

Proof. First we show that all possible divisors are given by 1-5. Since l is a polynomial, it has a pole at $\mathcal{O}$ and $\mathcal{O}$ is the only pole. By Prop. 4.11 $\operatorname{ord}_{\mathcal{O}}(l) = -\deg(l) \in \{-2, -3\}$. By Thm. 4.17 and combinatorial arguments we get for

case $\operatorname{ord}_{\mathcal{O}}(l) = -3$**:** there can only be

- three single roots (1. $\operatorname{div}(l) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \mathcal{O} \rangle$)
- one single root and one double root (2. $\operatorname{div}(l) = 2\langle P_1 \rangle + \langle P_2 \rangle - 3\langle \mathcal{O} \rangle$)
- one tripple root (3. $\operatorname{div}(l) = 3\langle P_1 \rangle - 3\langle \mathcal{O} \rangle$)

case $\operatorname{ord}_{\mathcal{O}}(l) = -2$**:** there can only be

- two single roots (4. $\operatorname{div}(l) = \langle P_1 \rangle + \langle P_2 \rangle - 2\langle \mathcal{O} \rangle$)
- one double root (5. $\operatorname{div}(l) = 2\langle P_1 \rangle - 2\langle \mathcal{O} \rangle$)

Now we show that all this divisors are possible.

Case $\operatorname{ord}_{\mathcal{O}}(l) = -3$:

three single roots For $l(x,y) = y$ we get:

$$\operatorname{div}(l) = \langle \Omega_1 \rangle + \langle \Omega_2 \rangle + \langle \Omega_3 \rangle - 3\langle \mathcal{O} \rangle$$

one single root and one double root Prop. 5.20

one tripple root We know that $P = (0, \sqrt{B}) \in E$ is a point on $l(x,y) = Ax - y + \sqrt{B}$. If $B \neq 0$ (which means that P is not of order two) we can take the uniformizer $u(x,y) = x$ and calculate **TODO**

Case $\text{ord}_{\mathcal{O}}(l) = -2$: Let $P = (a,b) \in E$ be finite and $l(x,y) := x - a$.

P **not of order two** Exa. 4.13 says that P and $(a,-b)$ are two single roots of L

P **of order two** W.l.o.g. $P = \Omega_1$. Pick the uniformizer $u(x,y) = y$ at P. Then we get for $d = 2$ and $s(x,y) = \frac{1}{(x-\omega_2)(x-\omega_3)}$ (which is finite and non-zero at P):

$$u^d(x,y)s(x,y) = \frac{y^2}{(x-\omega_2)(x-\omega_3)} = x - \omega_1 = r(x,y)$$

This says, that l has a double zero at P.

□

Notation 5.23. *Whenever we write an ? as a coefficient in a divisor, the statement in which the divisor occures is meant to be quantified with "it exists an integral ?". In other words: we are not interested in the special value of the coefficient.*

Theorem 5.24 (Linear Reduction)**.** *Let* $\Delta \in \text{Div}(E)$*. Then there exists* $\tilde{\Delta} \in \text{Div}(E)$ *with:*

- $\tilde{\Delta} \sim \Delta$
- $\deg(\tilde{\Delta}) = \deg(\Delta)$
- $|\tilde{\Delta}| \le 1$

Proof. The idea is, that we can, given an arbitrary divisor Δ, add or substract associated divisors of lines, listed in Prop. 5.22 to optain a divisor Δ_1. This operation will not change the linear equivalence class since

$$[\Delta_1 = \Delta \pm \text{div}(l)] \Leftrightarrow [\Delta_1 - \Delta = \text{div}(l) \text{ or } \Delta - \Delta_1 = \text{div}(l)] \Leftrightarrow [\Delta \sim \Delta_1]$$

and obtain the degree of Δ because

$$\deg(\Delta_1) \overset{\text{Prop. 5.4}}{=} \deg(\Delta) + \deg(l) \overset{\text{Thm. 4.17}}{=} \deg(\Delta)$$

We try to do it in a way, that the norm reduces.

So write $\Delta = \sum_{P \in E} \lambda(P)\langle P \rangle$. We first want to reduce Δ to a linear equivalent divisor Δ' of same degree, with an equal or lesser norm which can be written as:

$$\Delta' = n_1\langle P \rangle - n_2\langle Q \rangle + ?\langle \mathcal{O} \rangle \tag{1}$$

where $n_1, n_2 \in \mathbb{N}_{>0}$.

Suppose Δ is not of this form. If Δ contains only one finite point, say $\langle P \rangle$ and this point $P = (\omega, 0)$ is of order two, we can subtract or add (depending on the sign of $\langle P \rangle$ in Δ) the divisor of $l(x,y) := x - \omega$ which is $\langle l \rangle = 2\langle P \rangle - 2\langle \mathcal{O} \rangle$ and are finished. If P is not of order two, we can subtract or add the divisor of

l from Prop. 5.20 through P and get a norm-reduced divisor which is in form Equation 1 or contains at least two different points with the same sign.

So now suppose that we can take finite Q and R with $Q \neq R$ such that $\langle Q \rangle$ and $\langle R \rangle$ appear with nonzero coefficient of the same sign. Let l be a line through Q and R (Prop. 5.19). This line has two or three distinct roots.

If $\lambda(Q), \lambda(R) < 0$: Set $\Delta_1 := \Delta + \operatorname{div}(l)$

If $\lambda(Q), \lambda(R) > 0$: Set $\Delta_1 := \Delta - \operatorname{div}(l)$

For $\Delta_1 = \sum_{P \in E} \mu(P)\langle P \rangle$ we get $|\mu(Q)| = |\lambda(Q)| - 1$ and $|\mu(R)| = |\lambda(R)| - 1$ i.e. the norm of the coefficients of $\langle Q \rangle$ and $\langle R \rangle$ each decreases by one.

In the case where l has three distinct roots, we changed the coefficient of another $\langle S \rangle$ for a finite point $S \in E$ in Δ_1 by 1. So summing up, two coefficient decrease by one and maximal one increases by one, which implies $|\Delta_1| < |\Delta|$.

We can repeat this process a finite number of times until we get the divisor Δ', linear equivalent to and of same degree as Δ in the form:

$$\Delta' = n_1\langle P \rangle - n_2\langle Q \rangle + ?\langle \mathcal{O} \rangle$$

where $n_1, n_2 \in \mathbb{N}_{>0}$.

Suppose $n_1 > 1$.

P not of order two Let l be the line from 5.20 $\Rightarrow \operatorname{div}(l) = 2\langle P \rangle + \langle S \rangle - 3\langle \mathcal{O} \rangle$

$P = (\omega, 0)$ of order two $l(x,y) = x - \omega \Rightarrow \langle l \rangle = 2\langle P \rangle - 2\langle \mathcal{O} \rangle$

Subtraction reduces n_1 and $|\Delta'|$ and brings us back to the form of the start with reduced norm. The same algorithm works for n_2 and we end up with a divisor of the form

$$\langle P \rangle - \langle Q \rangle + ?\langle \mathcal{O} \rangle$$

with $P = (a,b)$. The line $l(x,y) = x - a$ has divisor $\operatorname{div}(l) = \langle P \rangle + \langle R \rangle - 2\langle \mathcal{O} \rangle$ or $\operatorname{div}(l) = 2\langle P \rangle - 2\langle \mathcal{O} \rangle$, subtracting brings us back to a previous case. ◻

Corrolar 5.25. *For each $\Delta \in \operatorname{Div}_0(E)$ there is a unique $P \in E$ such that:*

$$\Delta \sim \langle P \rangle - \langle \mathcal{O} \rangle$$

Proof. Thm. 5.24 tells us that Δ is equivalent to a divisor of norm 1, i.e. a divisor $\Delta_1 = \pm\langle P \rangle + ?\langle \mathcal{O} \rangle$. We can w.l.o.g. assume that the sign of $\langle P \rangle$ is a plus, because otherwise for $P = (a,b)$, we add $\operatorname{div}(l)$ for $l(x,y) = x - a$ which, since Prop. 5.22, is

$$\operatorname{div}(l) = \begin{cases} \langle P \rangle + \langle Q \rangle - 2\langle \mathcal{O} \rangle & \text{if } P \text{ not of order two} \\ 2\langle P \rangle - 2\langle \mathcal{O} \rangle & \text{if } P \text{ of order two} \end{cases}$$

to optain $\Delta_1 \sim \langle Q \rangle + ?\langle \mathcal{O} \rangle$ and after renaming: $\langle P \rangle + ?\langle \mathcal{O} \rangle \sim \Delta_1$. But we are given that $\Delta \in \operatorname{Div}_0(E)$ i.e. $0 = \deg \Delta = \deg \Delta_1$ and therefore conclude that the coefficient of $\langle \mathcal{O} \rangle$ is -1 i.e. $\Delta \sim \Delta_1 = \langle P \rangle - \langle \mathcal{O} \rangle$.

So its left to show that P is unique. Assume

$$\langle P \rangle - \langle \mathcal{O} \rangle \sim \Delta \sim \langle Q \rangle - \langle \mathcal{O} \rangle$$

Then $\langle Q \rangle \sim \Delta + \langle \mathcal{O} \rangle \sim \langle P \rangle$ which means that $\langle Q \rangle - \langle P \rangle$ is principal i.e. there is a rational function $r \in K(E)$ s.t. $\operatorname{div}(r) = \langle P \rangle - \langle Q \rangle$. Similarly as above, as long as $P \neq Q$ we add and subtract lines such that we end up at a rational function r with $\operatorname{div}(r) = \langle S \rangle - \langle \mathcal{O} \rangle$. This shows that r has no finite poles and is a polynomial because of Lemma 4.20. But it has only one single zero, which is impossible because of Lemma 4.18. So we conclude $P = Q$. □

Define a map $\bar{\sigma} : \operatorname{Div}_0(E) \to E$ by $\bar{\sigma}(\Delta) = P$ where P is the unique point with $\Delta \sim \langle P \rangle - \langle \mathcal{O} \rangle$. Since $\operatorname{div}(r) \sim 0$ it follows that $\bar{\sigma}(\langle r \rangle) = \mathcal{O}$ and we see that $\bar{\sigma}$ induces a map $\sigma : \operatorname{Pic}_0(E) \to E$.

Corrolar 5.26. *σ is a bijection.*

Proof.

surjective Let $P \in E$, then $\sigma(\langle P \rangle - \langle \mathcal{O} \rangle) = P$.

injective Let $P, Q \in E$, $\Delta \in \operatorname{Pic}_0(E)$ s.t. $\sigma(\Delta) = P$ and $\sigma(\Delta) = Q$. Since Cor. 5.25 we know that $\exists! S \in E$ s.t. $\Delta \sim \langle S \rangle - \langle \mathcal{O} \rangle$, which then implies $P = S = Q$.

□

References

[CRD] Leonard S. Charlap, David P. Robbins, CRD Expository Report 31 “An Elementary Introduction to Elliptic Curves”, December 1988

[WER] Anette Werner, “Elliptische Kurven in der Kryptographie”, Springer Verlag 2002, ISBN 3-540-42518-7