SEC

Masterarbeit

Pairing based Cryptography

Daniel Koch

Studiengang:	Mathematik
Prüfer/in:	Prof. Dr. Ralf Küsters
Betreuer/in:	Nicolas Huber
Beginn am:	25. April 2022
Beendet am:	25. Oktober 2022

Kurzfassung

In dieser Masterarbeit untersuchen wir Pairings auf elliptischen Kurven, deren Anwendung in der Kryptographie und deren Berechnung. Pairings sind bestimmte bilineare Funktionen zwischen Gruppen, wobei wir solche Abbildungen insbesondere für die Gruppe der Punkte elliptischer Kurven finden können. Beide diese Begriffe werden in dieser Arbeit eingeführt. Diese Funktionen können für kryptographische Anwendungen, insbesondere für den Schlüsselaustausch, die digitale Signatur und Identity based Cryptography genutzt werden. Um Pairings für diese Zwecke nutzbar machen zu können, stellen wir zwei Algorithmen zur Berechnung der Pairings vor.

Inhaltsverzeichnis

Abbildungsverzeichnis

Verzeichnis der Algorithmen

Abkürzungsverzeichnis

BDHP Bilinear-Diffie-Hellman Problem. 8, 9, 10, 11

CA Certifying Authority. 10

DHP Diffie-Hellman Problem. 8

DLP Discrete Logarithm Problem. 8, 9

TTP Trusted Third Party. 11

1 Einleitung

Elliptic Curve Cryptography ist eine weit verbreitete Art der Verschlüsselung. Dabei definiert man mithilfe der Punkte auf diesen Kurven eine Gruppe und kann diese praktisch überall dort einsetzen, wo sonst die Sicherheit eines Verfahrens auf dem diskreten Logarithmus endlicher Gruppen basiert.

Weniger bekannt ist jedoch der Einsatz von Pairings, bestimmter bilinearer Funktionen, auf elliptischen Kurven. Ursprünglich wurden diese genutzt, um das diskrete Logarithmus Problem auf bestimmten elliptischen Kurven zu brechen, bis man realisierte, dass sie eine ganz neue Welt an Verschlüsselungsverfahren eröffnen.

Diesen Verfahren widmen wir uns bereits im zweiten Kapitel. Dort definieren wir Pairings zunächst unabhängig von elliptischen Kurven und stellen drei verschiedene kryptographische Anwendungen vor.

Danach widmen wir uns im dritten Kapitel den elliptischen Kurven. Nachdem es unser Ziel ist, Pairings auf diesen zu definieren, müssen wir sie uns zunächst allgemein anschauen. Dabei wählen wir einen Weg, bei dem wir zunächst affine und projektive Kurven unabhängig von elliptischen Kurven betrachten, bevor wir uns auf diese spezialisieren. Dabei werden wir sehen, dass elliptische Kurven zunächst nichts anderes sind als spezielle projektive Kurven, die die sogenannte Weierstraßgleichung und eine Bedingung an ihre Diskriminante erfüllen. Dies ermöglicht dann, eine Gruppenoperation auf ihnen zu definieren.

Im vierten Kapitel kommen wir schließlich zu den Pairings. Für diese ist zunächst einiges ein Vorarbeit notwendig. Sie werden nicht auf der ganzen Gruppe der elliptischen Kurve definiert, sondern nur auf einer speziellen Untergruppe, den Torsionspunkten. Zur Definition der Pairings benötigen wir auch noch ein mächtiges Hilfsmittel, die Divisorengruppe. Diese ermöglicht es uns Punkte auf einer elliptischen Kurve aus einem anderen Blickwinkel zu betrachten und insbesondere Null- und Polstellen von Funktionen handhabbar zu machen. Deswegen widmen wir Funktionen auf elliptischen Kurven vorher auch einen längeren Abschnitt. Dabei betrachten wir insbesondere Polynome und rationale Funktionen mitsamt ihrer Null- und Polstellen. Schließlich definieren wir zwei verschiedene Pairings und beweisen zentrale Eigenschaften derer.

Die Pairings werden nur in Abhängigkeit bestimmter Divisoren definiert, ohne konkrete Berechnungsvorschrift. Daher benötigen wir noch Algorithmen zur Berechnung dieser. Für beide Pairings können wir dafür Millers Algorithmus nutzen, mit dem wir bestimmte rationale Funktionen, gegeben durch ihre Divisoren, berechnen können. Speziell für das Tate-Lichtenbaum-Pairing stellen wir noch einen Algorithmus aus dem Paper [Sta07] von Katherine Stange unter Benutzung elliptischer Netze vor.

2 Paring Based Cryptography

Wir werden in diesem Kapitel zunächst Pairings im Allgemeinen definieren und mit diesen verschiedene kryptographische Anwendungen vorstellen. Die Definition für Pairings ist in der Literatur nicht komplett einheitlich, wir entscheiden uns aber für die Folgende.

Definition 2.1 *Seien G_1 und G_2 zwei, in diesem Fall additiv geschriebene, Gruppen und G_T eine hier multiplikativ geschriebene Gruppe, alle von Ordnung n. Seien außerdem $e_1 \in G_1$ und $e_2 \in G_2$ die neutralen Elemente der Gruppen G_1 und G_2. Ein Pairing ist eine Abbildung $e : G_1 \times G_2 \to G_T$ mit den folgenden Eigenschaften:*

a. *Bilinearität: $\forall a, b \in \mathbb{Z}, \forall P \in G_1, Q \in G_2 : e(aP, bQ) = e(P, Q)^{ab}$*
b. *Nicht-Entartet: Sollte $e(S, T) = 1$ für alle $T \in G_2$ gelten, so gilt $S = e_1$. Ebenso sollte $e(S, T) = 1$ für alle $S \in G_1$ gelten, so ist $T = e_2$.*
c. *Berechenbar: e kann effizient berechnet werden.*

Bevor wir zu den Anwendungen in der Kryptographie kommen, definieren wir zunächst einige Sicherheitsbegriffe.

Definition 2.2 *Sei $G = \langle P \rangle$ eine additiv geschriebene Gruppe von Ordnung n. Dann definieren wir die folgenden Sicherheitsbegriffe:*

- *Das Discrete Logarithm Problem (DLP). Gegeben $P \in G$ und $Q \in G$, finde die Zahl $x \in \{0, 1, \ldots, n-1\}$ mit $xP = Q$.*
- *Das Diffie-Hellman Problem (DHP). Gegeben $P, aP, bP \in G$, bestimme abP.*
- *Das Bilinear-Diffie-Hellman Problem (BDHP). Seien $G_1 = G_2$ und G_T die Gruppen aus Definition 2.1. Dann, gegeben $P, aP, bP, cP \in G_1$, berechne $e(P, P)^{abc}$.*

Von all diesen Sicherheitsproblemen wird angenommen, dass sie, in entsprechenden Gruppen, nicht effizient berechenbar sind.

Wir schauen uns zunächst einfache Beispiele für Pairings an.

Beispiel 2.3
- *Sei $\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i$ das Standardskalarprodukt über einem Vektorraum F_q^n. Dieses ist nach bekannten Sätzen aus der linearen Algebra bilinear, nicht-entartet und offensichtlich einfach zu berechnen.*

- *Sei det* : $M_{2\times 2}(F_q) \to F_q$ *die Determinante auf den* 2×2 *Matrizen. Gesehen als eine Abbildung* $F_q^2 \times F_q^2 \to F_q$ *erfüllt diese die Eigenschaften eines Pairings.*

Diese einfachen Beispiele bieten allerdings keine große Sicherheit. Schauen wir uns dafür beispielsweise das Skalarprodukt an. Das BDHP fordert von uns, sollte v, av, bv, cv *für* $v \in F_q^n$ *und* $a, b, c \in F_q$ *bekannt sein, dass wir* $abc\langle v, v\rangle$ *berechnen. Dafür können wir aber zunächst einfach* $\langle v, av\rangle = a\langle v, v\rangle$ *bestimmen. Mit einfacher Multiplikation mit* $\langle v, v\rangle^{-1}$ *können wir so a berechnen. Verfahren wir dann ebenso mit b und c, erhalten wir* $abc\langle v, v\rangle$.

Wir machen weiter mit einer direkt ersichtlichen schlechten Nachricht. Existiert ein Pairing $e : G_1 \times G_1 \to G_T$, so lässt sich das DLP in G_1 leicht auf das DLP in der Gruppe G_T reduzieren. Diese Methode ist [Men, Kapitel 2] entnommen. Sie kann ein Problem darstellen, sollte das DLP in G_T deutlich einfacher zu lösen sein als in G_1. Sei jetzt $P = xQ$ für $P, Q \in G_1$. Mithilfe des Pairings erhalten wir $e(P, Q) = e(P, xP) = e(P, P)^x$. Demnach gilt $\log_P Q = \log_{e(P,P)} e(P, Q)$.

2.1 3 Party Key Exchange

Eines der wichtigsten Probleme in den Informationssicherheit ist der Schlüsselaustausch eines symmetrischen Schlüssels. Die bekannteste Art dies umzusetzen, ist der Diffie-Hellman Schlüsselaustausch. Dieser ermöglicht es zwei Parteien, einen gemeinsamen Schlüssel zu berechnen. Außerdem ist er folgendermaßen leicht auf drei Parteien auszuweiten, siehe dafür auch [Men, Kapitel 1].

Alice, Bob und Charlie wollen einen gemeinsamen Schlüssel austauschen. Dafür einigen sie sich auf eine Gruppe G der Ordnung n und einen Erzeuger P. Diese Informationen sind öffentlich zugänglich. Jede der drei Personen wählt entsprechend eine geheime Zahl $a, b, c \in \{0, \dots n-1\}$, Alice schickt dann aP an Bob, Bob bP an Charlie und Charlie cP an Alice. In einer zweiten Runde kann nun Alice acP an Bob, Bob abP an Charlie und Charlie bcP an Alice schicken. Alle drei können nun das Geheimnis $abcP$ berechnen. Was an dieser Methode allerdings auffällt, ist, dass zwei Kommunikationsdurchgänge benötigt werden. Joux hat in seinem Paper [Jou04] einen drei Parteien Schlüsselaustausch präsentiert, welcher nur eine Runde benötigt und Pairings nutzt.

Wir setzen $G_1 = G_2$ als eine endliche Gruppe von Ordnung n und wählen ein öffentliches Gruppenelement P. Die einzelnen Parteien berechnen dann $P_A = aP$, $P_B = bP$ und $P_C = cP$ und senden dieses Element an die beiden anderen. Diese können dann das gemeinsame Geheimnis berechnen:

$$e(aP, bP)^c = e(bP, cP)^a = e(cP, aP)^b = e(P, P)^{abc}$$

Dieses liefert uns bereits einen fertigen Schlüsselaustausch. Allerdings entsteht ein Problem, wenn $e(P, P) = 1$ ist, da dann obige Gleichung immer gleich 1 ist. Genau dieser Fall wird für das Weil-Pairing, welches wir in Kapitel 4.4 kennenlernen werden, auftreten. Joux schlägt mehrere Lösungen für dieses Problem vor, eine werden wir hier vorstellen.

In einer geeigneten Gruppe können wir zwei unabhängige Gruppenelemente P und Q wählen, wobei unabhängig in diesem Fall bedeutet, dass keine Zahl $a \in 0, \ldots n-1$ mit $aP = Q$ existiert. Dann berechnen die drei Teilnehmer jeweils die Elemente (P_A, Q_A), (P_B, Q_B) und (P_C, Q_C) und schicken diese an die anderen. Jede Partei kann jetzt das gemeinsame Geheimnis berechnen:

$$e(aP, bQ)^c = e(bP, cQ)^a = e(cP, aQ)^b = e(P, Q)^{abc}$$

Nach Annahme b können P und Q so gewählt werden, dass $e(P, Q) \neq 1$ ist.

Ist dieses Verfahren denn sicher? Hört ein Angreifer aP, bP und cP mit, steht er genau vor der Aufgabe ein BDHP zu lösen, welches als nicht effizient lösbar angenommen wird. Für eine genauere Analyse der Sicherheit siehe [Jou04].

2.2 Digital Signature

Das Ziel einer digitalen Signatur ist, die Integrität einer Nachricht sicherzustellen. Dafür wird für eine Nachricht M mithilfe eines privaten Schlüssels eine Signatur S berechnet und zusammen mit der Nachricht veröffentlicht. Diese Nachricht-Schlüssel Kombination kann dann mithilfe eines öffentlichen Schlüssels verifiziert werden. Für ein sicheres Signaturverfahren sollte es nur dem Autor der Nachricht möglich sein, eine gültige Signatur zu erzeugen.

Dan Boneh, Benn Lynn und Hovav Shacham präsentieren in [BLS01, Kapitel 3.4] ein Verfahren für die digitale Signatur mithilfe von Pairings.

Wir setzen zunächst wieder $G_1 = G_2$ als eine Gruppe der Ordnung n. Wie bei vielen anderen digitalen Signaturen wird eine Hash-Funktion genutzt. Die Autoren präsentieren eine solche Funktion $h : \{0,1\}^* \to G_1 \backslash \{0\}$ in ihrem Artikel, welche in die Gruppe G_1 abbildet. Als privaten Schlüssel erzeugt Alice eine Zahl $x \in \{1, \ldots n-1\}$ und erstellt mithilfe eines Erzeugers $P \in G_1$ das Element $R = xP$ und damit den öffentlichen Schlüssel (n, P, R).

Um jetzt eine Nachricht $M \in \{0,1\}^*$ zu signieren, berechnet Alice $P_M = h(M)$ und damit $S = xP_M$. Bob verifiziert diese, indem er $e(P, S) = e(P, xP_M) = e(P, P_M)^x$ berechnet und mit $e(R, P_M) = e(xP, P_M) = e(P, P_M)^x$ vergleicht. Sind die beiden gleich, so ist die Signatur gültig.

Hier beruht die Sicherheit auf dem Problem des diskrete Logarithmus in der Gruppe G_1. Ist es möglich aus P und R Alice privaten Schlüssel x zu berechnen, kann ein Angreifer beliebige Nachrichten signieren.

2.3 Identity Based Encryption

Bei einem Public-Key Encryption Schema steht man vor dem Problem, dass eine Partei Bob, die eine Nachricht an Alice verschlüsseln möchten, sichern gehen muss, dass sie auch wirklich ihren öffentlichen Schlüssel hat. Ansonsten könnte sich eine Angreiferin als Alice ausgeben, ihren öffentlichen Schlüssel als den von Alice einschleusen und die Nachricht so entschlüsseln. Die gängige Lösung, dieses Problem zu lösen, ist eine Certifying Authority (CA). Diese stellt ein Zertifikat für Alice Public Key aus und signiert dieses. Mithilfe des Zertifikats kann Bob sicher sein, dass er auch wirklich Alice öffentlichen Schlüssel besitzt.

Identity Based Encryption bietet einen anderen Ansatz, dieses Problem zu lösen. Dabei ist Alice öffentlicher Schlüssel ein Teil ihrer Identität, beispielsweise ihre Email-Adresse. Das erste Verfahren dafür wurde 2001 von Boneh und Franklin in [BF01] vorgestellt. Wir folgen der Beschreibung dessen aus [Men].

Dafür seien wieder $G_1 = G_2$ sowie G_T Gruppen. Zusätzlich benötigen wir noch zwei Hashfunktionen $H_1 : \{0,1\}^* \to G_1 \backslash \{0\}$ und $H_2 : G_T \to \{0,1\}^l$, wobei l die Bitlänge des Klartext ist. Auch dieses Mal kommen wir leider nicht ganz ohne eine Trusted Third Party (TTP) aus. Diese hat einen zufällig erzeugten privaten Schlüssel $t \in \{1, \dots n-1\}$, mit dem sie für ein Element $P \in G_1$ ihren öffentlichen Schlüssel $T = tP$ berechnet. Wenn Alice ihren privaten Schlüssel anfragt, berechnet die TTP aus Alice Identität ID_A den privaten Schlüssel $d_A = tH_1(ID_A)$.

Wenn Bob nun eine Nachricht $m \in \{0,1\}^l$ verschlüsseln möchte, so berechnet er $Q_A = H_1(ID_A)$, wählt eine zufällige Zahl $r \in \{1, \dots n\}$ und berechnet damit $R = rP$ und $c = m \oplus H_2(e(Q_A, T)^r)$, wobei $\oplus$ das bitweise XOR bezeichnet. Den Ciphertext (R, c) kann er dann Alice übermitteln. Um die Nachricht zu entschlüsseln, berechnet Alice $m = c \oplus H_2(e(d_A, R))$. Dies funktioniert, da

$$e(d_A, R) = e(tQ_A, rP) = e(Q_A, tP)^r = e(Q_A, T)^r.$$

Die Sicherheit dieses Verfahrens beruht nun darauf, dass ein Angreifer aus P, Q_A, T und R genau $e(Q_A, T)^r$ berechnen müsste, was eine Instanz des BDHP ist.

Dieses Verfahren ist aber nicht sicher gegen Chosen-Ciphertext Attacks. So könnte ein Angreifer einfach das erste Bit eines Ciphertexts c flippen und dieses entschlüsseln lassen. Von dieser Entschlüsselung kann er wieder das erste Bit flippen und erhält die ursprünglich verschlüsselte Nachricht.

Um das Verfahren gegen Chosen-Ciphertext Angriffe sicher zu machen, führt man noch zwei weitere Hashfunktionen $H_3 : \{0,1\}^+ \to 1, \dots n-1$ und $H_4 : \{0,1\}^l \to \{0,1\}^l$ ein. Um jetzt m zu verschlüsseln, wählt Bob einen zufälligen Bitstring $\sigma \in \{0,1\}^l$ und berechnet $g = e(Q_A, T), r = H_3(\sigma, m), R = rP, c_1 = \sigma \oplus H_2(g^r)$ und $c_2 = m \oplus H_4(\sigma)$ und verschickt (R, c_1, c_2) als Ciphertext. Zur Entschlüsselung berechnet Alice $g^r = e(d_A, R), \sigma = c_1 \oplus H_2(g^r), m = c_2 \oplus H_4(\sigma)$ und $r = H_3(\sigma, m)$. Jetzt akzeptiert Alice einen Text m nur dann, wenn $R = rP$. Damit funktioniert der vorher beschriebene Angriff nicht mehr.

3 Elliptische Kurven im Allgemeinen

Im letzten Kapitel haben wir gesehen, was ein Pairing ist, und wie simple Pairings konstruiert werden können. Dabei haben wir in Beispiel 2.3 auch gesehen, wie sehr wir aufpassen müssen, dass auch wirklich ein sicheres kryptographisches Verfahren dabei entsteht, da die dort genannten Pairings keinerlei Sicherheit geboten haben. Der Frage, wie wir sichere Pairings konstruieren können, widmen wir uns im Großteil dieser Arbeit.

Um dies zu erreichen, werden wir Pairings auf bestimmten Untergruppen elliptischer Kurven definieren. Dafür führen wir zunächst die elliptischen Kurven selbst ein. Eine elliptische Kurve ist die Lösungsmenge eines Polynoms in zwei Variablen, ausgestattet mit einer Operation, mit der sie zu einer Gruppe wird. Um diese Operation zu definieren, reicht die bekannte affine Ebene nicht aus, weswegen zusätzlich die projektive Ebene eingeführt wird. Dort ist es möglich einen „Punkt im Unendlichen“ zu definieren, der als neutrales Element in der Gruppe dienen wird.

In diesem Kapitel ist K immer ein beliebiger Körper. Dies ist für die allgemeine Einführung ausreichend, werden uns in späteren Kapiteln aber für kryptographische Anwendungen auf endliche Körper beschränken.

3.1 Affine und projektive Kurven

Für diesen Abschnitt folgen wir weitestgehend [Wer02, Kapitel 2].

Bevor wir elliptische Kurven definieren können, benötigen wir noch etwas allgemeine Vorbereitung. Dabei beginnen wir mit der Definition des affinen Raumes und affiner Kurven.

Definition 3.1 *Wir bezeichnen mit*

$$\mathbb{A}^2(K) := \{(a, b) | a, b \in K\}$$

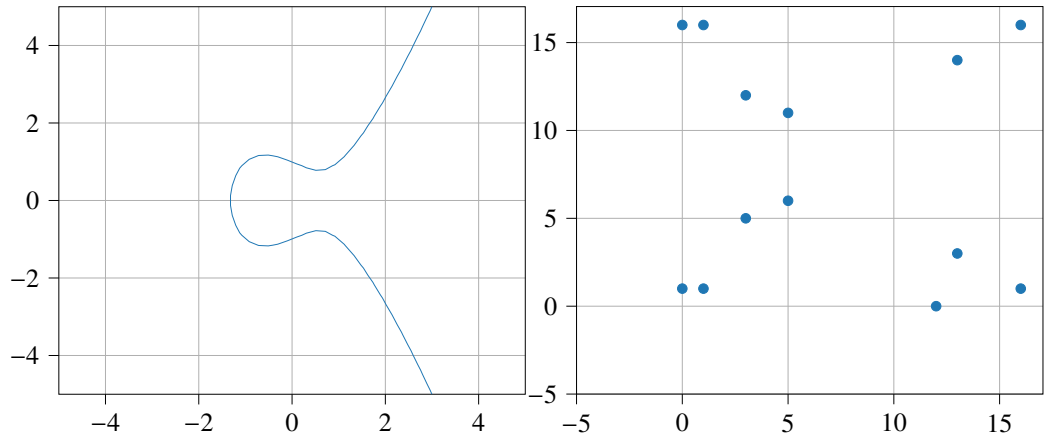
den zweidimensionalen affinen Raum.

Definition 3.2 *Sei $f \in K[x, y]$ und $f \neq 0$. Dann nennen wir die Menge*

$$C(K) = C_f(K) := \{(a, b) \in K | f(a, b) = 0\}$$

eine affine ebene Kurve.

Wir möchten diese Definitionen kurz anhand eines Beispiels illustrieren.



(a) Plot über $\mathbb{R}$ **(b)** Plot über F_{17}

Abbildung 3.1: Vergleich von Plots über die reellen Zahlen und einen endlichen Körper

Beispiel 3.3 *Sei $f(x, y) = y^2 - x^3 + x - 1$. Dann ist es einfach möglich ein sinnvolles Bild von $C(\mathbb{R})$ zu zeichnen. Ein Bild über beispielsweise F_{17} hingegen ist zwar möglich zu zeichnen, hilft unserer Vorstellungskraft allerdings nur wenig weiter. Ein Vergleich ist in Abbildung 3.1 dargestellt. Deswegen werden wir von nun an Abbildungen von affinen ebenen Kurven immer über $\mathbb{A}^2(\mathbb{R})$ zeichnen.*

Sei nun L ein zweiter Körper mit $K \subset L$. Dann können wir zu einem gegebenen Polynom $f \in K[x, y]$ nicht nur $C_f(K)$ betrachten, sondern auch $C_f(L)$. Dann gilt offensichtlich

$$C_f(K) \subset C_f(L).$$

Insbesondere können wir auch den algebraischen Abschluss $\bar{K}$ betrachten. Da gilt

$$C_f(K) \subset C_f(\bar{K}).$$

Da wir allgemeine Körper betrachten, können wir nicht generell von einer Ableitung sprechen, welche wir aber benötigen werden. Deswegen definieren wir die formale Ableitung.

Definition 3.4 *Sei K ein Körper und $K[x]$ der Polynomring über K. Für ein Polynom*

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

definieren wir die formale Ableitung $f'(x)$ als

$$f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}.$$

Wir schreiben auch $\frac{\partial f}{\partial x}(x)$ für $f'(x)$. So können wir auch Ableitungen für Polynome mehrerer Veränderlicher angeben.

Dies erlaubt uns zu definieren, wann eine affine ebene Kurve singulär ist.

Definition 3.5 *a. Die ebene affine Kurve $C_f(K)$ heißt singulär im Punkt $(a,b) \in C_f(K)$, falls beide Ableitungen von f in (a,b) verschwinden, es also gilt, dass $f(a,b) = 0$, $\frac{\partial f}{\partial x}(a,b) = 0$ und $\frac{\partial f}{\partial y}(a,b) = 0$.*

b. $C_f(K)$ heißt nicht-singulär, wenn die Kurve $C_f(\bar{K})$ in keinem Punkt (a,b) singulär ist.

An dieser Stelle lohnt es sich nochmal zu betonen, dass wir in der Definition der Nicht-Singularität den algebraischen Abschluss $\bar{K}$ betrachten.

Beispiel 3.6 *Dieses Beispiel ist [Wer02, Kapitel 2.1] entnommen. Sei $K = \mathbb{R}$ und $f(x,y) = y^2 - x^4 - 2x^2 - 1$. Dann ist*

$$\frac{\partial f}{\partial x}(x,y) = -4x(x^2+1) \text{ und}$$
$$\frac{\partial f}{\partial y}(x,y) = 2y.$$

Dabei hat $\frac{\partial f}{\partial x}(x,y)$ die Nullstellen $(0,b)$ für $b \in \mathbb{R}$ und $\frac{\partial f}{\partial y}(x,y)$ die Nullstellen $(a,0)$ für $a \in \mathbb{R}$. Die einzige gemeinsame Nullstelle ist demnach $(0,0)$. Es gilt allerdings $f(0,0) = -1$, weswegen die drei Polynome keine gemeinsame Nullstelle über $\mathbb{R}$ haben.

Über $\mathbb{C}$ kommen allerdings die beiden Nullstellen $(i,0)$ und $(-i,0)$ für $\frac{\partial f}{\partial x}$ dazu, welche auch Nullstellen der beiden anderen Polynome f und $\frac{\partial f}{\partial y}$ sind. Demnach ist die Kurve $C_f(\mathbb{R})$ keine nicht-singuläre Kurve.

Da affine ebene Kurven für unsere Zwecke nicht ausreichen werden, wenden wir uns nun der projektiven Ebene zu. Auch da beginnen wir direkt mit der Definition.

Definition 3.7 *a. Wir nennen (a,b,c) und (a',b',c') aus $K \times K \times K$ äquivalent und schreiben $(a,b,c) \sim (a',b',c')$, falls es ein $t \in K\backslash\{0\}$ gibt mit $a = ta'$, $b = tb'$ und $c = tc'$.*

b. Wir definieren den zweidimensionalen projektiven Raum $\mathbb{P}^2(K)$ als den Quotienten von $K \times K \times K\backslash\{(0,0,0)\}$ nach der Äquivalenzrelation $\sim$:

$$\mathbb{P}^2(K) = (K \times K \times K\backslash\{(0,0,0)\})/\sim .$$

Satz 3.8 *Die Relation aus Definition 3.7 ist wohldefiniert, ist also tatsächlich eine Äquivalenzrelation.*

Beweis Reflexivität: Sei $(a,b,c) \in K \times K \times K$. Dann gilt für $t = 1$, dass $a = ta$, $b = tb$ und $c = tc$, also $(a,b,c) \sim (a,b,c)$.

Symmetrie: Sei $(a,b,c) \sim (a',b',c')$. Also existiert ein $t \in K\backslash\{0\}$ mit $a = ta'$, $b = tb'$ und $c = tc'$. Durch Multiplikation mit t^{-1} erhalten wir $a' = t^{-1}a$, $b' = t^{-1}b$ und $c' = t^{-1}c$, also $(a',b',c') \sim (a,b,c)$.

Transitivität: Sei $(a, b, c) \sim (a', b', c')$ und $(a', b', c') \sim (a'', b'', c'')$. Es existieren also $t_1 \in K\backslash\{0\}$ und $t_2 \in K\backslash\{0\}$ mit $a = t_1a', b = t_1b', c = t_1c', a' = t_2a'', b' = t_2b'', c' = t_2c''$. Einsetzen der letzten drei Gleichungen in die ersten drei ergibt $a = t_1t_2a'', b = t_1t_2b''$ und $c = t_1t_2c''$ und somit $(a, b, c) \sim (a'', b'', c'')$.

Dies beendet den Beweis. □

Jedes Tripel $(a, b, c) \neq (0, 0, 0)$ gibt uns also einen Punkt in $\mathbb{P}^2$, den wir mit $[a : b : c]$ bezeichnen. Mit dieser Schreibweise wird verdeutlicht, dass es nur um das Verhältnis der Zahlen zueinander geht.

Welche Punkte befinden sich in $\mathbb{P}^2(K)$? Zunächst betrachten wir die Abbildung

$$i : \mathbb{A}^2(K) \to \mathbb{P}^2(K)$$

definiert durch

$$i(a, b) = [a : b : 1].$$

Man sieht leicht, dass diese Abbildung injektiv ist, wodurch wir sie als Einbettung auffassen können. Wir können $\mathbb{A}^2(K)$ also als Teilmenge von $\mathbb{P}^2(K)$ sehen. Allerdings liegen nicht alle Punkte in $\mathbb{P}^2(K)$ im Bild von i. Während alle Punkte $[a : b : c]$ mit $c \neq 0$ im Bild liegen, was durch Division mit c einfach zu sehen ist, können wir keinen Punkt mit $c = 0$ treffen. Denn das würde bedeuten, dass $[a : b : 1] = [a' : b' : 0]$ für $(a, b) \in \mathbb{A}^2(K)$ und $[a' : b' : 0] \in \mathbb{P}^2(K)$. Daraus folgt $0 = t1$ für ein $t \in K$, was unmöglich ist.

Dies motiviert uns, die nächste Abbildung

$$j : K \to \mathbb{P}^2(K)$$

durch

$$j(a) := [a : 1 : 0]$$

zu definieren. Auch diese ist injektiv und im Bild liegen dieses Mal alle Punkte der Form $[a : b : 0]$ mit $b \neq 0$. Analog zur Argumentation von gerade kann man zeigen, dass jetzt noch ein Punkt fehlt, nämlich $[1 : 0 : 0]$. Damit haben wir gezeigt, dass wir $\mathbb{P}^2(K)$ schreiben können als

$$\mathbb{P}^2(K) = i(\mathbb{A}^2(K)) \cup j(K) \cup \{[1 : 0 : 0]\}.$$

Nachdem wir gesehen haben, wie sich der projektive Raum zusammensetzt, widmen wir uns der Frage, von welcher Form Polynome sein müssen, sodass sie bzgl. der Äquivalenzrelation Sinn ergeben. Ist nämlich (a, b, c) eine Nullstelle eines Polynoms $f \in K[X, Y, Z]$, so sollten es auch alle Vielfachen (ta, tb, tc) sein. Dies führt zu folgender Definition.

Definition 3.9 *Sei $g \in K[X, Y, Z]$. Dann heißt g homogen von Grad d, falls gilt:*

$$g(X, Y, Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$$

mit Koeffizienten $\gamma_{\nu_1,\nu_2,\nu_3}$, die nicht alle Null sind und für die $\nu_1 + \nu_2 + \nu_3 = d$ ist, wenn $\gamma_{\nu_1,\nu_2,\nu_3}$ nicht verschwindet.

Betrachten wir nur diese Polynome, finden wir die gewünschte Eigenschaft.

Satz 3.10 *Sei $g \in K[X,Y,Z]$ homogen von Grad d. Dann gilt für alle $a,b,c \in K$ und $t \in K\backslash\{0\}$*

$$g(a,b,c) = 0 \Leftrightarrow g(ta,tb,tc) = 0.$$

Beweis Wir folgen dem Beweis in [Wer02, Lemma 2.2.3].

Sei $g(x,y,z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} x^{\nu_1} y^{\nu_2} z^{\nu_3}$. Dann gilt

$$\begin{aligned} g(ta,tb,tc) &= \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} (ta)^{\nu_1} (tb)^{\nu_2} (tc)^{\nu_3} \\ &= \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} t^{\nu_1+\nu_2+\nu_3} a^{\nu_1} b^{\nu_2} c^{\nu_3} \\ &= t^d g(a,b,c). \end{aligned}$$

Es werden also beide Seiten gleichzeitig Null. □

Mit diesem Wissen können wir Kurven in der projektiven Ebene ganz ähnlich zu denen in der affinen Ebene definieren.

Definition 3.11 *Sei $g \in K[X,Y,Z]$ ein homogenes Polynom. Dann bezeichnen wir die Menge der Nullstellen von g in $\mathbb{P}^2(K)$ als $C_g(K)$:*

$$C(K) = C_g(K) := \{[a:b:c] \in \mathbb{P}^2(K) | g(a,b,c) = 0\}$$

Jede solche Nullstellenmenge nennen wir eine projektive ebene Kurve.

Im nächsten Beispiel wollen wir illustrieren, in welchem Zusammenhang affine ebene Kurven und projektive ebene Kurven stehen.

Beispiel 3.12 *Dieses Beispiel ist [Wer02, Kapitel 2.2] entnommen.*

Sei $C_f(K)$ die affine ebene Kurve gegeben durch

$$f(x,y) = y^2 - x^3 - x.$$

Für eine Nullstelle (a,b) dieses Polynoms gilt

$$b^2 = a^3 + a.$$

Sei nun $0 \neq c \in K$. Wir definieren $a' = ac$ und $b' = bc$. Damit gilt

$$\left(\frac{b'}{c}\right)^2 = \left(\frac{a'}{c}\right)^3 + \frac{a'}{c}.$$

Multiplikation mit c^3 liefert

$$b'^2 c = a'^3 + a' c^2.$$

Demnach ist (a', b', c) *eine Lösung von*

$$Y^2Z = X^3 + XZ^2, \tag{3.1}$$

einer Gleichung in drei Variablen. Welche Lösungen hat diese nun? Sei dafür (a, b, c) *eine Lösung. Da können wir jetzt zwei Fälle unterscheiden. Sei zunächst* $c \neq 0$*. Dann können wir die obere Herleitung rückwärts gehen und durch* c^3 *teilen. Damit erhalten wir* $\left(\frac{a}{c}, \frac{b}{c}\right)$ *als Lösung des ursprünglichen Polynoms, also einen Punkt auf* $C_f(K)$*.*

Ist hingegen $c = 0$ *und setzen dies ein, erhalten wir die Gleichung* $a^3 = 0$*. Also muss auch* $a = 0$ *sein und* b *bleibt beliebig.*

Wir stellen noch fest, dass Gleichung 3.1, als Polynom gesehen, homogen von Grad 3 ist. Also sind nach Satz 3.10 auch alle Vielfachen von Nullstellen wieder Nullstellen.

Zusammenfassend lässt sich also sagen, dass wir für jeden Punkt (a, b) *auf* $C_f(K)$ *eine Lösung* (ac, bc, c) *von Gleichung 3.1 erhalten. Da dies auch für alle Vielfachen gilt, gilt dass* $[a, b, 1] \in C_g(K)$*. Die Abbildung, die wir hierfür verwenden, ist aber gerade die Abbildung* i *von oben. Unter dieser wird also* $C_f(K)$ *nach* $C_g(K)$ *abgebildet. Zusätzlich zu den Punkten aus* $C_f(K)$ *kommt auch noch der Punkt* $[0 : 1 : 0]$ *dazu, wie wir gesehen haben. Also ist*

$$C_g(K) = i(C_f(K)) \cup \{[0 : 1 : 0]\}.$$

Der Punkt $[0 : 1 : 0]$ *ist der, den wir den Punkt im Unendlichen nennen werden.*

Das hier gezeigte Verfahren funktioniert natürlich auch ganz allgemein.

Satz 3.13 *Sei* $0 \neq f \in K[x, y]$*, also* $f(x, y) = \sum_{\nu_1, \nu_2 \geq 0} \gamma_{\nu_1, \nu_2} x^{\nu_1} y^{\nu_2}$ *und* $d = \max\{\nu_1 + \nu_2\}$ *der Grad von* f*. Dann ist das Polynom*

$$g(X, Y, Z) = \sum_{\nu_1, \nu_2 \geq 0, \nu_1 + \nu_2 \leq d} \gamma_{\nu_1, \nu_2} X^{\nu_1} Y^{\nu_2} Z^{d - \nu_1 - \nu_2}$$

homogen von Grad d *und erfüllt* $g(a, b, 1) = f(a, b)$ *für alle* $(a, b) \in \mathbb{A}^2(K)$*.*

Unter der Abbildung $i : \mathbb{A}^2(K) \to \mathbb{P}^2(K)$ *wird* $C_f(K)$ *nach* $C_g(K)$ *abgebildet. Wenn sich ein Punkt* $[a : b : c] \in \mathbb{P}^2(K)$ *als* $i(x)$ *für ein* $x \in \mathbb{A}^2(K)$ *schreiben lässt, so liegt* x *schon in* $C_f(K)$*.*

Beweis Wir folgen dem Beweis in [Wer02, Proposition 2.2.5].

Die Homogenität prüft man schnell nach, indem man die Exponenten aufaddiert. So erhält man

$$\nu_1 + \nu_2 + (d - \nu_1 - \nu_2) = d.$$

Also ist g homogen von Grad d.

Auch die Eigenschaft $g(a, b, 1) = f(a, b)$ prüft man durch Einsetzen schnell nach:

$$\begin{aligned} g(a, b, 1) &= \sum_{\nu_1, \nu_2 \geq 0, \nu_1 + \nu 2 \leq d} \gamma_{\nu_1, \nu_2} a^{\nu_1} b^{\nu_2} 1^{d - \nu_1 - \nu_2} \\ &= f(a, b) \end{aligned}$$

Wenn für ein beliebiges $(a, b) \in \mathbb{A}^2(K)$ gilt, dass $i(a, b) = [a : b : 1] \in C_g(K)$, dann gilt $g(a, b, 1) = 0 = f(a, b)$, also ist $(a, b) \in C_f(K)$. □

Dies ermöglicht uns jetzt die Singularität projektiver ebener Kurven analog zu der Singularität der affinen ebenen Kurven zu definieren.

Definition 3.14 *Sei $g \in K[X,Y,Z]$ homogen von Grad d.*

a. *Die projektive ebene Kurve $C_g(K)$ heißt singulär im Punkt $P = [a : b : c] \in C_g(K)$, falls alle Ableitungen von g in P verschwinden, es also gilt, dass $\frac{\partial g}{\partial X}(a,b,c) = 0$, $\frac{\partial g}{\partial Y}(a,b,c) = 0$, $\frac{\partial g}{\partial Z}(a,b,c) = 0$.*

b. *$C_g(K)$ heißt nicht-singulär, falls $C_g(\bar{K})$ keinen singulären Punkt enthält.*

Satz 3.15 *Die Definition 3.14 ist wohldefiniert, es ist also irrelevant, welche projektiven Koordinaten (a,b,c) mit $P = [a : b : c]$ wir betrachten.*

Beweis Sei zunächst $g \in K[X,Y,Z]$ homogen von Grad d mit $g(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$. Wir betrachten zunächst die Ableitung von g nach X:

$$\frac{\partial g}{\partial X}(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} \nu_1 X^{\nu_1 - 1} Y^{\nu_2} Z^{\nu_3}$$

Dieses Polynom ist homogen von Grad $d-1$. Dafür unterscheiden wir zwei Fälle. Ist $\nu_1 = 0$, so verschwindet der entsprechende Term in der Ableitung und spielt somit für die Homogenität keine Rolle mehr. Ist $\nu_1 \neq 0$, so gilt $\nu_1 - 1 + \nu_2 + \nu_3 = d - 1$. Die Ableitungen nach Y und Z berechnen sich analog.

Seien $[a : b : c] \sim [a', b', c'] \in \mathbb{P}^2(K)$. Es existiert also ein $t \in K$ mit $a = ta'$, $b = tb'$ und $c = tc'$. Nach Satz 3.10 ist

$$\frac{\partial g}{\partial X}(a,b,c) = 0 \Leftrightarrow \frac{\partial g}{\partial X}(ta,tb,tc) = 0.$$

Für die anderen Ableitungen gilt dies wieder analog. Das beweist die Behauptung. □

Zum Schluss halten wir noch fest, dass diese Definition für projektive Kurven mit der für affine Kurven zusammenpasst.

Satz 3.16 *Es sei $g(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$ ein homogenes Polynom von Grad d. Sei außerdem $f = \sum_{\nu_1,\nu_2 \geq 0, \nu_1+\nu_2 \leq d} \gamma_{\nu_1,\nu_2,d-\nu_1-\nu_2} x^{\nu_1} y^{\nu_2}$. Für jeden Punkt $P \in C_g(K)$ gilt: Falls $P = i(Q)$ in $i(\mathbb{A}^2(K))$ liegt, so ist $C_g(K)$ singulär in P genau dann, wenn die affine Kurve $C_f(K)$ singulär in Q ist.*

Beweis Wir folgen dem Beweis in [Wer02, Lemma 2.2.8].

Nach Satz 3.13 liegt Q in $C_f(K)$. Ist $Q = (a,b)$, so ist $P = i(Q) = [a : b : 1]$. Nun ist

$$\frac{\partial g}{\partial X}(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} \nu_1 X^{\nu_1 - 1} Y^{\nu_2} Z^{\nu_3},$$

sodass $\frac{\partial g}{\partial X}(a,b,1) = \frac{\partial f}{\partial x}(a,b)$. Die Gleichheit $\frac{\partial g}{\partial Y}(a,b,1) = \frac{\partial f}{\partial y}(a,b)$ zeigt man analog. Außerdem gilt

$$\frac{\partial g}{\partial Z}(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} \nu_3 X^{\nu_1} Y^{\nu_2} Z^{\nu_3 - 1},$$

sodass

$$\frac{\partial g}{\partial Z}(a,b,1) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} \nu_3 a^{\nu_1} b^{\nu_2}$$

ist. Nun ist $\nu_1 + \nu_2 + \nu_3 = d$ in allen Summanden ungleich Null. Daraus folgt

$$\begin{aligned}\frac{\partial g}{\partial Z}(a,b,1) &= \sum_{\nu_1,\nu_2 \geq 0, \nu_1+\nu_2 \leq d} \gamma_{\nu_1,\nu_2,d-\nu_1-\nu_2}(d-\nu_1-\nu_2) a^{\nu_1} b^{\nu_2} \\ &= df(a,b) - a\frac{\partial f}{\partial x}(a,b) - b\frac{\partial f}{\partial y}(a,b).\end{aligned}$$

In allen drei Fällen gilt jetzt, dass, wenn die linke Seite Null ist, es auch die rechte ist, und sich so die Singularität eines Punktes überträgt. □

3.2 Elliptische Kurven

Für diesen Abschnitt folgen wir weitestgehend [Wer02, Kapitel 2.3].

Nachdem wir uns affine und projektive Kurven im Allgemeinen angeschaut haben, widmen wir uns nun einer speziellen Klasse von Kurven, den elliptischen Kurven. Diese erlauben die Definition einer Gruppenoperation auf der Kurve, welcher wir uns im nächsten Abschnitt widmen werden. Zunächst starten wir mit der Definition elliptischer Kurven.

Definition 3.17 *Eine elliptische Kurve ist eine nicht-singuläre projektive ebene Kurve $C_g(K)$, wobei g ein homogenes Polynom vom Grad drei der folgenden Gestalt ist:*

$$g(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{3.2}$$

Dabei gilt $a_1, a_2, a_3, a_4, a_6 \in K$.

Die Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

deren Lösungen gerade die Punkte auf $C_g(K)$ sind, nennt man die allgemeine Weierstraßgleichung. Die eigenartige Bezeichnung der Koeffizienten hat historische Gründe. Wir werden diese zunächst beibehalten, später aber etwas vereinfachen.

Statt $C_g(K)$ schreiben wir ab sofort vereinfachend $E(K)$. Ist L eine Körpererweiterung von K und die Koeffizienten $a_1, a_2, a_3, a_4, a_6 \in K$, wir aber Lösungen der Gleichung über L betrachten möchten, so schreiben wir $E_K(L)$.

Diese allgemeine Form der Weierstraßgleichung ist allerdings recht kompliziert und unhandlich. In vielen Fällen ist es uns möglich, diese um einiges zu vereinfachen.

Satz 3.18 *Es sei $E(K)$ ein elliptische Kurve.*

a. Falls die Charakteristik von K ungleich 2 ist, so erhält man mit der Substitution

$$[r : s : t] \to \left[r : s + \frac{a_1}{2}r + \frac{a_3}{2}t : t\right]$$

wieder eine Gleichung für eine elliptische Kurve der Form

$$Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

mit entsprechenden Koeffizienten $a_2, a_4, a_6 \in K$.

b. Ist zusätzlich die Charakteristik von K ungleich 3, so erhält man mit der Substitution

$$[r : s : t] \to [36r + 3b_2t : 216s : t]$$

wieder eine Gleichung für eine elliptische Kurve von der Form

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

mit entsprechenden Koeffizienten $a_4, a_6 \in K$.

Beweis Der Beweis besteht aus länglichem und wenig Einsicht bringendem Nachrechnen, weswegen wir ihn hier überspringen. Man findet ihn in [Wer02, Proposition 2.3.2]. □

Wir werden oft die Annahme $char(K) \notin \{2, 3\}$ machen, was es uns möglich macht mit der einfachsten Form der Weierstraßgleichung zu arbeiten.

Als nächstes stellen wir uns die Frage, welche Punkte auf $E(K)$ liegen. Dafür betrachten wir zunächst die Punkte, die nicht in $i(\mathbb{A}^2(K))$ liegen. Diese sind von der Form $P = [r : s : 0] \in \mathbb{P}^2(K)$. Setzen wir $(r, s, 0)$ in die Weierstraßgleichung ein, so erhalten wir $r^3 = 0$. Daraus folgt, dass $r = 0$ ist und $s \neq 0$, da $[0 : 0 : 0] \notin \mathbb{P}^2(K)$. P hat also die Form

$$P = [0 : 1 : 0].$$

Damit haben wir gezeigt, dass elliptische Kurven nur einen Punkt haben, welcher nicht in $i(\mathbb{A}^2(K))$ liegt. Diesen bezeichnen wir mit O. Dieser Punkt ist nie singulär, denn es gilt

$$\frac{\partial g}{\partial Z}(X, Y, Z) = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z2$$

und damit

$$\frac{\partial g}{\partial Z}(0, 1, 0) = 1.$$

Diesen Punkt kann man sich auch so vorstellen, dass er sowohl ganz oben als auch ganz unten auf der y-Achse sitzt. Deswegen nennen wir ihn auch den Punkt im Unendlichen.

Will man feststellen, ob eine Gleichung der Form 3.2 nicht singulär ist, muss man also nur noch die Punkte der affinen Kurve testen. Dafür reicht es nach Satz 3.13 aus, die Kurve $C_f(K)$ für

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

auf nicht-Singularität zu testen. Dafür gibt es glücklicherweise ein einfaches Kriterium.

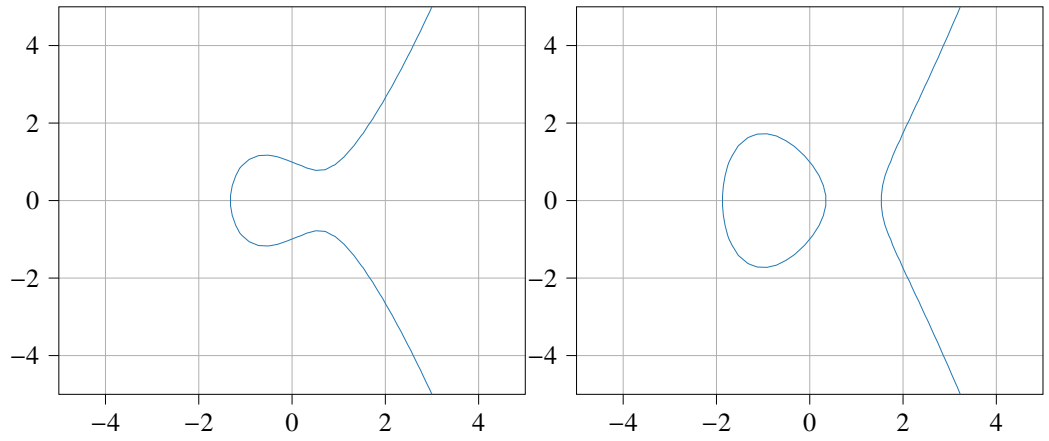
Satz 3.19 *Sei* $g(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ *ein Weierstraßpolynom. Wir definieren die Diskriminante von* g *als* $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ *mit Koeffizienten*

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6.$$

Dann ist die Kurve $C_g(K)$ *nicht-singulär genau dann, wenn* $\Delta \neq 0$.

Beweis Auch dieser Beweis ist nur langes Nachrechnen und eine Unterscheidung der verschiedenen Charakteristiken. Man findet ihn in [Wer02, Proposition 2.3.3]. □

Bemerkung 3.20 *Für eine Gleichung in Form der vereinfachten Weierstraßgleichung* $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ *vereinfacht sich die Diskriminante deutlich zu* $\Delta = -16(4a_4^3 + 27a_6^2)$.



(a) $y^2 = x^3 - x + 1$ **(b)** $y^2 = x^3 - 3x + 1$

Abbildung 3.2: Die zwei grundlegenden Formen elliptischer Kurven

Beispiel 3.21 *Was bedeutet die Bedingung* $\Delta \neq 0$ *nun für unsere Kurve? Man kann zeigen, dass, wenn die Diskriminante Null ist, dies bedeutet, dass zwei Nullstellen des Polynoms* $x^3 + a_4x + a_6$ *über einem Körper* K *mit* $\mathrm{char}(K) \notin \{2,3\}$ *gleich sein müssen. Das heißt, dass genau dieser Fall herausgefiltert wird. Übrig bleiben dann noch zwei Möglichkeiten. Entweder hat das Polynom eine oder drei Nullstellen in x. Dies ergibt zwei grundlegende Formen für elliptische Kurven, dargestellt in Abbildung 3.2.*

3.3 Gruppenstruktur

Eine der besonderen Eigenschaften elliptischer Kurven ist, dass es möglich ist, eine Gruppenstruktur auf ihnen zu definieren. Diese wollen wir in diesem Abschnitt herleiten. Dazu wählen wir zunächst einen anschaulichen Weg, bevor wir konkrete Berechnungsvorschriften dafür herleiten. Dafür folgen wir [Sil09, Kapitel III.2].

In diesem Abschnitt betrachten wir elliptische Kurven immer in affinen Koordinaten. In diesem Sinne stellen wir uns den Punkt im Unendlichen so vor, dass er sich oben und unten an der y-Achse befindet. Damit beginnen wir direkt mit der Definition der Gruppenoperation.

Definition 3.22 *Seien $P, Q \in E(K)$ und L die Linie durch P und Q. Sollte $P = Q$ gelten, legen wir stattdessen die Tangente an P an. Diese Linie wird $E(K)$ an einem dritten Punkt schneiden. Sei dieser Punkt R. Sei jetzt L' die Linie durch R und O, das heißt, die senkrechte Linie durch R.. Dann schneidet L' $E(K)$ wieder in einem dritten Punkt. Diesen bezeichnen wir mit $P \oplus Q$.*

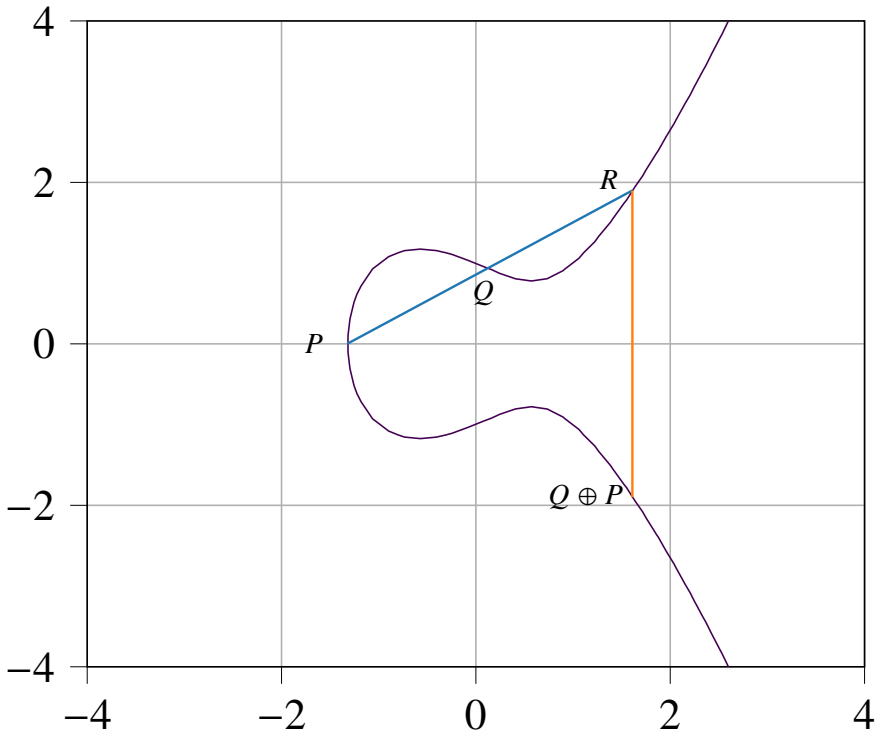


Abbildung 3.3: Die Gruppenoperation

Die Gruppenoperation ist in Abbildung 3.3 verdeutlicht. Wir wollen als nächstes zeigen, dass die eben definierte Operation auch wirklich eine Gruppenoperation ist.

Satz 3.23 *Die in Definition 3.22 definierte Operation hat folgende Eigenschaften:*

a. Falls eine Linie L die Kurve $E(K)$ an den drei Punkten $P, Q, R \in E(K)$ schneidet, dann gilt

$$(P \oplus Q) \oplus R = O.$$

b. $P \oplus O = P$ für alle $P \in E(K)$.

c. $P \oplus Q = Q \oplus P$ für alle $P, Q \in E(K)$.

d. Sei $P \in E(K)$ Dann existiert ein Punkt auf $E(K)$, bezeichnet mit $\ominus P$, mit

$$P \oplus (\ominus P) = O.$$

e. *Seien $P, Q, R \in E(K)$. Dann gilt*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Mit diesen Eigenschaften wird $E(K)$ zusammen mit der Operation $\oplus$ zu einer abelschen Gruppe mit neutralem Element O.

Beweis Wir folgen dem Beweis in [Sil09, Proposition 2.2].

a. Dies erkennt man am einfachsten in Abbildung 3.3. Da sieht man, dass $P \oplus Q$ und R auf einer senkrechten Linie liegen. Damit ist die Summe der beiden O. Sind $P = Q = O$, so legen wir eine Tangente an O an. Diese schneidet wieder nur den Punkt im Unendlichen.

b. Wählen wir $Q = O$ in Definition 3.22, stellen wir fest, dass die Linien L und L' die gleichen sind. Erstere schneidet $E(K)$ in P, O, R und letztere in $R, O, P \oplus O$. Vergleichen der Punkte liefert $P \oplus O = P$.

c. Da es keinen Unterschied macht, ob man eine Linie durch P und Q oder durch Q und P legt, folgt die Behauptung.

d. Sei L die Linie durch P und O. Wir nennen den letzten Schnittpunkt R und erhalten damit

$$O = (P \oplus O) \oplus R = P \oplus R.$$

Also ist $R = \ominus P$.

e. Wir werden diese Aussage an dieser Stelle nicht beweisen. Später werden wir in Bemerkung 4.52 einen Beweis sehen. Alternativ kann sie auch mithilfe der später hergeleiteten Formeln mühsam nachgerechnet werden. Für einen theoretischeren Beweis verweisen wir auf [Sil09, Proposition III 3.4e], für einen geometrischen auf [Wer02, Satz 2.3.12 iv]. □

Bemerkung 3.24 *Die Begriffe der Tangente, Linie oder eines Schnittpunkts in dieser anschaulichen Form ergeben natürlich nur über die reellen Zahlen Sinn. Wir betrachten elliptische Kurven allerdings auch über beliebige Körper, wo die geometrische Vorstellung zerfällt. Dort sind dann präzise Definitionen dieser Begriffe notwendig. Eine rigorose Einführung für beliebige Körper findet man in [Wer02, Kapitel 2.3]. Ebenso kann man die obigen Eigenschaften mit den jetzt hergeleiteten Formeln nachrechnen.*

Wir wollen die in Definition 3.22 definierte Gruppenoperation berechenbar machen. Dafür ist es möglich, Formeln herzuleiten. Dafür folgen wir größtenteils [Was08, Kapitel 2.2].

Seien $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ für eine elliptische Kurve $E(K)$ mit Weierstraßgleichung $y^2 = x^3 + Ax + B$ mit $A, B \in K$.

Wir nehmen zunächst an, dass $P_1 \neq P_2$ und, dass keiner der beiden Punkte O ist. Zusätzlich nehmen wir für den Moment an, dass $x_1 \neq x_2$ ist, diesen Fall betrachten wir später. Um die Linie durch die beiden Punkte zu berechnen, bestimmen wir zunächst die Steigung dieser. Diese ist, wie man schnell sieht

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

Damit erhält man leicht die Gleichung für die Linie durch P_1 und P_2:

$$y = m(x - x_1) + y_1$$

Um den Schnittpunkt mit $E(K)$ zu finden, setzen wir dies in die Weierstraßgleichung ein:

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Dies kann umgeformt werden zu:

$$x^3 - x^2m^2 + x(2x_1m^2 - 2my_1 + A) + (-x_1^2m^2 - y_1^2 + 2mx_1y_1 + B) = 0$$

Im Allgemeinen ist es nicht einfach, ein solches Polynom zu lösen. Allerdings kennen wir bereits zwei Nullstellen, nämlich die x-Werte von P_1 und P_2. Dies können wir ausnutzen. Sei dafür $x_3 + ax^2 + bx + c$ ein beliebiges kubisches Polynom mit Nullstellen r, s, t. Dann gilt

$$x_3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \dots.$$

Ein Koeffizientenvergleich liefert

$$-a = r + s + t.$$

Setzen wir die Werte aus unserem Fall ein, erhalten wir

$$x = m^2 - x_1 - x_2$$

und

$$y = m(x - x_1) + y_1.$$

Dies ist der Punkt R. Um jetzt den finalen Punkt unserer Addition zu erhalten, müssen wir noch eine Linie durch den eben berechneten Punkt und O legen. Wie bereits erwähnt, ist dies die senkrechte Linie durch R, was bedeutet, dass ihr x-Wert konstant ist. Daher stellen wir uns die Frage, welche Lösungen die Weierstraßgleichung $y^2 = x^3 + Ax + B$ für festgehaltenes x hat. Ist (x, y) eine Lösung, so ist aufgrund des Quadrats auf der linken Seite auch $(x, -y)$ eine Lösung. Dies ist genau der dritte Schnittpunkt mit der senkrechten Geraden. Damit erhalten wir den Punkt $P_3 = (x_3, y_3) = P_1 \oplus P_2$ mit

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1. \tag{3.3}$$

Für den Fall, dass $x_1 = x_2$ ist, aber $y_1 \neq y_2$, ist die Linie durch die beiden Punkte senkrecht. Der dritte Schnittpunkt ist also O. Das heißt, wir müssen die Tangente an O anlegen, um unseren finalen Punkt zu erhalten. Wie schon im Beweis von Satz 3.23 erörtert, ist dieser Punkt wieder O.

Sei nun $P_1 = P_2 = (x_1, y_1)$. Nach der Berechnungsvorschrift müssen wir eine Tangente an diesen Punkt anlegen. Die Steigung dieser erhalten wir durch implizites Differenzieren:

$$2y\frac{dy}{dx} = 3x^2 + A, \text{also } m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

Ist $y_1 = 0$, so haben wir eine „unendliche“ Steigung und die Linie ist senkrecht und wir erhalten $P_1 + P_2 = O$. Andernfalls erhalten wir wieder die Gleichung für L:

$$y = m(x - x_1) + y_1.$$

Wie zuvor können wir dies in die Weierstraßgleichung einsetzen und erhalten die kubische Gleichung

$$0 = x^3 - m^2x^2 + \dots.$$

Dieses mal kennen wir nur eine Nullstelle, nämlich x_1, welche aber eine doppelte ist. Damit erhalten wir $P_3 = (x_3, y_3)$ mit

$$x_3 = m^2 - 2x_1,\ y_3 = m(x_1 - x_3) - y_1.$$

Wir fassen die obigen Ergebnisse in folgendem Satz zusammen.

Satz 3.25 *Sei $E(K)$ eine elliptische Kurve definiert durch $y^2 = x^3 + Ax + B$. Seien $O \neq P_1 = (x_1, y_1) \in E(K)$ und $O \neq P_2 = (x_2, y_2) \in E(K)$. $P_1 + P_2 = P_3 = (x_3, y_3)$ ist wie folgt definiert:*

a. Gilt $x_1 \neq x_2$, so gilt

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

b. Gilt $x_1 = x_2$, aber $y_1 \neq y_2$, so ist $P_1 + P_2 = O$.

c. Ist $P_1 = P_2$ und $y_1 \neq 0$, so gilt

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

d. Gilt $P_1 = P_2$ und $y_1 = 0$, so ist $P_1 + P_2 = O$.

Außerdem gilt $P + O = P$ für alle Punkte $P \in E(K)$.

Zuletzt führen wir noch etwas Notation ein. Da wir uns klar gemacht haben, dass $\oplus$ tatsächlich eine Gruppenoperation definiert, schreiben wir ab jetzt einfach $P + Q$ statt $P \oplus Q$ und $-P$ statt $\ominus P$. Außerdem definieren wir

$$\begin{aligned} mP &:= \underbrace{P + \dots + P}_{m\text{-mal}}, \text{ für } m > 0, \\ (-m)P &:= -(mP), \text{ für } m > 0, \\ 0P &:= O. \end{aligned}$$

4 Pairings

Nachdem wir im letzten Kapitel elliptische Kurven im Allgemeinen eingeführt haben, widmen wir uns nun dem Hauptobjekt dieser Arbeit, den Pairings auf elliptischen Kurven. Dafür müssen wir zunächst etwas Vorarbeit leisten. Zum einen werden unsere Pairings nicht auf der elliptischen Kurve selbst definiert, sondern auf einer Untergruppe dieser, der Torsionsgruppe, zum anderen müssen wir Funktionen auf elliptischen Kurven und ihre Nullstellen genauer untersuchen. Damit können wir schließlich das Weil- und das Tate-Lichtenbaum-Pairing konstruieren.

4.1 Torsionspunkte

Unsere Pairings werden nicht auf der gesamten elliptischen Kurve definiert werden, sondern auf Untergruppen dieser. Die Untergruppen, die wir dafür nutzen, sind die Torsionspunkte. Dies sind genau die Punkte, die nach n-maliger Multiplikation mit sich selbst verschwinden.

Definition 4.1 *Sei $n \in \mathbb{N}$ und $E(K)$ eine elliptische Kurve. Dann definieren wir*

$$E[n] := \{P \in E(\bar{K}) | nP = O\}.$$

Wir nennen $E[n]$ die Torsionsgruppe.

Beispiel 4.2 *Wir wolllen $E[2]$ für eine elliptische Kurve $E(\bar{K})$ genauer betrachten. Dafür folgen wir dem Beispiel in [Was08, Kapitel 3.1]. Seien $e_1, e_2, e_3 \in \bar{K}$ die Nullstellen von $x^3 + Ax + B$. Demnach gilt*

$$y^2 = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3).$$

Wie wir am Ende von Kapitel 3 bei der Herleitung der Formeln für die Gruppenoperation gesehen haben, erfüllt ein Punkt P die Gleichung $2P = O$ genau dann, wenn die Tangente senkrecht ist, also $y = 0$ ist. Das liefert uns vier Punkte in $E[2]$:

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

Wir halten direkt das Hauptresultat über Torsionspunkte fest.

Satz 4.3 *Sei $E(K)$ eine elliptische Kurve und $n \in \mathbb{N}$. Falls $\mathrm{char}(K) \nmid n$ oder $\mathrm{char}(K) = 0$, so ist*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Ist die Charakteristik von $K = p > 0$ und $p|n$, so schreiben wir $n = p^r n'$ mit $p \nmid n'$. Dann gilt

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ oder } E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

Beweis Der Beweis ist lang und benötigt einiges an Vorarbeit, weswegen wir ihn hier nicht führen werden. Man findet ihn beispielsweise in [Was08, Kapitel 3.2]. □

4.2 Rationale Funktionen und Endomorphismen

4.2.1 Rationale Funktionen

Bevor wir uns den Divisoren widmen können, müssen wir uns zunächst Funktionen, und dabei insbesondere Polynome und Quotienten davon, auf elliptischen Kurven genauer anschauen. Insbesondere sind für Divisoren die Definition und Untersuchung von Null- und Polstellen essentiell. Dazu folgen wir [Wal10, Kapitel 3]. In diesem Kapitel gehen wir stets davon aus, dass K ein algebraisch abgeschlossener Körper ist. Wir benötigen zunächst einige Definitionen.

Definition 4.4 *Für eine elliptische Kurve $E(K)$ bezeichnen wir*

$$K[E] := K[x,y]/\langle y^2 - x^3 - Ax - B\rangle$$

als die Menge der Polynome auf $E(K)$.

Bemerkung 4.5 *Da wir in der Definition 4.4 in den Quotienten übergehen, können wir in einem Polynom $f \in K[E]$ jedes y^2 durch $x^3 + Ax + B$ ersetzen. So kann f geschrieben werden als $f(x,y) = v(x) + yw(x)$ für $v, w \in K[x]$. Dies nennen wir die kanonische Form von f.*

Beispiel 4.6 *Sei $f(x,y) = y^3x^2 + x - yx + 1 \in K[E]$. Ersetzen wir y^2, erhalten wir*

$$\begin{aligned} f(x,y) &= y^3x^2 + x - yx + 1 \\ &= y(x^3 + Ax + B)x^2 + x - yx + 1 \\ &= x + 1 + y(x^5 + Ax^3 + Bx^2 - x) \\ &= v(x) + yw(x) \end{aligned}$$

für $v(x) := x + 1$ und $w(x) = x^5 + Ax^3 + Bx^2 - x$.

Satz 4.7 *$K[E]$ ist ein Integritätsring, also nullteilerfrei.*

Beweis Sei $K[x] + yK[x]$ der Ring, der in Bemerkung 4.5 beschrieben wird. Bei der Multiplikation ersetzen wir also jedes y^2 durch $x^3 + Ax + B$. Die Ringeigenschaften übertragen sich dabei trivialerweise. Nach Bemerkung 4.5 sind die Ringe $K[x,y]/\langle y^2 - x^3 - Ax - B\rangle \approx K[x] + yK[x]$ isomorph. Für letzteren können wir die Nullteilerfreiheit nachrechnen. Seien dafür $f_1, f_2, g_1, g_2 \in K[x]$ und $h_1(x,y) = f_1(x) + yg_1(x), h_2(x,y) = f_2(x) + yg_2(x) \in K[x] + yK[x]$. Angenommen $h_1(x,y)h_2(x,y) = 0$, dann gilt:

$$\begin{aligned} 0 &= (f_1(x) + yg_1(x))(f_2(x) + yg_2(x)) \\ &= f_1(x)f_2(x) + yf_1(x)g_2(x) + yg_1(x)f_2(x) + y^2g_1(x)g_2(x) \\ &= f_1(x)f_2(x) + (x^3 + Ax + B)(g_1(x)g_2(x)) + y(f_1(x)g_2(x) + g_1(x)f_2(x)) \end{aligned}$$

Da die ersten beiden Terme von y unabhängig sind, muss $f_1(x)g_2(x) + g_1(x)f_2(x) = 0$ und $f_1(x)f_2(x) + (x^3 + Ax + B)(g_1(x)g_2(x)) = 0$ sein. Wir unterscheiden zwei Fälle.

- Seien zunächst $f_1(x) = 0 = f_2(x)$. Dies impliziert aber $(x^3 + Ax + B)(g_1(x)g_2(x)) = 0$, also wieder aufgrund der Nullteilerfreiheit von $K[x]$, dass $g_1(x) = 0$ oder $g_2(x) = 0$. Beides ist ein Widerspruch. Analog verläuft der Fall, wenn $g_1(x) = 0 = g_2(x)$.

- Seien alle Polynome f_1, f_2, g_1, g_2 ungleich Null. Dann folgt mithilfe des Gradsatzes und $f_1(x)g_2(x) + g_1(x)f_2(x) = 0$, dass $\deg(f_1) + \deg(g_2) = \deg(g_1) + \deg(f_2)$. Aus $f_1(x)f_2(x) + (x^3 + Ax + B)(g_1(x)g_2(x)) = 0$ folgt $\deg(f_1) + \deg(f_2) = 3 + \deg(g_1) + \deg(g_2)$. Ineinander eingesetzt erhalten wir $2(\deg(f_2) - \deg(g_2)) = 3$. Dies ist ein Widerspruch, da $\deg(f_2) \in \mathbb{N}$ und $\deg(g_2) \in \mathbb{N}$. □

Definition 4.8 *Für eine elliptische Kurve $E(K)$ definieren wir die Menge der rationalen Funktionen auf $E(K)$ als*

$$K(E) := (K[E] \times K[E] \backslash \{0\})/\sim$$

mit folgender Äquivalenzrelation: Seien $(f, g), (h, k) \in K[E] \times K[E] \backslash \{0\}$:

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

Wir bezeichnen die Äquivalenzklasse von $(f, g) \in K(E)$ mit $\frac{f}{g}$. Wir nennen eine rationale Funktion $r \in K(E)$ an einem Punkt $P \in E(K) \backslash \{O\}$ endlich, falls ein Repräsentant $r = \frac{f}{g}$ mit $f, g \in K[E]$ und $g(P) \neq 0$ existiert. In diesem Fall definieren wir $r(P) := \frac{f(P)}{g(P)}$. Ist r an einem Punkt P nicht endlich, schreiben wir $r(P) = \infty$.

Satz 4.9 *Die Relation aus Definition 4.8 ist wohldefiniert.*

Beweis Reflexivität: Seien $f, g \in K[E]$. Dann ist $fg = fg$ und somit $(f, g) \sim (f, g)$.

Symmetrie: Seien $(f, g), (h, k) \in K[E]^2$. Dann ist

$$\begin{aligned}(f, g) \sim (h, k) &\Leftrightarrow fk = gh \\ &\Leftrightarrow gh = fk \\ &\Leftrightarrow (h, k) \sim (f, g).\end{aligned}$$

Transitivität: Seien $(f, g), (h, k), (l, m) \in K[E]^2$ und $(f, g) \sim (h, k)$ sowie $(h, k) \sim (l, m)$. Dann ist $(f, g) \sim (h, k) \Leftrightarrow fk = gh \Leftrightarrow fkl = ghl$. Zusammen mit $(h, k) \sim (l, m) \Leftrightarrow hm = kl$ folgt $(f, g) \sim (h, k) \Leftrightarrow fhm = ghl \Leftrightarrow fm = gl \Leftrightarrow (f, g) \sim (l, m)$. □

Definition 4.10 *Sei $f \in K[E]$ in kanonischer Form $f(x, y) = v(x) + yw(x)$. Dann definieren wir*

- *das Konjugierte von f als $\bar{f}(x, y) := v(x) - yw(x)$,*
- *die Norm von f als $N_f := f\bar{f} \in K[E]$.*

Bemerkung 4.11 *Auch für rationale Funtionen können wir eine kanonische Form herleiten. Dafür stellen wir zunächst fest, dass die Norm eines Polynoms $f(x, y) = v(x) + yw(x) \in K[E]$ in kanonischer Form von y unabhängig ist:*

$$\begin{aligned}N_f(x, y) &= f(x, y)\bar{f}(x, y) \\ &= (v(x) + yw(x))(v(x) - yw(x)) \\ &= v(x)^2 - y^2 w(x)^2 \\ &= v(x)^2 - (x^3 + Ax + B)w(x)^2\end{aligned}$$

Sei nun $r = \frac{f}{g} \in K(E)$. *Damit gilt*

$$\frac{f}{g} = \frac{f\bar{g}}{g\bar{g}} = \frac{f\bar{g}}{N_g}.$$

Schreiben wir $(f\bar{g})(x, y) = v(x) + yw(x)$ *in kanonischer Form, so erhalten wir*

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

als kanonische Form für rationale Funktionen.

Wie wir eine rationale Funktion an den affinen Punkten einer elliptischen Kurve auswerten, ist damit klar. Als nächstes wollen wir definieren, wie wir eine rationale Funktion an O auswerten. Dafür benötigen wir, wie wir sehen werden, den Grad einer rationalen Funktion. Da diese allerdings in zwei Variablen gegeben sind, ist dies nicht so einfach wie für ein Polynom mit einer Variablen. Die Gleichung $y^2 = x^3 + Ax + B$ legt nahe, dass der Grad von y „$\frac{2}{3}$ so viel sein sollte“ wie der von x.

Definition 4.12 *Sei* $f(x, y) = v(x) + yw(x) \in K[E]$ *in kanonischer Form. Dann definieren wir den Grad von* f *als*

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

wobei $\deg_x(g)$ *den Grad eines Polynoms* $g \in K[x]$ *bezeichnet. Außerdem setzen wir* $\deg(0) = -\infty$.

Wir halten noch eine Eigenschaft des Grads fest.

Satz 4.13 *Für* $f, g \in K[E]$ *gilt*

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

Beweis Teile dieses Beweises sind aus [Wal10, Lemma 3.13 und Lemma 3.14] übernommen.

Seien zunächst $f(x, y) = v_1(x) + yw_1(x), g(x, y) = v_2 + yw_2(x) \in K[E]$. Dann gilt

$$\begin{aligned}
\overline{fg} &= \overline{(v_1(x) + yw_1(x))(v_2 + yw_2(x))} \\
&= \overline{v_1(x)v_2(x) + yv_1(x)w_2(x) + yw_1(x)v_1(x) + y^2w_1(x)w_2(x)} \\
&= v_1(x)v_2(x) + y^2w_1(x)w_2(x) - yv_1(x)w_2(x) - yw_1(x)v_1(x) \\
&= (v_1(x) - yw_1(x))(v_2 - yw_2(x)) \\
&= \overline{(v_1(x) + yw_1(x))(v_2 + yw_2(x))} \\
&= \bar{f}\bar{g}.
\end{aligned}$$

Damit können wir jetzt zeigen, dass

$$\begin{aligned}
N_{fg} &= fg\overline{fg} \\
&= f\bar{f}g\bar{g} \\
&= N_fN_g.
\end{aligned}$$

Außerdem können wir noch folgende Eigenschaft herleiten. Sei $f(x,y) = v(x) + yw(x) \in K[E]$ wieder in kanonischer Form. Dann ist $N_f = (v(x) + yw(x))(v(x) - yw(x)) = v(x)^2 - y^2w(x)^2 = v(x)^2 - (x^3 + Ax + B)w(x)^2$. Damit erhalten wir

$$\begin{aligned}\deg_x(N_f) &= \deg_x(v(x)^2 - (x^3 + Ax + B)w(x)^2) \\ &= \max\{\deg_x(v(x)^2), \deg_x((x^3 + Ax + B)w(x)^2)\} \\ &= \max\{\deg_x(2v(x)), \deg_x(3 + 2w(x))\} \\ &= \deg(f).\end{aligned}$$

Damit haben wir alle Eigenschaften zusammengetragen, damit wir den Satz beweisen können:

$$\begin{aligned}\deg(fg) &= \deg_x(N_{fg}) \\ &= \deg_x(N_f N_g) \\ &= \deg_x(N_f) + \deg_x(N_g) \\ &= \deg(f) + \deg(g)\end{aligned}$$

□

Bemerkung 4.14 *Aus dem Beweis von Satz 4.13 erhalten wir noch zwei Eigenschaften der Norm. Sind $f, g \in K[E]$, so gilt zum einen $N_{fg} = N_f N_g$, sowie $\deg_x(N_f) = \deg(f)$.*

Wo es zwar keinen Sinn ergibt, über den Grad des Zählers oder Nenners einer rationalen Funktion für sich zu sprechen, stellen wir für zwei Repräsentanten $r = \frac{f}{g} = \frac{h}{k} \in K(E)$ mithilfe von Satz 4.13 fest, dass

$$\deg(f) - \deg(g) = \deg(h) - \deg(k).$$

Damit können wir die Auswertung einer rationalen Funktion an O definieren.

Definition 4.15 *Sei $r = \frac{f}{g} \in K(E)$. Wir unterscheiden folgende Fälle:*

- $\deg(f) < \deg(g)$*: Setze $r(O) = 0$.*
- $\deg(f) > \deg(g)$*: Wir sagen, r ist nicht endlich an O.*
- $\deg(f) = \deg(g)$ *und* $\deg(f)$ *ist gerade: Schreibe f und g in kanonischer Form. Beide haben führende Terme der Form ax^d und bx^d für $a, b \in K$ und $d = \frac{\deg(f)}{2}$ und wir setzen $r(O) = \frac{a}{b}$.*
- $\deg(f) = \deg(g)$ *und* $\deg(f)$ *ist ungerade: Schreibe f und g in kanonischer Form. Beide haben führende Terme der Form ayx^d und byx^d für $a, b \in K$ und $d = \frac{\deg(f)-3}{2}$ und wir setzen $r(O) = \frac{a}{b}$.*

Nachdem wir uns jetzt die Auswertung rationaler Funktionen angeschaut haben, widmen wir uns nun der Definition und Untersuchung von deren Nullstellen und Polen.

Definition 4.16 *Sei $r \in K(E)$. Wir sagen, dass r an $P \in E(K)$ eine Nullstelle hat, wenn $r(P) = 0$ gilt. r hat an P einen Pol, wenn $r(P)$ nicht endlich ist.*

Zusätzlich sind wir auch an der Vielfachheit einer Nullstelle oder eines Pols interessiert. Dies benötigt allerdings etwas Vorarbeit.

Definition 4.17 *Sei $P \in E(K)$ ein Punkt auf einer elliptischen Kurve $E(K)$. Wir nennen eine Funktion $u \in K(E)$ mit $u(P) = 0$ einen Uniformizer an P, wenn sie folgende Eigenschaft hat: $\forall r \in K(E)\backslash\{0\} \exists d \in \mathbb{Z}, s \in K(E)$ endlich an P mit $s(P) \neq 0$, so dass*

$$r = u^d s.$$

Diese Definition erinnert schon an die Definition der Vielfachheit einer Nullstelle für klassische Polynome. Um dies für elliptische Kurven aber sinnvoll definieren zu können, müssen wir zunächst zeigen, dass ein Uniformizer für jeden Punkt einer elliptischen Kurve existiert. Dafür müssen wir einige Fälle unterscheiden.

Satz 4.18 *Sei $E(K)$ eine elliptische Kurve und $P = (a, b) \in E(K)\backslash E[2]$ ein Punkt in der affinen Ebene. Dann ist die Funktion $u(x, y) := x - a$ ein Uniformizer an P.*

Beweis Wir folgen dem Beweis in [Wal10, Lemma 4.3].

Wir stellen als erstes fest, dass $u(a, b) = a - a = 0$. Sei nun $r \in K(E)\backslash\{0\}$ beliebig. Hat r an P weder eine Nullstelle noch einen Pol, so setzen wir $d = 0$ und $s = r$ und sind fertig.

Sei deswegen zunächst $r(P) = 0$. Dann können wir r schreiben als $r = \frac{f}{g}$ mit $f(P) = 0$ und $g(P) \neq 0$. Schaffen wir es f als $f = u^d s$ zu zerlegen, können wir r folgendermaßen schreiben:

$$r = \frac{f}{g} = \frac{u^d s}{g} = u^d \frac{s}{g}.$$

Damit haben wir $\tilde{s} := \frac{s}{g} \in K(E)$ wie gewünscht gefunden.

Um dieses d und s zu finden wiederholen wir folgenden Prozess. Sei zunächst $s_0(x, y) := f(x, y)$. Während $s_i(P) = 0$ ist, schreiben wir $s_i(x, y) = v_i(x) + y w_i(x)$ in kanonischer Form und unterscheiden dann die Fälle $\overline{s_i}(P) = 0$ und $\overline{s_i}(P) \neq 0$.

$\overline{s_i}(P) = 0$: Da $P \notin E[2]$, gilt $y(P) = b \neq 0$. So ist das lineare Gleichungssystem

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

eindeutig lösbar und wir erhalten $v_i(a) = w_i(a) = 0$. Dadurch erhalten wir

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

für $s_{i+1}(x, y) = v_{i+1}(x) + y w_{i+1}(x)$ und geeigneten Polynomen $v_{i+1}, w_{i+1} \in K[x]$.

$\overline{s_i}(P) \neq 0$: Wir multiplizieren s_i mit $1 = \frac{\overline{s_i}}{\overline{s_i}}$ und erhalten

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

Da $s_i(P) = 0$ und $\overline{s_i}(P) \neq 0$ ist, erhalten wir $N_{s_i}(a) = 0$ und können $N_{s_i}(x) = (x - a) n_i(x)$ mit geeignetem $n_i \in K[x]$ schreiben. Setzen wir $s_{i+1}(x, y) := \frac{n_i(x)}{\overline{s_i}(x, y)}$, so erhalten wir

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

Terminiert dieser Prozess, so bekommen wir

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

für ein $i \in \mathbb{N}$, wobei $s := s_i$ Nicht-Null ist. Mit $u(x,y) = x - a$ und $d := i$ haben wir die gesuchte Zerlegung gefunden.

Da s_i eine rationale Funktion ist, müssen wir noch zeigen, dass dieser Prozess auch wirklich terminiert. Dazu berechnen wir

$$\begin{aligned} N_f(x) &= N_{u(x,y)^i s_i(x,y)}(x) \\ &= u(x,y)^i s_i(x,y)\overline{u(x,y)^i s_i(x,y)} \\ &= (x-a)^i s_i(x,y)(x-a)^i\overline{s_i(x,y)} \\ &= (x-a)^{2i} s_i(x,y)\overline{s_i(x,y)} \\ &= (x-a)^{2i} N_{s_i}(x). \end{aligned}$$

Dies zeigt uns, dass $\deg_x(N_f) = 2i + deg_x(N_{s_i}) \geq 2i$, womit i und damit die Anzahl der Iterationen durch eine endliche Zahl beschränkt ist.

Es fehlt nur noch der Fall, in dem r einen Pol an P hat. Dafür betrachten wir die Funktion $\frac{1}{r}$, welche an P eine Nullstelle hat und können somit das gleiche u mit negativem d nehmen. □

Satz 4.19 *Sei $E(K)$ eine elliptische Kurve und $P \in E[2]\backslash\{O\}$. Dann ist $u(x,y) := y$ ein Uniformizer an P.*

Beweis Wir folgen dem Beweis in [Wal10, Lemma 4.4].

Wir erinnern uns zunächst daran, dass $E[2] = \{O, (e_1,0), (e_2,0), (e_3,0)\}$, wobei $e_1, e_2, e_3 \in K$ die Nullstellen von $x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3)$ sind. Ohne Beschränkung der Allgemeinheit betrachten wir den Fall der ersten Nullstelle.

Wir stellen fest, dass $u(P) = 0$ ist. Sei nun $r \in K(E)\backslash\{0\}$ beliebig mit $r(P) = 0$, sodass sie die Form $r = \frac{f}{g}$ mit $f(P) = 0$ hat. Schreiben wir $f(x,y) = v(x) + yw(x)$ in kanonischer Form, impliziert das, dass $v(e_1) = 0$. Da v also einen Linearfaktor hat, können wir $v(x) = (x-e_1)v_1(x)$ für ein geeignetes Polynom v_1 schreiben. Da die drei Nullstellen e_1, e_2, e_3 unterschiedlich sind, gilt für $w_1(x) := w(x)(x-e_2)(x-e_3)$

$$\begin{aligned} f(x,y) &= (x-e_1)v_1(x) + yw(x) \\ &= \frac{(x-e_1)(x-e_2)(x-e_3)v_1(x) + yw_1(x)}{(x-e_2)(x-e_3)} \\ &= \frac{y^2 v_1(x) + yw_1(x)}{(x-e_2)(x-e_3)} \\ &= y\frac{yv_1(x) + w_1(x)}{(x-e_2)(x-e_3)} \\ &= u(x,y)W(x,y) \end{aligned}$$

mit $W(x,y) := \frac{yv_1(x)+w_1(x)}{(x-e_2)(x-e_3)}$. Ist $W(P) \neq 0$, sind wir fertig. Wenn nicht, können wir den Prozess mit W wiederholen. Dies ist, da v nur endlich viele Faktoren hat, nur endlich oft möglich und das Verfahren terminiert. □

Satz 4.20 *Sei $E(K)$ eine elliptische Kurve. Dann ist die Funktion $u(x,y) := \frac{x}{y}$ ein Uniformizer an $O \in E(K)$.*

Beweis Wir folgen dem Beweis in [Wal10, Lemma 4.5].

Da $deg(y) = 3 > 2 = deg(x)$, ist $u(0) = 0$. Sei nun $r = \frac{f}{g} \in K(E)\backslash\{0\}$ eine beliebige rationale Funktion mit $r(O) = 0$ oder $r(O)$ nicht endlich. Das bedeutet, dass $d := \deg(g) - \deg(f) \neq 0$. Wir wollen $s(x,y) = \left(\frac{y}{x}\right)^d r(x,y)$ setzen, welches also an O endlich und ungleich Null sein muss. Dann erhalten wir

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

Wir berechnen

$$\begin{aligned}\deg(y^d f(x,y)) - \deg(x^d g(x,y)) &= \deg(y^d) + \deg(f) - \deg(x^d) - \deg(g)\\ &= 3d + \deg(f) - 2d - \deg(g)\\ &= d + (\deg(f) - \deg(g))\\ &= 0,\end{aligned}$$

weswegen $s(x,y)$ tatsächlich endlich und ungleich Null ist. □

Wir fassen die letzten drei Sätze im folgenden Satz zusammen.

Satz 4.21 *Jeder Punkt auf einer elliptischen Kurve hat einen Uniformizer und die Zahl d in Definition 4.17 ist unabhängig von der Wahl dessen.*

Beweis Wir folgen dem Beweis in [Wal10, Theorem 4.6].

Die Existenz eines Uniformizers haben wir in den vorhergehenden Sätzen gezeigt. Es fehlt also nur noch, dass die Zahl d nicht von der Wahl des Uniformizers abhängig ist.

Seien dafür u und $\tilde{u}$ zwei Uniformizer an einem Punkt $P \in E(K)$. Da u und $\tilde{u}$ selbst rationale Funktionen sind, können wir $u = \tilde{u}^a q$ und $\tilde{u} = u^b p$ für geeignete $a, b \in \mathbb{Z}$ und $q, p \in K(E)$ endlich und nicht null an P schreiben. Damit können wir

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

berechnen. Wir nehmen zunächst $ab \neq 1$ an. Teilen wir durch u, so erhalten wir $1 = u^{ab-1}(p^a q)$. Werten wir dies an P aus, folgt daraus $1 = 0$, also muss $ab = 1$ sein. Nehmen wir zunächst an, es gilt $a = b = -1$. Damit erhalten wir

$$u = \tilde{u}^{-1} q \Leftrightarrow u\tilde{u} = q,$$

was, wenn wir es an P auswerten, zu $0 = u(P)\tilde{u}(P) = q(P) \neq 0$ führt. Also muss $a = b = 1$ gelten.

Sei nun $r \in K(E)\backslash\{0\}$ beliebig. Es existieren also $d, \tilde{d} \in \mathbb{Z}$ und $s, t \in K(E)$ endlich und nicht Null an P mit $r = u^d s$ und $r = \tilde{u}^{\tilde{d}} t$. Damit können wir $u^d s = \tilde{u}^{\tilde{d}} t = (up)^{\tilde{d}} t = u^{\tilde{d}}(p^{\tilde{d}} t)$ berechnen, was zu

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

führt. Auf der rechten Seiten stehen nur rationale Funktionen, welche endlich und an P nicht Null sind. Ist aber $d - \tilde{d} \neq 0$, so ist die linke Seite an P Null. Also gilt $d = \tilde{d}$. □

Das Wissen, dass die Zahl d an einem Punkt P immer gleich ist, erlaubt uns, sie als die Vielfachheit einer Nullstelle bzw. Pols zu definieren.

Definition 4.22 *Für eine elliptische Kurve $E(K)$ sei $P \in E(K)$ ein Punkt und u ein Uniformizer an P. Für $r \in K(E)\backslash\{0\}$ mit $r = u^d s$ nennen wir d die Ordnung von r an P und schreiben*

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

Die Vielfachheit einer Nullstelle ist die Ordnung an diesem Punkt und die Vielfachheit eines Pols das Negative der Ordnung.

Wir möchten zunächst die Ordnungen an bestimmten Punkten hervorheben.

Satz 4.23 *a. Sei $r \in K(E)$ und $P \in E(K)$, sodass $r(P) \neq 0$ und r an P endlich ist. Dann ist*

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

b. Sei $f \in K[E]$ und $P \in E(K)\backslash\{O\}$, sodass $f(P) \neq 0$. Dann ist

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

c. Für $f \in K[E]\backslash\{0\}$ gilt

$$\mathrm{ord}_O(f) = -\deg(f).$$

Beweis Für diesen Beweis folgen wir [Wal10, Proposition 4.9 - 4.11].

a. Wir wählen einen Uniformizer $u \in K(E)$ und setzen $s(x, y) = r(x, y)$. Letzteres ist nach Annahme endlich und nicht Null an P. Damit gilt

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

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

b. Da Polynome an allen Punkten endlich sind, folgt die Behauptung direkt aus dem vorhergehenden Teil.

c. Nach Satz 4.20 ist $u(x, y) = \frac{x}{y}$ ein Uniformizer an O. Mit $k := \deg(f)$ können wir $s(x, y) := \frac{x^k}{y^k} f(x, y)$ setzen. Diese muss nicht Null und endlich sein. Dies gilt da nach Satz 4.13 $\deg(x^k f(x, y)) = 2k + \deg(f) = 3k$ und $\deg(y^k) = 3k$ ist. Also können wir schreiben:

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

Damit ist $\mathrm{ord}(f) = -k = -\deg(f)$. □

Außerdem gelten folgende Rechenregeln.

Satz 4.24 *Seien $f, g \in K(E)\backslash\{0\}$, $c \in K\backslash\{0\}$ und $P \in E(K)$. Dann gilt*

- $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$,

- $\operatorname{ord}_P\left(\frac{f}{g}\right) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$,
- $\operatorname{ord}_P(cf) = \operatorname{ord}_P(f)$.

Beweis
- Mit den Sätzen 4.18 bis 4.21 können wir davon ausgehen, dass die Uniformizer u von f und g gleich sind. Für Punkt P gilt also $f = u^d s$ und $g = u^{d'} t$ für $d, d' \in K$ und Funktionen $s, t \in K(E)$ endlich, welche an P ungleich 0 sind. Es gilt also

  $$fg = u^d s u^{d'} t = u^{d+d'} st.$$

  $s \cdot t$ ist noch immer eine endliche Funktion und ungleich 0 an P, also ist $\operatorname{ord}_P(st) = d + d'$.
- $\operatorname{ord}_P\left(\frac{f}{g}\right) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$ wird analog bewiesen.
- Sei u ein Uniformizer an P, es gilt also $f = u^d s$ für $d \in K$ und $s \in K(E)$ endlich an P mit $s(P) \neq 0$. Also gilt auch $cf = cu^d s = u^d cs$. Die Funktion $c \cdot s$ ist wieder endlich und ungleich 0 an P, was den Beweis abschließt. □

Als nächstes schauen wir uns eine wichtige Eigenschaft des Grades an.

Satz 4.25 *Für $f \in K[E]$ gilt*

$$\deg(f) = \sum_{\substack{P \in E(K) \\ f(P)=0}} \operatorname{ord}_P(f). \tag{4.1}$$

Beweis Wir folgen dem Beweis in [Wal10, Lemma 4.16].

Sei $n := \deg(f)$. Mit Bemerkung 4.14 folgt, dass $n = \deg_x(N_f)$. Wir können also

$$(f\bar{f})(x) = N_f(x) = \prod_{i=1}^{n}(x - a_i) \tag{4.2}$$

mit nicht notwendigerweise unterschiedlichen $a_i \in K$ schreiben.

Wir schauen uns nun erst allgemein an, was mit Nullstellen von Polynomen in $K[x]$ passiert, wenn wir sie über $K[E]$ betrachten. Sei also $f \in K[x]$ mit

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

mit $g \in K[x], g(a) \neq 0, k \in \mathbb{N}_{>0}, a \in K$. f hat an a also eine Nullstelle der Ordnung k.

Wir betrachten zunächst den Fall, wo $a^3+Aa+B \neq 0$ und damit die Punkte $P = (a, \pm\sqrt{a^3 + Aa + B}) \notin E[2]$ liegen. Wir betrachten f jetzt als Polynom $f \in K[E]$ und wählen nach Satz 4.18 den Uniformizer $u(x, y) = x - a$ an P. Damit können wir f als

$$f(x, y) = (x - a)^k g(x) = u(x, y)^k g(x)$$

schreiben, was $\operatorname{ord}_P(f) = k$ impliziert.

Seien jetzt $e_1, e_2, e_3 \in K$ die Nullstellen von $x^3 + Ax + B$ und ohne Beschränkung der Allgemeinheit $a = e_1$. Wir betrachten den Punkt $P = (a, 0)$ mit Uniformizer $u(x, y) = y$ nach Satz 4.19. Setzen wir $s(x, y) = \frac{g(x)}{(x-e_2)^k(x-e_3)^k}$, so erhalten wir

$$\begin{aligned} f(x, y) &= (x - a)^k g(x) \\ &= y^{2k} \frac{(x - a)^k g(x)}{y^{2k}} \\ &= y^{2k} \frac{(x - a)^k g(x)}{(x - e_1)^k (x - e_2)^k (x - e_3)^k} \\ &= y^{2k} \frac{g(x)}{(x - e_2)^k (x - e_3)^k} \\ &= u(x, y)^{2k} s(x, y). \end{aligned}$$

Damit ist $\mathrm{ord}_P(f) = 2k$.

Wir kehren jetzt zum Beweis des Satzes selbst zurück. Wie wir gerade gesehen haben, erhalten wir für jede Nullstelle a_i in Gleichung 4.2 zwei Nullstellen auf E. Im ersten Fall die beiden einfachen Nullstellen $(a, \pm\sqrt{a^3 + Axa + B})$, im zweiten Fall die doppelte Nullstelle $(a, 0)$. Zählen wir die Vielfachheiten, so hat $f\bar{f}$ $2n$ Nullstellen auf $E(K)$. Da f und $\bar{f}$ gleich viele Nullstellen auf $E(K)$ haben, hat f mit Vielfachheiten genau n Nullstellen. Dies ist aber genau die rechte Seite von Gleichung 4.1. □

Bemerkung 4.26 *Aus der Argumentation im Beweis von Satz 4.25 folgt auch, dass ein Polynom $f \in K[E]$ nur endlich viele Nullstellen auf $E(K)$ hat. Betrachten wir den Kehrwert des Polynoms, so gilt dies auch für Polstellen.*

Satz 4.27 *Für $r \in K(E)$ gilt*

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

Beweis Wir folgen dem Beweis in [Wal10, Theorem 4.17].

Für eine rationale Funktion $r = \frac{h}{g} \in K(E)$ gilt

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

Daher genügt es, die Behauptung für ein Polynom $f \in K[E]$ zu zeigen. Mit Satz 4.23 und Satz 4.25 folgt

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

Mit Satz 4.23 folgt außerdem $\mathrm{ord}_O(f) = -\deg(f)$, was das Ergebnis liefert. □

Satz 4.28 *Sei $r = \frac{h}{g} \in K(E)$ eine rationale Funktion. Hat r keine Null- und Polstellen, so ist r konstant.*

Beweis Nach Satz 4.25 ist

$$\deg(h) = \sum_{\substack{P \in E(K) \\ h(P)=0}} ord_P(h) = 0.$$

Also ist h konstant. Mit der selben Argumentation zeigt man auch, dass g konstant ist, woraus folgt, dass r konstant ist. □

4.2.2 Endomorphismen

In diesem Abschnitt wollen wir zeigen, dass bestimmte Abbildungen zwischen elliptischen Kurven entweder trivial oder surjektiv sind. Dies werden wir später insbesondere für die Multiplikation eines Punktes mit n benötigen. Wir folgen für diesen Abschnitt [Was08, Abschnitt 2.9].

Definition 4.29 *Als Endomorphismus einer elliptischen Kurve $E(K)$ bezeichnen wir einen Homomorphismus $\alpha : E_K(\bar{K}) \to E_K(\bar{K})$, der durch rationale Funktionen gegeben ist. Das heißt, α is linear und es existieren rationale Funktionen $R_1(x, y), R_2(x, y) \in \bar{K}(E)$, sodass*

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)).$$

Beispiel 4.30 *Wir erinnern uns an die Formeln für die Addition von Punkten auf einer elliptischen Kurve aus Satz 3.25. Seien dafür $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_K(\bar{K})$. Mit $m = \frac{y_2 - y_1}{x_2 - x_1}$ gilt*

$$P_3 = (x_3, y_3) = P_1 + P_2 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1).$$

Mit $m = \frac{3x_1^2 + A}{2y_1}$ gilt

$$P_3 = (x_3, y_3) = 2P_1 = (m^2 - 2x_1, m(x_1 - x_3) - y_1).$$

Betrachten wir letztere Abbildung genauer, so sehen wir, dass sie ein Homomorphismus und durch rationale Funktionen geben ist. Demnach ist sie nach obiger Definition ein Endomorphismus. Verknüpfen wir diese noch mit der Addition eines Punktes, bzw. in diesem Fall mit dem ursprünglichen Punkt, so erhalten wir, dass nP für alle $n \in \mathbb{Z}$ ein Endomorphismus ist. Aufpassen müssen wir nur in Körpern K mit $\mathrm{char}(K) \neq 0$. *Dann ist die Abbildung nP für $n \in \mathbb{Z}$ mit* $\mathrm{char}(K) | n$ *nämlich die Nullabbildung und dadurch nach Definition kein Endomorphismus.*

Bemerkung 4.31 *Wie zuvor können wir auch für Endomorphismen eine kanonische Form herleiten. Dafür erinnern wir uns zunächst an die kanonische Form für rationale Funktionen. Sei dafür $R(x, y) \in \bar{K}(E)$ und $v, w \in \bar{K}[E]$. Dann können wir nach Bemerkung 4.11 schreiben*

$$R(x, y) = \frac{v(x) + yw(x)}{N_g}.$$

Wir betrachten jetzt einen Endomorphismus

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)).$$

Da α ein Homomorphismus ist, gilt

$$\begin{aligned}(R_1(x,-y),R_2(x,-y)) &= \alpha(x,-y)\\ &= \alpha(-(x,y))\\ &= -\alpha(x,y)\\ &= -(R_1(x,y),R_2(x,y))\\ &= (R_1(x,y),-R_2(x,y)).\end{aligned}$$

Die zweite Gleichheit folgt dabei aus der Herleitung der Formel in Satz 3.25 b. Wir folgern, dass

$$R_1(x,-y) = R(x,y) \text{ und } R_2(x,-y) = -R_2(x,y).$$

Ist R_1 in kanonischer Form geschrieben, können wir also annehmen, dass $w(x) = 0$ ist. Ebenso gilt für R_2, dass $v(x) = 0$ ist. Zusammen ergibt das

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

mit rationalen Funktionen $r_1(x), r_2(x) \in \bar{K}(x)$.

Interessant ist jetzt noch zu betrachten, was passiert, wenn eine der rationalen Funktionen an einem Punkt nicht definiert ist. Sei dafür $r_1(x) = \frac{p(x)}{q(x)}$. Sollte $q(x) = 0$ sein für einen Punkt (x,y), dann setzen wir $\alpha(x,y) = O$. Die anderen Fälle beantwortet der folgende Satz.

Satz 4.32 *Sei $\alpha(x,y) = (r_1(x), r_2(x)y)$ ein Endomorphismus und $r_1(x) = \frac{p(x)}{q(x)}, r_2(x) = \frac{s(x)}{t(x)}$ mit $p,q,s,t \in \bar{K}[x]$. Ist r_1 definiert, also $q(x) \neq 0$, so ist auch r_2 definiert, also $t(x) \neq 0$.*

Beweis Seien r_1 und r_2 vollständig gekürzt, also haben p und q sowie s und t keine gemeinsamen Nullstellen. Da $\alpha(x,y) = (r_1(x), r_2(x)y)$ auf $E_K(\bar{K})$ liegt, gilt

$$\begin{aligned}&\left(y\frac{s(x)}{t(x)}\right)^2 = \left(\frac{p(x)}{q(x)}\right)^3 + A\frac{p(x)}{q(x)} + B\\ \Leftrightarrow\ &\frac{(x^3+Ax+B)s(x)^2}{t(x)^2} = \frac{p(x)^3 + p(x)q(x)^2 + Bq(x)^3}{q(x)^3}\\ \Leftrightarrow\ &\frac{(x^3+Ax+B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}\end{aligned}$$

für $u(x) = p(x)^3 + p(x)q(x)^2 + Bq(x)^3$.

u und q haben keine gemeinsamen Nullstellen. Angenommen x_0 wäre eine gemeinsame Nullstelle, dann ist insbesondere $q(x_0) = 0$. Damit folgt

$$0 = u(x_0) = p(x_0)^3 + p(x_0)q(x_0)^2 + Bq(x_0)^3 = p(x_0)^3,$$

also auch $p(x_0) = 0$. Dies ist aber ein Widerspruch zur Annahme, dass p und q teilerfremd sind.

Sei jetzt x_1 eine Nullstelle von t, also $t(x_1) = 0$. Da s und t teilerfremd sind, haben $s(x)^2$ und $t(x)^2$ keine gemeinsamen Nullstellen, also ist $s(x)^2 \neq 0$. Wir nehmen jetzt an, $q(x_1) \neq 0$. Da $x^3 + Ax + B$ keine mehrfachen Nullstellen hat, unterscheiden wir zwei Fälle.

Seien zunächst $x^3 + Ax + B$ und $t(x)$ teilerfremd. Dann ist $x_1^3 + Ax_1 + B \neq 0$ und

$$0 \neq (x_1^3 + Ax_1 + B)s(x_1)^2 q(x_1)^3 = u(x_1)t(x_1)^2 = 0,$$

was ein Widerspruch ist.

Sei jetzt x_1 auch eine Nullstelle von $x^3 + Ax + B$. Dann existieren zwei Polynome $v, w \in K[x]$ mit $x^3 + Ax + B = v(x)(x - x_1)$ und $t(x)^2 = w(x)(x - x_1)$. Da $x^3 + Ax + B$ nach Beispiel 3.21 keine mehrfachen Nullstellen hat, sind v und w teilerfremd und, da alle Nullstellen in $t(x)^2$ doppelt sind, $w(x_1) = 0$. Nach Kürzen von $(x - x_1)$ gilt

$$0 \neq v(x_1)s(x_1)^2 q(x_1)^3 = u(x_1)w(x_1) = 0.$$

Erneut ein Widerspruch.

Also muss auch $q(x_1) = 0$ sein, wodurch der Satz durch Kontraposition bewiesen ist. □

Definition 4.33 *Sei α ein Endomorphismus in kanonischer Form und außerdem $r_1(x) = \frac{p(x)}{q(x)}$. Wir definieren den Grad von α als*

$$\deg(\alpha) = \max\{\deg(p(x)), \deg(q(x))\},$$

sollte α nicht trivial sein. Ist $\alpha = 0$, so ist $\deg(\alpha) = 0$.

Außerdem nennen wir einen Endomorphismus $\alpha \neq 0$ separabel, wenn die Ableitung $r_1'(x)$ nicht konstant Null ist.

Satz 4.34 *Sei $\alpha \neq 0$ ein separabler Endomorphismus auf einer elliptischen Kurve $E_K(\bar{K})$. Dann gilt*

$$\deg(\alpha) = |\mathrm{Ker}(\alpha)|,$$

wobei $\mathrm{Ker}(\alpha)$ *den Kern des Homomorphismus α bezeichnet.*

Ist $\alpha \neq 0$ nicht separabel, so gilt

$$\deg(\alpha) > |\mathrm{Ker}(\alpha)|.$$

Beweis Für diesen Beweis folgen wir [Was08, Proposition 2.21].

Wir schreiben wie zuvor $\alpha(x, y) = (r_1(x), yr_2(x))$ mit $r_1(x) = \frac{p(x)}{q(x)}$. Ist α separabel, so ist $r_1' = \frac{p'q - pq'}{q^2} \neq 0$, also ist auch $p'q - pq' \neq 0$.

Sei $S = \{x \in \bar{K} | (pq' - p'q)(x)q(x) = 0\}$. Sei $(a, b) \in E_K(\bar{K})$ so gewählt, dass

a. $a \neq 0, b \neq 0, (a, b) \neq O$,

b. $\deg(p(x)) - aq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$,

c. $a \notin r_1(S)$,

d. $(a, b) \in \alpha(E_K(\bar{K}))$.

Wieso existiert ein solches (a, b)? $r_1(x)$ nimmt unendlich viele verschiedene Werte an, während x durch $\bar{K}$ läuft. Da auch für jedes x ein Punkt $(x, y) \in E_K(\bar{K})$ existiert, ist $\alpha(E_K(\bar{K}))$ eine unendliche Menge. Für Eigenschaft d haben wir also eine unendliche Anzahl an Punkten zur Auswahl. Eigenschaft a und b reduzieren diese Auswahl offensichtlich nur um eine endliche Anzahl. Da nach Annahme $pq' - p'q$ nicht das Null Polynom ist, ist S eine endliche Menge. Also ist auch ihr Bild unter α bzw. r_1 endlich. Zusammen können wir schließen, dass ein solches (a, b) existiert.

Wir wollen zeigen, dass genau $\deg(\alpha)$ viele Punkte $(x_1, y_1) \in E_K(\bar{K})$ existieren, so dass $\alpha(x_1, y_1) = (a, b)$. Für einen solchen Punkt gilt

$$\frac{p(x_1)}{q(x_1)} = a \text{ und } y_1 r_2(x_1) = b.$$

Da $(a, b) \neq O$, muss $q(x_1) \neq 0$ sein. Nach Satz 4.32 ist auch $r_2(x_1)$ definiert. Da $b \neq 0$ ist, gilt $y_1 = \frac{b}{r_2(x_1)}$. y_1 ist also vollständig durch x_1 bestimmt, weswegen wir nur die verschiedenen Werte von x_1 zählen müssen.

Nach Annahme b hat $p(x) - aq(x)$ mit Vielfachheiten $\deg(\alpha)$ Nullstellen. Demnach müssen wir nur noch zeigen, dass $p - aq$ keine mehrfachen Nullstellen hat. Dafür nehmen wir an, dass x_0 eine mehrfache Nullstelle ist. Dann gilt

$$p(x_0) - aq(x_0) = 0 \text{ und } p'(x_0) - aq'(x_0) = 0.$$

Multiplizieren wir die Gleichungen $p = aq$ und $aq' = p'$ miteinander, erhalten wir

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Da $a \neq 0$ ist, muss x_0 eine Nullstelle von $pq' - p'q$ sein, also ist $x_0 \in S$. Damit erhalten wir $a = r_1(x_0) \in r_1(S)$, im Widerspruch zu c. Daraus folgt, dass $p - aq$ keine mehrfachen Nullstellen hat und damit $\deg(\alpha)$ verschiedene Nullstellen.

Nachdem es also $\deg(\alpha)$ Punkte (x_1, y_1) mit $\alpha(x_1, y_1) = (a, b)$ gibt, hat der Kern von α genau $\deg(\alpha)$ Elemente.

Ist α nicht separabel, dann können wir den gleichen Beweis wie oben führen, mit dem Unterschied, dass $p' - aq'$ immer das Nullpolynom ist. Also hat $p(x) - aq(x)$ immer mehrfache Nullstellen und damit weniger als $\deg(\alpha)$ Lösungen. □

Satz 4.35 *Sei $E(\bar{K})$ eine elliptische Kurve und sei $\alpha \neq 0$ ein Endomorphismus auf $E(K)$. Dann ist $\alpha : E_K(\bar{K}) \to E_K(\bar{K})$ surjektiv.*

Beweis Für diesen Beweis folgen wir [Was08, Theorem 2.22].

Sei $(a, b) \in E_K(\bar{K})$. Da α ein Homomorphismus ist und deswegen $\alpha(O) = O$, können wir annehmen, dass $(a, b) \neq O$. Sei außerdem $r_1(x) = \frac{p(x)}{q(x)}$ wie oben.

Wir nehmen zunächst an, dass $p(x) - aq(x)$ nicht konstant ist. Demnach hat es also eine Nullstelle x_0. Da p und q keine gemeinsamen Nullstellen haben, ist $q(x_0) \neq 0$. Wir wählen $y_0 \in \bar{K}$ als eine der beiden Wurzeln von $x_0^3 + Ax_0 + B$. Nach Satz 4.32 ist $\alpha(x_0, y_0)$ definiert und gleich (a, b') für ein $b' \in \bar{K}$. Da $b'^2 = a^3 + Aa + B = b^2$, ist $b = \pm b'$. Ist $b = b'$, sind wir fertig. Ansonsten gilt $\alpha(x_0, -y_0) = (a, -b') = (a, b)$.

Jetzt betrachten wir den Fall, bei dem $p - aq$ konstant ist. Nachdem $E_K(\bar{K})$ unendlich viele Punkte enthält und der Kern von α nach Satz 4.34 endlich ist, können nur endlich viele Punkte auf $E_K(\bar{K})$ auf einen Punkt mit gegebener x-Koordinate abbilden. Also muss entweder $p(x)$ oder $q(x)$ nicht konstant sein. Sind p und q zwei nicht konstante Polynome, gibt es höchstens eine Konstante a, sodass $p - aq$ konstant ist. Wäre nämlich a' eine andere solche Zahl, so wären $(a'-a)q = (p-aq)-(p-a'q)$ und $(a'-a)p = a'(p-aq)-a(p-a'q)$ konstant, was implizieren würde, dass p und q konstant sind. Es kann also höchstens zwei Punkte, nämlich (a, b) und $(a, -b)$ geben, die nicht im Bild von α liegen. Sei jetzt $(a_1, b_1) \in E_K(\bar{K})$ ein beliebiger anderer Punkt. Dann existiert ein $P_1 \in E_K(\bar{K})$ mit $\alpha(P_1) = (a_1, b_1)$. Wir können (a_1, b_1) so wählen, dass $(a_1, b_1) + (a, b) \neq (a, \pm b)$, sodass ein $P_2 \in E_K(\bar{K})$ mit $\alpha(P_2) = (a_1, b_1) + (a, b)$ existiert. Damit gilt

$$\alpha(P_2 - P_1) = (a, b) \text{ und } \alpha(P_1 - P_2) = (a, -b).$$

Also ist α surjektiv. □

Bemerkung 4.36 *Satz 4.35 gilt nicht nur für elliptische Kurven, sondern ganz allgemein für Kurven. Für einen Beweis dieser Aussage siehe beispielsweise [Har77, Proposition II.6.8].*

Beispiel 4.37 *Nach Beispiel 4.30 ist die Multiplikation mit n ein Endomorphismus, also ist auch Satz 4.35 anwendbar. Nachdem die Abbildung offensichtlich nicht trivial ist für $n \in \mathbb{Z}$ mit $\mathrm{char}(K) \nmid n$, ist sie surjektiv. Für alle $P \in E_K(\bar{K})$ finden wir also ein $Q \in E_K(\bar{K})$ mit $nQ = P$.*

4.2.3 Der Frobenius Endomorphismus und Hasses Theorem

In diesem Abschnitt werden wir uns einen wichtigen Endomorphismus, den Frobenius Endomorphismus, und eine Folgerung aus ihm genauer anschauen. Dies werden wir später für das Tate-Lichtenbaum-Pairing benötigen. Dafür folgen wir [Was08, Kapitel 4.2].

Definition 4.38 *Sei F_q ein endlicher Körper mit algebraischem Abschluss $\bar{F}_q$. Dann bezeichnen wir mit*

$$\begin{aligned} \phi_q : \bar{F}_q &\to \bar{F}_q \\ x &\mapsto x^q \end{aligned}$$

die Frobenius Abbildung. Diese können wir mit

$$\phi_q(x, y) = (x^q, y^q),\ \phi_q(O) = O$$

auch auf $E(\bar{F}_q)$ fortsetzen.

Diese Abbildung ist nach folgendem Satz wohldefiniert.

Satz 4.39 *Sei $E(\bar{F}_q)$ eine elliptische Kurve mit Koeffizienten in F_q und $(x, y) \in E_{F_q}(\bar{F}_q)$. Dann gilt*

a. $\phi_q(x, y) \in E_{F_q}(\bar{F}_q)$

b. $(x, y) \in E_{F_q}(F_q)$ *genau dann, wenn* $\phi_q(x, y) = (x, y)$.

Beweis Für den Beweis folgen wir [Was08, Lemma 4.5].

a. Für diesen Teil müssen wir nur die Weierstraß Gleichung

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

mit q potenzieren und erhalten

$$\begin{aligned}&(y^2)^q = (x^3 + Ax + B)^q \\ &\Leftrightarrow (y^q)^2 = (x^q)^3 + Ax^q + B^q\end{aligned}$$

Dabei benutzen wir, dass wir in einem Körper mit Charakteristik q sind und deswegen gilt, dass $a^q = a$ für alle $a \in F_q$ und $(a + b)^q = a^q + b^q$ für alle $a, b \in \bar{F}_q$.

b. Wir zeigen zunächst, dass gilt

$$F_q = \{x \in \bar{F}_q | \phi_q(x) = x\}.$$

Die Inklusion $\subseteq$ ist klar, da für alle $x \in F_q$ gilt, dass $x^q = x$.

Für die andere Richtung erinnern wir uns, dass ein Polynom $g(x)$ genau dann eine mehrfache Nullstelle hat, wenn es und die Ableitung $g'(x)$ eine gemeinsame Nullstelle haben. Da aber

$$\frac{d}{dx}x^q - x = qx^{q-1} - 1 = -1$$

keine Nullstellen hat, hat das Polynom $x^q - x$ keine mehrfachen Nullstellen. Daher sind alle $\alpha \in \bar{F}_q$ mit $\alpha^q = \alpha$ unterschiedlich. Insbesondere gibt es auch q verschiedene davon.

Nachdem beide Seiten der Mengenungleichung gleich viele Elemente haben und die linke Seite in der rechten enthalten ist, müssen sie gleich sein.

Damit folgt schnell

$$\begin{aligned}(x, y) \in E(F_q) &\Leftrightarrow x, y \in F_q \\ &\Leftrightarrow \phi_q(x) = x \text{ und } \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y).\end{aligned}$$

□

Satz 4.40 *Sei $E_{F_q}(\bar{F}_q)$ eine elliptische Kurve mit Koeffizienten in F_q. Dann ist ϕ_q ein nicht separabler Endomorphismus von Grad q.*

Beweis Wir folgen dem Beweis in [Was08, Lemma 2.20].

Die Abbildung ist offensichtlich durch rationale Funktionen gegeben und ebenso ist klar, dass der Grad q ist. Wir zeigen zuerst, dass $\phi_q : E_{F_q}(\bar{F}_q) \to E_{F_q}(\bar{F}_q)$ ein Homomorphismus ist. Seien dafür $(x_1, y_1), (x_2, y_2) \in E_{F_q}(\bar{F}_q)$ mit $x_1 \neq x_2$. Die Summe ist gegeben durch

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

Potenzieren wir alles mit q, so erhalten wir

$$x_3^q = m'^2 - x_1^q - x_2^q,\ y_3^q = m'(x_1^q - x_3^q) - y_1^q,\ \text{wobei } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

Dabei nutzen wir, dass wir über den Körper $\bar{F}_q$ rechnen. Die letzten Gleichungen bedeuten nichts anderes als

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2).$$

Gilt $x_1 = x_2$, so ist $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = O$. Da auch $x_1^q = x_2^q$ in diesem Fall gilt, gilt auch $\phi_q((x_1, y_1)) + \phi_q((x_2, y_2)) = O$. Zusammen erhalten wir

$$\begin{aligned}\phi_q((x_1, y_1) + (x_2, y_2)) &= \phi_q(O)\\ &= O\\ &= \phi_q((x_1, y_1)) + \phi_q((x_2, y_2)).\end{aligned}$$

Der Fall, dass einer der Punkte O ist, wird gleich nachgerechnet. Zuletzt betrachten wir noch den Fall, dass ein Punkt zu sich selbst addiert wird. Die Formel zur Verdopplung $2(x_1, y_1) = (x_3, y_3)$ ist gegeben durch

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

Potenzieren wir wieder alles mit q, erhalten wir

$$x_3^q = m'^2 - 2x_1^q,\ y_3^q = m'(x_1^q - x_3^q) - y_1^q,\ \text{wobei } m' = \frac{3^q (x_1^q)^2 + A^q}{2^q y_1^q}.$$

Da $2, 3, A \in F_q$ sind, gilt $2^q = 2, 3^q = 3$ und $A^q = A$, woraus die Behauptung folgt.

Da $\frac{d}{dx}x^q = qx^{q-1} = 0$, ist ϕ_q nicht separabel. □

Das bringt uns zum abschließenden Satz dieses Kapitels.

Satz 4.41 (Hasses Theorem) *Sei $E(F_q)$ eine elliptische Kurve. Dann gilt*

$$|q + 1 - \#E(F_q)| \leq 2\sqrt{q}.$$

Beweis Den Beweis findet man beispielsweise in [Was08, Theorem 4.2]. □

4.3 Divisoren

Die Pairings werden später nicht einfach als Funktionen definiert, sondern in Abhängigkeit von Nullstellen. Dafür werden Divisoren ein wichtiges Hilfsmittel. Für diesen Abschnitt folgen wir [Was08, Kapitel 11.1].

Wie immer beginnen wir direkt mit der Definition der Divisoren.

Definition 4.42 *Sei $E(K)$ eine elliptische Kurve. Für jeden Punkt $P \in E(\bar{K})$ können wir das formale Symbol $[P]$ definieren. Ein Divisor ist dann eine endliche Linearkombination dieser Symbole mit Koeffizienten aus $\mathbb{Z}$:*

$$D = \sum_j a_j [P_j],\ a_j \in \mathbb{Z}.$$

Alle diese Elemente bilden eine freie abelsche Gruppe, erzeugt von den Symbolen $[P]$. Wir bezeichnen sie mit $\mathrm{Div}(E)$. *Zusätzlich definieren wir den Grad und die Summe eines Divisors mit*

$$\deg\left(\sum_j a_j [P_j]\right) = \sum_j a_j \in \mathbb{Z},$$
$$\mathrm{sum}\left(\sum_j a_j [P_j]\right) = \sum_j a_j P_j \in E(\bar{K}).$$

Für zwei Divisoren D und D' gilt für die beiden Abbildungen offensichtlicherweise $\deg(D + D') = \deg(D) + \deg(D')$ und $\mathrm{sum}(D + D') = \mathrm{sum}(D) + \mathrm{sum}(D')$.

Satz 4.43 *Die Divisoren von Grad 0, bezeichnet mit* $\mathrm{Div}^0(E)$, *bilden eine Untergruppe von* $\mathrm{Div}(E)$.

Beweis Für den Divisor $D = 0$ gilt, dass $a_j = 0$ für alle j und somit ist $\deg(D) = 0$. Also liegt das neutrale Element in $\mathrm{Div}^0(E)$.

Seien $D_1 = \sum_j a_j [P_j]$ und $D_2 = \sum_j b_j [P_j]$ aus $\mathrm{Div}^0(E)$. Dann ist

$$\deg(D_1 + D_2) = \sum_j a_j + b_j = \sum_j a_j + \sum_j b_j = 0.$$

Also ist $D_1 + D_2$ in $\mathrm{Div}^0(E)$. □

Das Ziel dieses Abschnitts über Divisoren ist, eine Beziehung zwischen ihnen und den Punkten auf der elliptischen Kurve herzustellen. Dafür betrachten wir zunächst die Abbildung

$$\mathrm{sum} : \mathrm{Div}^0(E) \to E(\bar{K}).$$

Diese ist zum einen ein Homomorphismus und zum anderen surjektiv. Sie ist surjektiv, da für alle $P \in E(\bar{K})$ gilt

$$\mathrm{sum}([P] - [O]) = P.$$

Sie ist allerdings nicht injektiv. Dafür betrachten wir für zwei Punkte $P_1, P_2 \in E(K)$ und $P_3 = P_1 + P_2$ den Divisor $D = [P_1] + P_2 + [-P_3]$. Für ihn gilt $\mathrm{sum}(D) = P_1 + P_2 - P_3 = P_3 - P_3 = O$. Also ist $\mathrm{Ker}(\mathrm{sum}) \neq O$ und die Abbildung damit nicht injektiv.

Es ist kein Zufall, dass der Divisor genau aus den Nullstellen einer Funktion, in diesem Fall einer Geraden, besteht. Dies wird genau der Kern der Funktion sum werden.

Definition 4.44 *Sei $f \in \bar{K}(E)$ nicht konstant Null. Dann definieren wir den Divisor der Funktion f als*

$$\operatorname{div}(f) = \sum_{P \in E(\bar{K})} \operatorname{ord}_P(f)[P] \in \operatorname{Div}(E).$$

Wir nennen den Divisor einer Funktion einen Principal Divisor. Die Menge aller dieser Divisoren bezeichnen wir mit $\operatorname{Prin}(E)$. *Diese ist nach Satz 4.27 eine Untergruppe von* $\operatorname{Div}^0(E)$.

Satz 4.45 *Der Divisor einer Funktion ist tatsächlich ein Divisor.*

Beweis Wir müssen zeigen, dass die Linearkombination eines Divisors einer Funktion endlich ist. Dies gilt aber direkt nach Bemerkung 4.26, da eine rationale Funktion auf $E(\bar{K})$ nur endlich viele Nullstellen oder Pole hat und diese endliche Ordnung haben. □

Wir halten zunächst Rechenregeln für Principal Divisors fest.

Satz 4.46 *Seien $f, g \in \bar{K}(E)$ und $c \in \bar{K}$. Dann gilt*

- $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$,
- $\operatorname{div}(\frac{f}{g}) = \operatorname{div}(f) - \operatorname{div}(g)$,
- $\operatorname{div}(cf) = \operatorname{div}(f)$,
- $\operatorname{div}(f^m) = m\operatorname{div}(f)$.

Beweis Der Beweis folgt direkt aus Satz 4.24. Wir erhalten beispielsweise für die erste Behauptung

$$\begin{aligned}
\operatorname{div}(fg) &= \sum_{P \in E(\bar{K})} \operatorname{ord}_P(fg)[P] \\
&= \sum_{P \in E(\bar{K})} (\operatorname{ord}_P(f) + \operatorname{ord}_P(g))[P] \\
&= \sum_{P \in E(\bar{K})} \operatorname{ord}_P(f)[P] + \sum_{P \in E(\bar{K})} \operatorname{ord}_P(g)[P] \\
&= \operatorname{div}(f) + \operatorname{div}(g).
\end{aligned}$$

Die nächsten beiden Behauptungen folgen analog. Die letzte durch wiederholte Anwendung der ersten. □

Satz 4.47 *Sei $E(\bar{K})$ eine elliptische Kurve und $f \in \bar{K}(E)$ eine rationale Funktion ungleich Null. Dann gilt*

a. $\deg(\operatorname{div}(f)) = 0$

b. Gilt $\operatorname{div}(f) = 0$*, so ist f konstant.*

Beweis a. Dies ist genau Satz 4.27.

b. Dies ist genau Satz 4.28. □

Nach einem kleinen Hilfslemma können wir direkt zeigen, dass der Kern der sum Funktion die Divisoren von Funktionen sind.

Satz 4.48 *Seien $P, Q \in E(\bar{K})$. Angenommen es existiert eine Funktion $h \in \bar{K}(E)$ mit*

$$\operatorname{div}(h) = [P] - [Q],$$

dann ist $P = Q$.

Beweis Den Beweis kann man in [Was08, Lemma 1.3] nachlesen. □

Satz 4.49 *Sei $E(\bar{K})$ eine elliptische Kurve. Sei D ein Divisor auf $E(\bar{K})$ mit $\deg(D) = 0$. Dann existiert eine Funktion $f \in \bar{K}(E)$ mit*

$$\operatorname{div}(f) = D$$

genau dann, wenn

$$\operatorname{sum}(D) = O.$$

Beweis Wir folgen dem Beweis in [Was08, Theorem 11.2].

Seien $P_1, P_2, P_3 \in E(\bar{K})$ drei Punkte auf einer Linie $ax + by + c = 0$. Dann hat die rationale Funktion $f(x, y) = ax + by + c$ die Nullstellen P_1, P_2, P_3. Ist $b \neq 0$, so hat f nach Satz 4.27 eine dreifache Polstelle an O. Also gilt

$$\operatorname{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[O].$$

Die Linie durch die Punkte $P_3 = (x_3, y_3)$ und $-P_3$ ist $x - x_3 = 0$. Demnach ist der Divisor dieser Funktion

$$\operatorname{div}(x - x_3) = [P_3] + [-P_3] - 2[O]. \tag{4.3}$$

Damit überlegt man sich, dass

$$\begin{aligned}\operatorname{div}\left(\frac{ax + by + c}{x - x_3}\right) &= \operatorname{div}(ax + by + c) - \operatorname{div}(x - x_3) \\ &= [P_1] + [P_2] - [-P_3] - [O].\end{aligned}$$

Da $P_1 + P_2 = -P_3$ gilt, können wir die Gleichung umschreiben als

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \operatorname{div}\left(\frac{ax + by + c}{x - x_3}\right).$$

Zur Vereinfachung setzen wir $g := \frac{ax+by+c}{x-x_3}$. In anderen Worten können wir die Summe $[P_1] + [P_2]$ durch die Summe von $[P_1 + P_2] + [O] + \operatorname{div}(g)$ ersetzen. Außerdem gilt

$$\operatorname{sum}(\operatorname{div}(g)) = P_1 + P_2 - (P_1 + P_2) - O = O.$$

Gleichung 4.3 hingegen sagt uns, dass wir $[P_1] + [P_2]$ durch $2[O]$ plus den Divisor einer Funktion ersetzen können, sollte $P_1 + P_2 = O$ gelten. Zusammen können wir schließen, dass die Summe aller Terme mit positiven Koeffizienten in D zu $[P]$ plus ein Vielfaches von $[O]$ plus den Divisor

einer Funktion reduziert werden kann. Das Gleiche kann man auch mit allen Punkten mit negativen Koeffizienten machen. Also existieren zwei Punkte P und Q auf $E(\bar{K})$, eine rationale Funktion $g_1 \in \bar{K}(E)$ und eine ganze Zahl n, sodass

$$D = [P] - [Q] + n[O] + \mathrm{div}(g_1).$$

Da g_1 ein Quotient von Produkten von rationalen Funktionen g mit $\mathrm{sum}(\mathrm{div}(g)) = O$ ist, gilt auch für g_1

$$\mathrm{sum}(\mathrm{div}(g)) = O.$$

Da außerdem $\deg(\mathrm{div}(g_1)) = 0$ ist, gilt

$$0 = \deg(D) = 1 - 1 + n + 0 = n.$$

Daher ist

$$D = [P] - [Q] + \mathrm{div}(g_1)$$

und

$$\mathrm{sum}(D) = P - Q + \mathrm{sum}(\mathrm{div}(g_1)) = P - Q.$$

Angenommen $\mathrm{sum}(D) = O$. Dann ist $P - Q = O$, also $P = Q$ und $D = \mathrm{div}(g_1)$.

Andersrum nehmen wir an, dass $D = \mathrm{div}(f)$ für eine Funktion $f \in \bar{K}(E)$. Dann ist

$$[P] - [Q] = \mathrm{div}\left(\frac{f}{g_1}\right).$$

Daraus folgt mit Satz 4.48, dass $P = Q$ und daraus $\mathrm{sum}(D) = O$. □

Satz 4.50 *Die Abbildung*

$$\mathrm{sum} : \mathrm{Div}^0(E)/(\mathrm{Prin}(E)) \to E(\bar{K})$$

ist ein Gruppenisomorphismus.

Beweis Der Beweis ist [Was08, Korollar 11.4] entnommen.

Zunächst ist die Abbildung nach Satz 4.49 wohldefiniert.

Da für alle $P \in E(\bar{K})$ gilt, dass $\mathrm{sum}([P] - [O]) = P$, ist die Abbildung von $\mathrm{Div}^0(E)$ nach $E(\bar{K})$ surjektiv. Satz 4.49 zeigt, dass der Kern genau die Principal Divisors sind. □

Beispiel 4.51 *Wir möchten die Isomorphie aus Satz 4.50 anhand eines Beispiels deutlich machen. Dafür nutzen wir das Beispiel in [BSS04, Kapitel IX.2].*

Dafür betrachten wir die Gruppe $\mathrm{Div}^0(E)/\mathrm{Prin}(E)$. *Wir schreiben für zwei Divisoren* $D, D' \in \mathrm{Div}(E)$ $D \sim D'$, *falls* $D' = D + (f)$ *für eine Funktion* $f \in \bar{K}(E)$ *gilt und nennen sie äquivalent.*

Seien jetzt $P_1, P_2 \in E(\bar{K})$ *zwei Punkte auf einer elliptischen Kurve. Wir nehmen an, die Gleichung für die Gerade durch die beiden Punkte hat die Gleichung* $l(x, y) = 0$. *Diese Gerade schneidet die Kurve an einem dritten Punkt S. Demnach hat l, interpretiert als eine Funktion in* $\bar{K}(E)$ *den*

Divisor $\operatorname{div}(l) = [P_1] + [P_2] + [S] - 3[O]$. *Die vertikale Gerade v durch S schneidet die Kurve nach Definition in S und* $P_3 = P_1 + P_2$, *was bedeutet, dass wir den Divisor* $\operatorname{Div}(v) = [S] + [P_3] - 2[O]$ *erhalten. Wir betrachten*

$$\begin{aligned}\operatorname{div}\left(\frac{l}{v}\right) &= \operatorname{div}(l) - \operatorname{div}(v)\\ &= [P_1] + [P_2] + [S] - 3[O] - ([S] + [P_3] - 2[O])\\ &= [P_1] + [P_2] - [P_3] - [O].\end{aligned}$$

Dies können wir umstellen nach $[P_3] - [O] = [P_1] - [O] + [P_2] - [O] - \operatorname{div}\left(\frac{l}{v}\right)$. *Dies bedeutet aber genau, dass* $[P_3] - [O] \sim [P_1] - [O] + [P_2] - [O]$. *Wir können also die Gruppenoperation elliptischer Kurven durch Divisoren ausdrücken.*

Bemerkung 4.52 *Das vorangegangene Beispiel zeigt auch nochmal die Homomorphieeigenschaft der Abbildung. So hätten wir sie auch nutzen können, um die Gruppeneigenschaften der elliptischen Kurve mithilfe der Divisoren zu zeigen. Insbesondere zeigt das auch die bisher übersprungene Assoziativität der Gruppenoperation. Diese Herangehensweise findet man auch in [DKR13, Kapitel 5.1].*

In Beispiel 4.51 haben wir gesehen, wie man einen Divisor der Form $[P_1] + [P_2] - 2[O]$ äquivalent darstellen kann als $[P_3] - [O]$. Diese Idee wollen wir jetzt fortsetzen für Divisoren mit mehr als zwei Punkten.

Satz 4.53 *Seien* $P_1, \dots, P_n \in E(\bar{K})$ *und* $D = \sum_{i_1}^{n}([P_i] - [O]) \in \operatorname{Div}(E)$. *Dann ist D äquivalent zu einem Divisor der Form* $[P] - [O]$.

Beweis Sei $D \in \operatorname{Div}^0(E)/(\operatorname{Prin}(E))$. Dann ist $\operatorname{sum}(D) = P$ für einen Punkt $P \in E(\bar{K})$. Andererseits ist auch $\operatorname{sum}([P] - [O]) = P$. Nach Satz 4.50 ist also $D \sim [P] - [O]$. □

4.4 Weil-Pairing

In diesem Abschnitt werden wir ein Pairing, wie in Kapitel 2 vorgestellt, auf elliptischen Kurven definieren. Wir folgen dafür [Sil09, Kapitel III.8].

Sei $E(K)$ eine elliptische Kurve und $m \in \mathbb{N}$ eine Zahl, die nicht durch die Charakteristik von K teilbar ist. Dann ist nach Satz 4.3 die Torsionsgruppe

$$E[m] \simeq \mathbb{Z}_m \oplus \mathbb{Z}_m.$$

Sei jetzt $\mu_m := \{x \in \bar{K} | x^m = 1\}$ die Gruppe der Einheitswurzeln in $\bar{K}$. Die Gleichung $x^m = 1$ hat m verschiedene Lösungen in $\bar{K}$, da $\operatorname{char}(K) \nmid m$. Also ist μ_m eine Gruppe der Ordnung m. Sie ist zyklisch, da sie eine endliche Untergruppe der multiplikativen Gruppe eines Körpers ist.

Sei jetzt $T \in E[m]$. Dann existiert nach Satz 4.49 eine Funktion $f \in \bar{K}(E)$ mit

$$\operatorname{div}(f) = m[T] - m[O]. \tag{4.4}$$

Dies gilt, da die Bedingung $T \in E[m]$ genau bedeutet, dass $mT = O$. Da die Multiplikation mit m surjektiv ist, können wir ein $T' \in E(K)$ mit $mT' = T$ wählen. Dieser Punkt liegt in $E[m^2]$, da $O = mT = m^2T'$. Wir möchten zeigen, dass eine Funktion $g \in \bar{K}(E)$ existiert mit

$$\text{(4.5)}\quad \operatorname{div}(g) = \sum_{R \in E[m]} ([T' + R] - [R]).$$

Dafür müssen wir nach Satz 4.49 zeigen, dass die Summe der Punkte im Divisor O ergibt. Dafür halten wir zunächst fest, dass aus der Annahme $E[m] \simeq \mathbb{Z}_m \times \mathbb{Z}_m$ folgt, dass $E[m]$ aus m^2 Punkten besteht. Dann gilt

$$\begin{aligned}\operatorname{sum}(\operatorname{div}(g)) &= \sum_{R \in E[m]} T' + R - R \\ &= \sum_{R \in E[m]} T' \\ &= m^2 T' \\ &= O.\end{aligned}$$

Wir stellen fest, dass g nicht von der Wahl von T' abhängt. Seien dafür T'_1 und T'_2 zwei solche Wahlen. Dann folgt

$$\begin{aligned}& m(T'_1 - T'_2) = T - T = O \\ \Rightarrow\ & T'_1 - T'_2 \in E[m] \\ \Rightarrow\ & \exists R \in E[m] : T'_1 = T'_2 + R.\end{aligned}$$

Nachdem die Summe in Gleichung 4.5 über alle $R \in E[m]$ läuft, ist g von der Wahl von T' unabhängig. Wir hätten also auch schreiben können

$$\text{(4.6)}\quad \operatorname{div}(g) = \sum_{mT'' = T} [T''] - \sum_{mR = O} [R].$$

Sei nun $f \circ m$ die Funktion, die einen Punkt nimmt, ihn mit m multipliziert und dann f anwendet. Die Punkte $P = T' + R$ mit $R \in E[m]$ sind genau die Punkte P mit $mP = T$ und die Punkte $R \in E[m]$ genau die mit $mR = O$. Mithilfe davon und Gleichung 4.4 folgt

$$\operatorname{div}(f \circ m) = m\left(\sum_{R \in E[m]} [T' + R]\right) - m\left(\sum_{R \in E[m]} [R]\right) = \operatorname{div}(g^m).$$

Letztere Gleichheit folgt aus Satz 4.46. Dies bedeutet auch, dass $\operatorname{div}\left(\frac{f \circ m}{g^m}\right) = 0$ ist. Also ist nach Satz 4.28 $\frac{f \circ m}{g^m}$ konstant. Anders ausgedrückt heißt das, dass $f \circ m$ ein konstantes Vielfaches von g^m ist. Multiplizieren wir f also mit einer passenden Konstante, können wir annehmen, dass

$$f \circ m = g^m.$$

Sei jetzt $S \in E[m]$ und $X \in E(\bar{K})$ so gewählt, dass $g(X) \neq 0$. Dann ist

$$g(X + S)^m = f(m(X + S)) = f(mX) = g(X)^m.$$

Also ist $\frac{g(X+S)}{g(X)} \in \mu_m$. Tatsächlich ist $\frac{g(X+S)}{g(X)}$ unabhängig von X. Den Beweis dafür reißen wir nur an. In der Zariski Topologie ist die Abbildung $\frac{g(P+S)}{g(P)}$ stetig auf der zusammenhängenden Menge $E(K)$. Sie muss dann als Abbildung auf die endliche diskrete Menge μ_m konstant sein.

Definition 4.54 *Sei $m \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid m$. Sei $T \in E[m]$ und $f \in K(E)$ eine Funktion mit Divisor $\mathrm{div}(f) = m[T] - m[O]$. Wir setzen $g \in K(E)$ als die Funktion mit $f \circ m = g^m$. Sei jetzt $S \in E[m]$ und $X \in E(\bar{K})$ beliebig. Damit definieren wir das Weil-Pairing als*

$$\begin{aligned} e_m : E[m] \times E[m] &\to \mu_m \\ (S,T) &\mapsto \frac{g(X+S)}{g(X)}. \end{aligned}$$

Nach einem kleinen Hilfslemma halten wir einige Eigenschaften des Weil-Pairings fest.

Satz 4.55 *Sei $E(K)$ eine elliptische Kurve. Sei $f(x,y)$ eine Funktion von $E(K)$ nach $\bar{K} \cup \{O\}$ und $n \geq 1$ eine Zahl nicht teilbar durch die Charakteristik von K. Angenommen es gilt $f(P+T) = f(P)$ für alle $P \in E(\bar{K})$ und $T \in E[n]$. Dann existiert eine Funktion h auf $E(K)$, sodass $f(P) = h(nP)$ für alle $P \in E(\bar{K})$.*

Beweis Den Beweis findet man in [Was08, Proposition 9.34]. □

Satz 4.56 *Das Weil-Pairing e_m hat folgende Eigenschaften:*

a. Es ist bilinear.

$$\begin{aligned} e_m(S_1 + S_2, T) &= e_m(S_1, T) e_m(S_2, T), \text{ für alle } S_1, S_2, T \in E[m] \\ e_m(S, T_1 + T_2) &= e_m(S, T_1) e_m(S, T_2), \text{ für alle } S, T_1, T_2 \in E[m] \end{aligned}$$

b. Es ist alternierend.

$$e_m(T,T) = 1, \text{ für alle } T \in E[m]$$

Insbesondere gilt also auch $e_m(T,S)^{-1} = e_m(S,T)$ für alle $S, T \in E[m]$.

c. Es ist nicht entartet. Gilt $e_m(S,T) = 1$ für alle $S \in E[m]$, dann ist $T = O$. Ebenso falls $e_m(S,T) = 1$ für alle $T \in E[m]$, dann ist $S = O$.

Beweis Für diesen Beweis folgen wir [Sil09, Proposition III.8.1]

a. Für die Linearität im ersten Faktor nutzen wir, dass das Weil-Pairing unabhängig von der Wahl von X ist.

$$\begin{aligned} e_m(S_1 + S_2, T) &= \frac{g(X + S_1 + s_2)}{g(X)} \\ &= \frac{g(X * S_1 + S_2)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} \\ &= e_m(S_1, T) e_m(S_2, T) \end{aligned}$$

Für die Linearität im zweiten Faktor seien $f_1, f_2, f_3, g_1, g_2, g_3$ die entsprechenden Funktionen aus der Herleitung für die Punkte T_1, T_2 und $T_3 = T_1 + T_2$. Wähle eine Funktion $h \in \bar{K}(E)$ mit Divisor

$$\mathrm{div}(h) = [T_1 + T_2] - [T_1] - [T_2] + [O].$$

Dies ist möglich, da $\text{sum}(\text{div}(h)) = O$. Damit erhält man

$$\begin{aligned}\text{div}\left(\frac{f_3}{f_1 f_2}\right) &= \text{div}(f_3) - \text{div} f_1 - \text{div} f_2 \\ &= m[T_3] - m[O] - m[T_1] + m[O] - m[T_2] + m[O] \\ &= m([T_3] - [T_1] - [T_2] + [O]) \\ &= m\text{div}(h) \\ &= \text{div}(h^m)\end{aligned}$$

Demnach existiert eine Konstante $c \in \bar{K}^*$ mit

$$f_3 = c f_1 f_2 h^m.$$

Wir verknüpfen diese Abbildung mit der Multiplikation mit m Abbildung, nutzen die Eigenschaft, dass $f_i \circ m = g^m$ und ziehen die m-te Wurzel, um

$$g_3 = c' g_1 g_2 (h \circ m)$$

für ein $c' \in \bar{K}^*$ zu erhalten. Mithilfe der Eigenschaft $mS = O$ können wir dann die gewünschte Eigenschaft berechnen:

$$\begin{aligned}e_m(S, T_1 + T_2) &= \frac{g_3(X+S)}{g_3(X)} \\ &= \frac{g_1(X+S) g_2(X+S) h(mX + mS)}{g_1(X))}\end{aligned}$$

b. Wir definieren zunächst die Abbildung τ_P als die Addition von $P \in E(\bar{K})$:

$$\begin{aligned}\tau_P : E(\bar{K}) &\to E(\bar{K}) \\ T &\mapsto T + P\end{aligned}$$

Der Divisor der Funktion $f \circ \tau_{jP}$ ist $m[T - jT] - m[-jT]$. Daraus folgern wir

$$\begin{aligned}\text{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{iT}\right) &= m \sum_{i=0}^{m-1} [(1-i)T] - [-iT] \\ &= m([T] - [(-m+1)T]) \\ &= m([T] - [T]) \\ &= 0\end{aligned}$$

Dabei haben wir genutzt, dass $T \in E[m]$. Daraus folgt mit Satz 4.28, dass

$$\prod_{i=0}^{m-1} f \circ \tau_{iT}$$

konstant ist. Wählen wir jetzt ein $T' \in E(K)$ mit $T = mT'$, können wir auch zeigen, dass die Funktion $\prod_{i=0}^{m-1} g \circ \tau_{iT'}$ konstant ist. Dazu berechnen wir

$$\begin{aligned}\left(\prod_{i=0}^{m-1} g \circ \tau_{iT'}\right)^m (P) &= \prod_{i=0}^{m-1} f \circ m \circ \tau_{iT'}(P) \\ &= \prod_{i=0}^{m-1} f(m(P + iT')) \\ &= \prod_{i=0}^{m-1} f(mP + iT) \\ &= \prod_{i=0}^{m-1} f \circ \tau_{iT} \circ m(P)\end{aligned}$$

für alle $P \in E[m]$. Da die Multiplikation mit m surjektiv ist und $\prod_{i=0}^{m-1} f \circ \tau_{iT}$ konstant ist, ist es auch $\prod_{i=0}^{m-1} g \circ \tau_{iT'}$. Insbesondere nimmt die Funktion die gleichen Werte an X und $X + T'$ an:

$$\prod_{i=0}^{m-1} g(X + iT') = \prod_{i=0}^{m-1} g(X + (i+1)T')$$

Kürzen wir gleiche Terme auf der linken und rechten Seite, so erhalten wir

$$g(X) = g(X + mT') = g(X + T).$$

Zuletzt können wir damit die Behauptung zeigen:

$$e_m(T, T) = \frac{g(X + T)}{g(X)} = 1$$

Für die zweite Behauptung berechnen wir

$$\begin{aligned}1 &= e_m(S + T, S + T) \\ &= e_m(S, S) e_m(S, T) e_m(T, S) e_m(T, T) \\ &= e_m(S, T) e_m(T, S).\end{aligned}$$

c. Gilt $e_m(S, T) = 1$ für alle $S \in E[m]$, so ist $g(X + S) = g(X)$. Nach Satz 4.55 existiert dann eine Funktion $h \in \bar{K}(E)$ mit $g = h \circ [m]$. Dann gilt auch

$$(h \circ m)^m = g^m = f \circ m,$$

woraus wir $f = h^m$ schließen. Daher gilt

$$m\mathrm{div}(h) = \mathrm{div}(f) = m[T] - m[O],$$

also

$$\mathrm{div}(h) = [T] - [O].$$

Mit Satz 4.49 folgt $\mathrm{sum}(\mathrm{div}(h)) = T - O = O$, also $T = O$. Sei nun $e_m(S, T) = 1$ für alle $T \in E[m]$. Es ist auch $1 = e_m(S, T)^{-1} = e_m(T, S)$. Mit dem eben Bewiesenen ist also $S = O$. □

4.5 Tate-Lichtenbaum-Pairing

Wir möchten uns noch ein zweites Pairing anschauen, das Tate-Lichtenbaum Pairing. Für die Herleitung dessen folgen wir [Was08, Kapitel 11.3].

Sei $E(F_q)$ eine elliptische Kurve. Sei $n \in \mathbb{N}$, sodass $n|q-1$ und seien $nE(F_q) := \{nP | P \in E(F_q)\}$ und $(F_q^*)^n := \{a^n | a \in F_q^*\}$. Damit wollen wir ein Pairing

$$\langle \cdot, \cdot \rangle_n : E(F_q)[n] \times E(F_q)/nE(F_q) \to F_q^*/(F_q^*)^n$$

herleiten.

Wir werden dabei folgendermaßen vorgehen:

a. Für einen Punkt $P \in E(F_q)[n]$ definieren wir einen Divisor D_P mit bestimmten gewünschten Eigenschaften.

b. Der Divisor nD_P wird der Divisor einer Funktion sein. Wir wählen eine solche Funktion f mit bestimmten Eigenschaften.

c. Für eine Äquivalenzklasse $Q + nE(F_q) \in E(F_q)/nE(F_q)$ wählen wir einen Divisor D_Q, an welchem wir f auswerten können.

Sei also $P \in E(F_q)[n]$ und D_P ein Divisor mit $\deg(D_P) = 0$ und $\mathrm{sum}(D_P) = P$. Das heißt, dass auch $D_P - [P] + [O]$ Grad 0 hat und sich zu O summiert, womit eine Funktion $s \in K(E)$ mit $\mathrm{div}(s) = D_P - [P] + [O]$ existiert. Umgestellt bedeutet das nichts anderes als $D_P \sim [P] - [O]$ mit der Äquivalenzrelation aus Beispiel 4.51.

Definition 4.57 *Sei K ein Körper, $E(K)$ eine elliptische Kurve $D = \sum_{i=1}^{d} c_i[P_i]$ ein Divisor und $f : E(K) \to E(K)$ eine Funktion. Dann definieren wir*

$$f(D) := \sum_{i=1}^{d} c_i[f(P_i)]$$

Wir möchten zusätzlich annehmen, dass $\phi_q(D_P) = D_P$, wobei ϕ_q den Frobenius Endomorphismus bezeichnet. Dafür halten wir zunächst fest, dass ein solcher Divisor überhaupt existiert. Die Bedingung ist nämlich leicht erfüllt, wenn alle Punkte von D_P in $E(F_q)$ liegen. Dies folgt direkt aus Satz 4.39. Beispielsweise ist das für $D_P = [P] - [O]$ erfüllt. Der nächste Satz zeigt, dass sobald wir einen solchen Divisor gefunden haben, beliebig viele erzeugt werden können.

Satz 4.58 *Sei $E(F_q)$ eine elliptische Kurve und D_1 ein Divisor von Grad 0 mit $\phi_q(D_1) = D_1$. Sei außerdem $S \subset E(\bar{F}_q)$ eine endliche Menge an Punkten. Dann existiert ein Divisor D mit $\phi_q(D) = D$, $D \sim D_1$ und D enthält keine Punkte aus S.*

Beweis Für diesen Beweis folgen wir [Was08, Lemma 11.9].

Sei $D_1 = \sum_{j=1}^{d} c_j[P_j]$. Da Divisoren über den algebraischen Abschluss definiert sind, liegen die P_j in $E(\bar{F}_q)$. Dadurch liegen alle Punkte P_j in einer endlichen Gruppe $E(F_{g^k})$ und es gilt für $M = \mathrm{kgV}\{\mathrm{ord}(P_j) | j = 1, \ldots, d\}$, dass $MP_j = O$ für alle $j = 1, \ldots, d$. Sei jetzt $m \equiv 1 \mod M$. Für dieses m gilt $mP_j = P_j$ für alle $j = 1, \ldots, d$. Sei $T = (t_1, t_2) \in E(F_{q^m})$. Für diesen Punkt gilt

$\phi_q^m(T) = (t_1^{q^m}, t_2^{q^m}) = (t_1, t_2) = T$, ϕ_q permutiert also die Menge $\{T, \phi_q(T), \ldots, \phi_q^{m-1}(T)\}$. Wir definieren den Divisor D als

$$D = \sum_{i=0}^{m-1} \sum_{j=1}^{d} c_j \left([P_j + \phi_q^i(T)] - [\phi_q^i(T)] \right).$$

Für diesen Divisor gilt $\deg(D) = 0$. Da $\phi_q(D_1) = D_1$ gilt, haben wir auch für jedes $j = 1, \ldots, d$, dass $\phi_q(P_j) = P_{j'}$ und $c_j = c_{j'}$ für ein j'. Dadurch werden die Summanden in D durch ϕ_q permutiert, also erhalten wir $\phi_q(D) = D$. Für ein festgehaltenes j ergibt sich

$$\operatorname{sum}\left(c_j \sum_{i=0}^{m-1} \left([P_j + \phi_q^i(T)] - [\phi_q^i(T)] \right) \right) = c_j m P_j = c_j P_j.$$

Demnach gilt auch

$$\begin{aligned} \operatorname{sum}(D_1 - D) &= \sum_{j=1}^{d} c_j P_j - \sum_{j=1}^{d} c_j P_j \\ &= O \end{aligned}$$

und $\deg(D_1 - D) = \deg(D_1) - \deg(D) = 0$, weswegen $D_1 - D$ ein principal Divisor ist, also $D \sim D_1$.

Sollte D jetzt einen Punkt aus der Menge S enthalten, so liegt $\phi_q^i(T) \in S$ oder $P_j + \phi_q^i(T) \in S$ für bestimmte i, j. Das bedeutet, dass T in einer der Mengen liegt, wenn man zu $\phi_q^{-i}(S)$ entweder O oder $\phi_q^{-i}(P_j)$ addiert. Dann gibt es maximal $m(d+1)\#S$ Punkte in der Vereinigung dieser Mengen. Nach Satz 4.41 enthält $E(F_{q^m})$ mindestens $q^m + 1 - 2q^{\frac{m}{2}}$ Punkte. Da damit also $\#E(F_{q^m}) - m(d+1)\#S \to \infty$ für $m \to \infty$, können wir dadurch, dass wir m variieren, T so wählen, dass es in keiner dieser Mengen liegt und somit einen Divisor erhalten, der keinen Punkt aus S enthält. □

Wir nehmen jetzt an, wir hätten ein D_P gewählt. Dann existiert eine Funktion $f \in \bar{F}_q(E)$, sodass

$$\operatorname{div}(f) = nD_P.$$

Wir wollen aber noch mehr von f fordern. Dafür bezeichnen wir mit f^{ϕ_q} das Ergebnis nachdem wir ϕ_q auf die Koeffizienten von f anwenden. Dann gilt auch $\phi_q(f(X)) = f^{\phi_q}(\phi_q(X))$ für alle $X \in E(\bar{F}_q)$.

Satz 4.59 *Es gilt $\phi_q(f(X)) = f^{\phi_q}(\phi_q(X))$ für alle $X \in E[\bar{F}_q]$.*

Beweis Wir zeigen die Behauptung der Reihe nach für ein $f \in \bar{F}_q[x]$, dann für $f \in \bar{F}_q[E]$ und zuletzt $f \in \bar{F}_q(E)$.

Sei also $f(x) = \sum_{i=1}^{n} c_i x^i \in \bar{F}_q[x]$. Dann gilt

$$\begin{aligned} \phi_q(f(x)) &= \left(\sum_{i=1}^{n} c_i x^i \right)^q \\ &= \sum_{i=1}^{n} c_i^q (x^q)^i \\ &= f_{\phi_q}(\phi_q(x)). \end{aligned}$$

Für die zweite Gleichheit nutzen wir, dass wir uns in $\bar{F}_q$ befinden. Sei nun $f(x,y) = v(x) + yw(x) \in \bar{F}_q[E]$ mit $v, w \in \bar{F}_q[x]$ in kanonischer Form und $P = (x_P, y_P) \in E(\bar{F}_q)$. Dann gilt

$$\begin{aligned}\phi_q(f(P)) &= (v(x_P) + y_P w(x_P))^q \\ &= v(x_P)^q + y_P^q w(x_P)^q \\ &= v_{\phi_q}(x_P^q) y_P^q w_{\phi_q}(x_P^q) \\ &= f_{\phi_q}(\phi_q(P)).\end{aligned}$$

Sei jetzt $r(x,y) = \frac{f(x,y)}{g(x,y)} = \frac{v(x)}{N_g(x)} + y\frac{w(x)}{N_g(x)} \in \bar{F}_q(E)$ mit $v, w \in \bar{F}_q(E)$ in kanonischer Form und $P = (x_P, y_P) \in E(\bar{F}_q)$. Dann gilt

$$\begin{aligned}\phi_q(r(P)) &= \phi_q\left(\frac{f(x_P, y_P)}{g(x_P, y_P)}\right) \\ &= \left(\frac{v(x_P)}{N_g(x_P)} + y_P \frac{w(x_P)}{N_g(x_P)}\right)^q \\ &= \frac{v(x_P)^q}{N_g(x_P)^q} + y_P^q \frac{w(x_P)^q}{N_g(x_P)^q} \\ &= \frac{v_{\phi_q}(x_P^q)}{N_{g_{\phi_q}}(x_P^q)} + y_P^q \frac{w_{\phi_q}(x_P^q)}{N_{g_{\phi_q}}(x_P^q)} \\ &= r_{\phi_q}(\phi_q(P)).\end{aligned}$$

□

Satz 4.60 *Sei $D \in \mathrm{Prin}(E)$ mit $\phi_q(D) = D$. Dann existiert eine Funktion f, sodass $\mathrm{div}(f) = D$ und $f^{\phi_q} = f$. Das bedeutet, dass f über F_q definiert ist, also die Koeffizienten von f in F_q liegen.*

Beweis Für diesen Beweis folgen wir [Was08, Lemma 11.10].

Wir beginnen mit einem beliebigen f_1, sodass $\mathrm{div}(f_1) = D$. Dann gilt

$$\mathrm{div}(f_1^{\phi_q}) = \phi_q(D) = D = \mathrm{div}(f_1).$$

Das zeigt, dass $\frac{f_1^{\phi_q}}{f_1} = c \in \bar{F}_q^*$ konstant ist. Wir wählen also ein $d \in \bar{F}_q^*$, sodass $c = d^{q-1} = \frac{\phi_q(d)}{d}$. Dann gilt

$$\frac{\phi_q(d)}{d} = c = \frac{f_1^{\phi_q}}{f_1}$$

und damit auch

$$\left(\frac{1}{d} f_1\right)^{\phi_q} = \left(\left(\frac{1}{\phi_q(d)}\right)\right) f_1^{\phi_q} = \frac{1}{d} f_1.$$

Da d konstant ist, hat die Funktion $f = \frac{1}{d} f_1$ den gleichen Divisor wie f_1. □

Nach einer letzten kurzen Definition einer Notation können wir jetzt das Tate-Lichtenbaum Pairing definieren.

Definition 4.61 *Sei $f \in K(E)$ eine rationale Funktion, deren Divisor keine Punkte mit einem Divisor $D = \sum_i a_i [Q_i]$ gemein hat. Dann definieren wir*

$$f(D) := \prod_i f(Q_i)^{a_i}.$$

Sei nun $Q + nE(F_q) \in E(F_q)/nE(F_q)$. Zu Vereinfachung schreiben wir dafür auch nur Q. Sei dann $D_Q = \sum_i a_i [Q_i]$ ein Divisor mit Grad 0 und $\text{sum}(D_Q) = Q$, sodass D_P und D_Q keine gemeinsamen Punkte haben. Wir nehmen an, dass $\phi_q(D_Q) = D_Q$. f soll nun die Bedingung $f^{\phi_q} = f$ erfüllen. Dann definieren wir das Tate-Lichtenbaum Pairing als

$$\langle P, Q \rangle_n := f(D_Q) \mod (F_q^*)^n.$$

Dabei gilt es zu beachten, dass die Funktion f nur bis auf ein konstantes Vielfaches definiert ist. Da aber $0 = \deg(D_Q) = \sum_i a_i$ ist, gilt, falls $f = cf'$ für eine Konstante c und Funktion f' mit gleichem Divisor,

$$\begin{aligned}
f(D_Q) &= \prod_i f(Q_i)^{a_i} \\
&= \prod_i (cf'(Q_i))^{a_i} \\
&= \left(\prod_i c^{a_i} \right) \left(\prod_i f'(Q_i)^{a_i} \right) \\
&= c^{\sum_i a_i} \prod_i f'(Q_i)^{a_i} \\
&= \prod_i f'(Q_i)^{a_i} \\
&= f'(D_Q).
\end{aligned}$$

Wir fassen die obige Herleitung noch einmal zusammen.

Definition 4.62 *Sei $E(F_q)$ eine elliptische Kurve und $n \in \mathbb{N}$, sodass $n|q-1$. Sei dann $P \in E(F_q)[n]$ und D_P ein Divisor mit $D_P \sim [P] - [O]$ und $\phi_q(D_P) = D_P$. Es existiert dann eine Funktion $f \in K(E)$ mit $\text{div}(f) = nD_P$. Wir können diese so wählen, dass $f^{\phi_q} = f$. Sei zuletzt $Q + nE(F_q) \in E(F_q)/nE(F_q)$, vereinfachend einfach als Q geschrieben, und D_Q ein Divisor von Grad 0 und sum$(D_Q) = Q$, welcher keine Punkte mit D_P gemeinsam hat. Dann definieren wir das Tate-Lichtenbaum Pairing als*

$$\begin{aligned}
\langle \cdot, \cdot \rangle_n : E(F_q)[n] \times E(F_q)/nE(F_q) &\to F_q^*/(F_q^*)^n \\
(P, Q) &\mapsto f(D_Q) \mod (F_q^*)^n.
\end{aligned}$$

Wir benötigen noch eine wichtige Aussage, bevor wir die Eigenschaften des Pairings beweisen können.

Satz 4.63 *Seien $f, h \in K(E)$ zwei Funktionen auf E. Angenommen* $\text{div}(f)$ *und* $\text{div}(h)$ *haben keine gemeinsamen Punkte, dann gilt*

$$f(\text{div}(h)) = h(\text{div}(f)).$$

Diesen Satz nennt man auch die Weil Reziprozität.

Beweis Einen Beweis findet man in [BSS04, Kapitel IX, Appendix]. □

Satz 4.64 *Das Tate-Lichtenbaum-Pairing hat folgende Eigenschaften:*

a. Es ist unabhängig modulo n-ter Potenzen von der Wahl des Repräsentanten Q in $E(F_q)/nE(F_q)$.

b. Es ist unabhängig modulo n-ter Potenzen von der Wahl von D_P und D_Q.

c. Es ist linear in beiden Unbekannten.

d. Es ist nicht entartet.

Beweis Für den Beweis von Teil a folgen wir [Gal12, Lemma 26.3.2], für die restlichen Teile [Was08, Kapitel 11.3].

a. Seien $D_1 \sim [Q_1] - [O]$ und $D_2 \sim [Q_2] - [O]$ Divisoren, wobei $Q_1, Q_2 \in E(F_q)$ liegen, sodass $Q_1 \neq Q_2$ und $Q_1 - Q_2 \in nE(F_q)$. Anders geschrieben bedeutet das, dass $D_1 = [Q_1] - [O] + \operatorname{div}(h_1)$ und $D_2 = [Q_2] - [O] + \operatorname{div}(h_2)$ für $h_1, h_2 \in F_q(E)$. Wir können auch $Q_1 - Q_2 = nR$ für ein $R \in E(F_q)$ schreiben. Mit Teil b, welchen wir gleich beweisen werden, können wir annehmen, dass $R \neq O$ ist. Betrachtet als Divisoren können wir auf $[Q_1] - [Q_2] = n([R+S] - [S]) + \operatorname{div}(h_0)$ für ein $h_0 \in F_q(E)$ und ein $S \in E(F_q)$ mit $S \notin \{O, -R, P, P-R\}$ schließen. Zusammen erhalten wir

$$\begin{aligned}
f(D_2) &= f([Q_2] - [O] + \operatorname{div}(h_2)) \\
&= f([Q_1] - n([R+S] - [S]) - \operatorname{div}(h_0) + \operatorname{div}(h_2)) \\
&= f(D_1 + [O] - \operatorname{div}(h_1) - n([R+S] - [S]) - \operatorname{div}(h_1) + \operatorname{div}(h_2)) \\
&= f(D_1) f(n([R+S] - [S])) f\left(\operatorname{div}\left(\frac{h_2}{h_0 h_1}\right)\right) \\
&= f(D_1) f([R+S] - [S])^n \frac{h_2}{h_0 h_1}(\operatorname{div}(f)) \\
&= f(D_1) f([R+S] - [S])^n \frac{h_2}{h_0 h_1}(nD_P) \\
&= f(D_1) f([R+S] - [S])^n \frac{h_2}{h_0 h_1}(D_P)^n.
\end{aligned}$$

b. Seien D'_P und D'_Q zwei Divisoren mit Grad 0, die sich zu P und Q addieren. Außerdem soll $\phi_q(D'_Q) = D'_Q$ und $\phi_q(D'_P) = D'_P$ gelten. Dann haben wir für zwei Funktionen $g, h \in F_q(E)$

$$D'_P = D_P + \operatorname{div}(g),\ D'_Q = D_Q + \operatorname{div}(h).$$

Nach Satz 4.60 sind diese Funktionen über F_q definiert. Außerdem gilt für eine Funktion $f' \in F_q(E)$, welche ebenfalls über F_q definiert ist, $\operatorname{div}(f') = nD'_P$.

Wir nehmen zunächst an, dass sowohl D'_Q keine Punkte mit D_P und D'_P gemeinsam hat, als auch D'_P mit D_Q. Dann gilt

$$\begin{aligned}
\operatorname{div}(f') &= nD'_P \\
&= n(D_P + \operatorname{div}(g)) \\
&= \operatorname{div}(f) + \operatorname{div}(g^n) \\
&= \operatorname{div}(fg^n).
\end{aligned}$$

Daraus folgern wir $f' = cfg^n$ für eine Konstante c. Mit f' und D'_Q können wir jetzt ein neues Pairing definieren, welches wir mit $\langle \cdot, \cdot \rangle'$ bezeichnen. Damit gilt

$$\begin{aligned}\langle P, Q \rangle &= f'(D'_Q) \\ &= f(D'_Q)g(D'_Q)^n \\ &= f(D_Q + \operatorname{div}(h))g(D'_Q)^n \\ &= f(D_Q)f(\operatorname{div}(h))g(D'_Q)^n \\ &= f(D_Q)h(\operatorname{div}(f))g(D'_Q)^n \\ &= f(D_Q)h(D_P)^n g(D'_Q)^n.\end{aligned}$$

Von der vierten auf die fünfte Zeile haben wir Satz 4.63 genutzt. Da $\phi_q(h(D_P)) = h(\phi_q(D_P)) = h(D_P)$ und analog auch für $g(D'_Q)$, gilt $h(D_P), g(D'_Q) \in F_q^*$. Das ergibt

$$\langle P, Q \rangle'_n \equiv \langle P, Q \rangle_n \mod (F_q^*)^n.$$

Für den allgemeinen Fall, in dem D_P, D'_P, D_Q, D'_Q Punkte gemeinsam haben können, können wir nach Satz 4.58 Divisoren D''_P und D''_Q wählen, sodass diese von allen anderen disjunkt sind. Dann gilt

$$\langle P, Q \rangle'_n \equiv \langle P, Q \rangle''_n \equiv \langle P, Q \rangle_n \mod (F_q^*)^n.$$

c. Seien $Q_1, Q_2 \in E(F_q)$ und D_{Q_1}, D_{Q_2} die dazugehörigen Divisoren. Dann gilt nach Beispiel 4.51

$$D_{Q_1} + D_{Q_2} \sim [Q_1] - [O] + [Q_2] - [O] \sim [Q_1 + Q_2] - [O].$$

Daraus folgt schon

$$\begin{aligned}\langle P, Q_1 + Q_2 \rangle_n &= f(D_{Q_1} + D_{Q_2}) \\ &= f(D_{Q_1})f(D_{Q_2}) \\ &= \langle P, Q_1 \rangle_n \langle P, Q_2 \rangle_n.\end{aligned}$$

Seien jetzt $P_1, P_2 \in E(F_q)[n]$, D_{P_1}, D_{P_2} die dazugehörigen Divisoren und f_1, f_2 die entsprechenden Funktionen. Dann gilt wie zuvor

$$D_{P_1} + D_{P_2} \sim [P_1] - [O] + [P_2] + [O] \sim [P_1 + P_2] - [O].$$

Demnach können wir $D_{P_1+P_2} = D_{P_1} + D_{P_2}$ setzen und erhalten damit

$$\begin{aligned}\operatorname{div}(f_1 f_2) &= \operatorname{div}(f_1) + \operatorname{div}(f_2) \\ &= nD_{P_1} + nD_{P_2} \\ &= nD_{P_1+P_2}.\end{aligned}$$

Daraus folgt, nachdem $f_1 f_2$ ein wohldefiniertes Pairing liefert:

$$\langle P_1 + P_2, Q \rangle_n = f_1(D_Q)f_2(D_Q) = \langle P_1, Q \rangle_n \langle P_2, Q \rangle_n.$$

d. Siehe dafür [Was08, Kapitel 11.7]. □

Bemerkung 4.65 *Es gibt noch eine äquivalente Definition des Tate-Lichtenbaum Pairings, welche das Weil-Pairing nutzt. Sei dafür $E(F_q)$ eine elliptische Kurve und $n \in \mathbb{N}$ mit $n|q-1$. Sei $P \in E(F_q)[n]$ und $Q \in E(F_q)$. Wähle $R \in E(\bar{F}_q)$ mit $nR = Q$. Sei e_n das Weil-Pairing und ϕ_q der Frobenius Endomorphismus. Dann ist das Tate-Lichtenbaum Pairing durch*

$$\langle P, Q \rangle_n = e_n(P, R - \phi_q(R))^{\frac{1}{n}}$$

gegeben. Die beiden Definitionen des Tate-Lichtenbaum-Pairings sind äquivalent, für einen Beweis siehe [Was08, Kapitel 11.6.2].

5 Berechnung der Pairings

Im letzten Kapitel haben wir zwei verschiedene Pairings auf elliptischen Kurven hergeleitet. Was jedoch auffällt, ist, dass wir diese nur in Abhängigkeit ihrer Divisoren definiert haben und eine konkrete Berechnungsvorschrift fehlt. Dieser Fragestellung wollen wir uns in diesem Kapitel widmen.

5.1 Weil-Pairing

5.1.1 Alternative Formulierung

Für Millers Algorithmus, welcher im nächsten Abschnitt beschrieben wird, benötigen wir das Weil-Pairing in einer anderen Form. Diese wollen wir in diesem Abschnitt definieren und die Äquivalenz zum Weil-Pairing aus Definition 4.54 zeigen. Dafür folgen wir [Was08, Abschnitt 11.6.1].

Satz 5.1 *Seien $S, T \in E[n]$ und D_S, D_T Divisoren mit Grad 0, sodass*

$$\operatorname{sum}(D_S) = S,\ \operatorname{sum}(D_T) = T$$

und D_S und D_T keine gemeinsamen Punkte haben. Seien $f_S, f_T \in K(E)$ Funktionen, sodass

$$\operatorname{div}(f_S) = nD_S,\ \operatorname{div}(f_T) = nD_T.$$

Dann ist das Weil Pairing durch

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)}$$

gegeben.

Beweis Seien $V, W \in E[n^2]$ und $f_{nV}, g_{nV} \in E(K)$ die Funktionen aus Definition 4.54 mit

$$\operatorname{div}(f_{nV}) = n[nV] - n[O] \text{ und } g_{nV}^n = f_{nV} \circ n.$$

Wir definieren zwei neue Funktionen

$$c(nV, nW) := \frac{f_{nV+nW}(X)}{f_{nV}(X) f_{nW}(X - nV)} \text{ und } d(V,W) := \frac{g_{nV+nW}(X)}{g_{nV}(X) g_{nW}(X - V)}.$$

Für diese müssen wir rechtfertigen, dass diese auf der rechten Seite von X abhängen, auf der linken jedoch nicht. Dafür nutzen wir Satz 4.28 und zeigen, dass der Divisor der Funktionen, als Funktion in X betrachtet, 0 ist, woraus folgt, dass sie konstant sind. Wir beginnen mit c:

$$\begin{aligned}\operatorname{div}(c(nV,nW)) &= \operatorname{div}(f_{nV+nW}(X)) - (\operatorname{div}(f_{nV}(X)) + \operatorname{div}(f_{nW}(X-nV)))\\ &= n[nV+nW] - n[O] - (n[nV] - n[O] + n[nW+nV] - n[nV])\\ &= 0.\end{aligned}$$

Für d nutzen wir Gleichung 4.6:

$$\begin{aligned}\operatorname{div}(d(V,W)) &= \operatorname{div}(g_{nV+nW}(X)) - (\operatorname{div}(g_{nV}(X)) + \operatorname{div}(g_{nW}(X-V)))\\ &= \sum_{nT''=nV+nW}[T''] - \sum_{nR=0}[R]\\ &\quad - \left(\sum_{nT''=nV}[T''] - \sum_{nR=0}[R] + \sum_{nT''=nW}[T''+V] - \sum_{nR=0}[R+V]\right)\\ &= \sum_{nT''=nV+nW}[T''] - \sum_{nT''=nW}[T''+V] + \sum_{nR=0}[R+V] - \sum_{nT''=nV}[T'']\\ &= \sum_{nT''=nV+nW}[T''] - \sum_{nT''=nV+nW}[T''] + \sum_{nR=nV}[R] - \sum_{nT''=nV}[T'']\\ &= 0.\end{aligned}$$

Als nächstes werden wir verschiedene Gleichungen für c und d herleiten. Dafür sind $U, V, W \in E[n^2]$.

a. $d(V,W)^n = c(nV,nW)$:

$$\begin{aligned}d(V,W)^n &= \frac{g_{nV+nW}(X)^n}{g_{nV}(X)^n g_{nW}(X-V)^n}\\ &= \frac{f_{nV+nW}(nX)}{f_{nV}(nX) f_{nW}(nX-nV)}\\ &= c(nV,nW)\end{aligned}$$

b. $d(V,W+nU) = d(V,W)$ und $d(V+nU,W) = d(V,W)e_n(nU,nW)$:

Da $n(W+nU) = nW$ ist, gilt

$$\begin{aligned}d(V,W+nU) &= \frac{g_{nV+n(W+nU)}(X)}{g_{nV}(X) g_{n(W+nU)}(X-V)}\\ &= \frac{g_{nV+nW}(X)}{g_{nV}(X) g_{nW}(X-V)}\\ &= d(V,W).\end{aligned}$$

Und ebenso gilt

$$\begin{aligned}d(V+nU,W) &= \frac{g_{n(V+nU)+nW}(X)}{g_{n(V+nU)}(X) g_{nW}(X-V-nU)}\\ &= \frac{g_{nV+nW}(X)}{g_{nV}(X) g_{nW}(X-V)} \frac{g_{nW}(X-V)}{g_{nW}(X-V-nU)}\\ &= d(V,W)e_n(nU,nW).\end{aligned}$$

c. $\frac{d(U,V)}{d(V,U)} = \frac{d(V,W)d(U+W,V)}{d(V,U+W)d(W,V)}$

Wir wenden die Definition von d an:

$$\begin{aligned} g_{nU+(nV+nW)}(X) &= d(U, V+W)g_{nU}(X)g_{nV+nW}(X-U) \\ &= d(U, V+W)g_{nU}(X)d(V, W)g_{nV}(X-U)g_{nW}(X-U-V). \end{aligned}$$

Ebenso erhalten wir

$$\begin{aligned} g_{(nU+nV)+nW}(X) &= d(U+V, W)g_{nU+nv}(X)g_{nW}(X-U-V) \\ &= d(U+V, W)d(U, V)g_{nU}(X)g_{nV}(X-U)g_{nW}(X-U-V). \end{aligned}$$

Wir können die beiden Gleichungen gleichsetzen und gleiche Terme streichen, um

$$d(U, V+W)d(V, W) = d(U+V, W)d(U, V) \tag{5.1}$$

zu erhalten. Stellen wir sie nochmal mit vertauschtem U und V auf und teilen beide durcheinander, erhalten wir

$$\frac{d(U,V)}{d(V,U)} = \frac{d(U, V+W)d(V, W)}{d(V, U+W)d(U, W)}. \tag{5.2}$$

Vertauschen wir in Gleichung 5.1 nochmal V und W und lösen nach $d(U, W)$ auf, erhalten wir

$$d(U, W) = \frac{d(U, V+W)d(W, V)}{d(U+W, V)}.$$

Setzen wir dies noch in Gleichung 5.2 ein, erhalten wir das Ergebnis.

d. Seien $S, T \in E[n]$. Dann gilt $e_n(S,T) = \frac{c(S,T)}{c(T,S)}$:

Wir wählen $U, V \in E[n^2]$ so, dass $nU = S, nV = T$. Die linke Seite der vorigen Formel hängt nicht von W ab. Demnach können wir sie an $W = jU$ für $0 \leq j < n$ auswerten und dadurch folgendes erhalten

$$\begin{aligned} \frac{c(S,T)}{c(T,S)} &= \frac{c(nU, nV)}{c(nV, nU)} \\ &= \left(\frac{d(U,V)}{d(V,U)}\right)^n \\ &= \prod_{j=0}^{n-1} \frac{d(V, jU)d(U+jU, V)}{d(V, U+jU)d(jU, V)} \\ &= \frac{d(V, O)d(nU, V)}{d(V, nU)d(O, V)} \\ &= e_n(nU, nV) \\ &= e_n(S, T), \end{aligned}$$

wobei wir im vorletzten Schritt die Gleichungen aus Teil b genutzt haben.

Wir haben eben gezeigt, dass

$$e_n(S,T) = \frac{c(S,T)}{c(T,S)} = \frac{f_T(X)f_S(X-T)}{f_S(X)f_T(X-S)}. \tag{5.3}$$

Seien nun

$$D'_S = [S] - [O] \text{ und } D'_T = [X_0] - [X_0 - T],$$

wobei $X_0 \notin \{O, S, T, T+S\}$ so gewählt ist, dass D'_S und D'_T keine gemeinsamen Punkte haben. Seien jetzt $F'_S(X) := f_S(X)$ und $F'_T(X) := \frac{1}{f_T(X_0 - X)}$. Dann gilt

$$\begin{aligned}
\operatorname{div}(F'_S) &= n[S] - n[O] = nD'_S, \\
\operatorname{div}(F'_T) &= -\operatorname{div}(f_T(X_0 - X)) = n[X_0] - n[X_0 - T] = nD'_T.
\end{aligned}$$

Zusammen mit Gleichung 5.3 erhalten wir das gewünschte

$$e_n(S,T) = \frac{F'_T(D'_S)}{F'_S(D'_T)}.$$

Jetzt betrachten wir eine beliebige Wahl an Divisoren. Sei D_S ein beliebiger Divisor von Grad 0 mit Summe S, D_T ein beliebiger Divisor von Grad 0 mit Summe T. Dann gilt für entsprechende zwei Funktionen $h_1, h_2 \in K(E)$, dass $D_S = \operatorname{div}(h_1) + D'_S$ und $D_T = \operatorname{div}(h_2) + D'_T$. Seien $F_S := h_1^n F'_S$ und $F_T := h_2^n F'_T$. Dann gilt

$$\begin{aligned}
\operatorname{div}(F_S) &= \operatorname{div}(h_1^n) + \operatorname{div}(F'_S) \\
&= n\operatorname{div}(h_1) + nD'_S \\
&= nD_S
\end{aligned}$$

und ebenso $\operatorname{div}(F_T) = nD_T$. Wir nehmen zunächst an, dass D'_S und D_S disjunkt von D_T und D'_T sind. Dann gilt

$$\begin{aligned}
\frac{F_T(D_S)}{F_S(D_T)} &= \frac{h_2(D_S)F'_T(D_S)}{h_1(D_T)F'_S(D_T)} \\
&= \frac{h_2(\operatorname{div}(h_1))^n h_2(D'_S)^n F'_T(\operatorname{div}(h_1)F'_T(D'_S))}{h_1(\operatorname{div}(h_2))^n h_1(D'_T)^n F'_S(\operatorname{div}(h_2))F'_S(D'_T)}.
\end{aligned}$$

Mit Satz 4.63 erhalten wir $h_2(\operatorname{div}(h_1)) = h_1(\operatorname{div}(h_2))$,

$$h_2(D'_S)^n = h_2(nD'_S) = h_2(\operatorname{div}(F'_S)) = F'_S(\operatorname{div}(h_2))$$

und ebenso $h_1(D'_T)^n = F'_T(\operatorname{div}(h_2))$. Damit erhalten wir

$$\frac{F_T(D_S)}{F_S(D_T)} = \frac{F'_T(D'_S)}{F'_S(D'_T)} = e_n(S,T).$$

Sind D_S und D'_S nicht notwendigerweise von D'_T und D_T disjunkt, so definieren wir

$$D''_S = [X_1 + S] - [X_1],\ D''_T = [Y_1 + T] - [Y_1],$$

wobei X_1 und Y_1 so gewählt sind, dass D'_S und D''_S von D'_T und D''_T disjunkt sind und sodass D''_S und D_S disjunkt sind von D''_T und D_T. Das vorherige Argument zeigt

$$\frac{F_T(D_S)}{F_S(D_T)} = \frac{F''_T(D''_S)}{F''_S(D_T)} = \frac{F'_T(D'_S)}{F'_S(D'_T)} = e_n(S,T). \qquad \square$$

5.1.2 Millers Algorithmus

Für die im vorhergegangenen Abschnitt eingeführte Formulierung des Weil-Pairings können wir einen Algorithmus angeben, der dieses berechnet. Dafür benötigen wir auch nur den folgenden Satz.

Algorithmus 5.1 Millers Algorithmus

```
1: Setze T = P und f = 1
2: for i = t − 1 to 0 do
3:     f ← f^2 h_{T,T}
4:     T ← 2T
5:     if ε_i = 1 then
6:         f ← f h_{T,P}
7:         T = T + P
8:     end if
9: end for
10: return f
```

Satz 5.2 *Sei $E(K)$ eine elliptische Kurve und seien $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ zwei Punkte ungleich Null.*

a. Sei λ die Steigung der Linie, die P und Q verbindet, bzw. die Steigung der Tangente an $E(K)$ an P, falls $P = Q$. Sollte die Linie vertikal sein, setzen wir $\lambda = \infty$. Wir definieren die folgende Funktion:

$$h_{P,Q} = \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2}, & \text{falls } \lambda \neq \infty \\ x - x_P, & \text{falls } \lambda = \infty \end{cases}$$

Dann gilt

$$\operatorname{div}(h_{P,Q}) = [P] + [Q] - [P + Q] - [O].$$

b. Sei $N \geq 1$. Wir schreiben N in ihrer Binärdarstellung als

$$N = \epsilon_0 + \epsilon_1 2 + \epsilon_2 2^2 + \cdots + \epsilon_t 2^t$$

mit $\epsilon_i \in \{0, 1\}$ und $\epsilon_t = 1$. Algorithmus 5.1 berechnet dann eine Funktion f_P mit Divisor

$$\operatorname{div}(f_P) = N[P] - [NP] - (N - 1)[O].$$

Beweis In disem Beweis folgen wir [Sil09, Theorem XI.8.1].

a. Wir nehmen zunächst an, dass $\lambda \neq \infty$. Sei $y = \lambda x + \nu$ die Linie durch P und Q bzw. die Tangente an P, falls $P = Q$. Diese Linie schneidet $E(K)$ an den drei Punkten $P, Q, -P - Q$, woraus wir schließen, dass

$$\operatorname{div}(y - \lambda x - \nu) = [P] + [Q] + [-P - Q] - 3[O].$$

Außerdem erhalten wir

$$\operatorname{div}(x - x_{P+Q}) = [P+Q] + [-P-Q] - 2[O],$$

da die Linie senkrecht ist. Damit berechnen wir

$$\begin{aligned}
\operatorname{div}(h_{P,Q}) &= \operatorname{div}\left(\frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2}\right) \\
&= \operatorname{div}\left(\frac{y - \lambda x - \nu}{x - x_{P+Q}}\right) \\
&= \operatorname{div}(y - \lambda x - \nu) - \operatorname{div}(x - x_{P+Q}) \\
&= [P] + [Q] + [-P-Q] - 3[O] - ([P+Q] + [-P-Q] - 2[O]) \\
&= [P] + [Q] - [P+Q] - [O].
\end{aligned}$$

Für die zweite Gleichheit ziehen wir Gleichung 3.3 zur Hilfe. So können wir im Nenner $x_{P+Q} = \lambda^2 - x_P - x_Q$ setzen. Im Zähler ersetzen wir $y_P = \lambda x_P + \nu$.

Ist $\lambda = \infty$, so ist $P + Q = O$, also $Q = -P$. Dann hat

$$\begin{aligned}
\operatorname{div}(x - x_P) &= [P] + [-P] - 2[O] \\
&= [P] + [Q] - [P+Q] - [O]
\end{aligned}$$

die gewünschte Form.

b. In Teil a haben wir die Divisoren der beiden in Zeile 3 und Zeile 6 des Algorithmus benutzten Funktionen berechnet. Diese sind

$$\begin{aligned}
\operatorname{div}(h_{T,T}) &= 2[T] - [2T] - [O], \\
\operatorname{div}(h_{T,P}) &= [T] + [P] - [T+P] - [O].
\end{aligned}$$

Wir betrachten jetzt die i-te Iteration der Schleife von Zeile 2 bis 9. Die Startwerte der Variablen T und f in dieser Iteration nennen wir T_i^{start} und f_i^{start}, die Endwerte der Iteration T_i^{end} und f_i^{end}. Wir schauen uns zuerst T an. In Zeile 4 wird T zunächst verdoppelt und, falls $\epsilon_i = 1$, P addiert. Das führt uns zu der Relation

$$T_i^{\text{end}} = 2T_i^{\text{start}} + \epsilon_i P.$$

Ebenso können wir f betrachten. Diese Funktion wird in Zeile 3 zunächst quadriert und dann mit $h_{T,T}$ multipliziert. Sollte $\epsilon_i = 1$ sein, wird sie in Zeile 6 noch mit $h_{T,P}$ multipliziert. Dies führt uns zu

$$f_i^{\text{end}} = (f_i^{\text{start}})^2 \cdot h_{T_i^{\text{start}},T_i^{\text{start}}} \cdot h_{2T_i^{\text{start}},P}^{\epsilon_i}.$$

Damit können wir den Divisor von f_i^{start} mit dem von f_i^{end} in Relation setzen.

$$\begin{aligned}
\operatorname{div}(f_i^{\text{end}}) &= 2\operatorname{div}(f_i^{\text{start}}) + \operatorname{div}(h_{T_i^{\text{start}},T_i^{\text{start}}}) + \epsilon_i \operatorname{div}(h_{2T_i^{\text{start}},P}) \\
&= 2\operatorname{div}(f_i^{\text{start}}) + (2[T_i^{\text{start}}] - [2T_i^{\text{start}}] - [O]) \\
&\quad + \epsilon_i([2T_i^{\text{start}}] + [P] - [2T_i^{\text{start}} + P] - [O]) \\
&= 2\operatorname{div}(f_i^{\text{start}}) + 2[T_i^{\text{start}}] - [2T_i^{\text{start}} + \epsilon_i P] + \epsilon_i[P] - (1+\epsilon_i)[O] \\
&= 2\operatorname{div}(f_i^{\text{start}}) + 2[T_i^{\text{start}}] - [T_i^{\text{end}}] + \epsilon_i[P] - (1+\epsilon_i)[O].
\end{aligned}$$

Die finalen Werte von T und f nach jedem Schleifendurchlauf sind die Anfangswerte der nächsten Iteration, weswegen gilt $T_i^{\text{end}} = T_{i-1}^{\text{start}}$ und $f_i^{\text{end}} = f_{i-1}^{\text{start}}$. Dies erlaubt uns, die Gleichungen für T und f umzuschreiben:

$$\begin{aligned} T_{i-1}^{\text{start}} - 2T_i^{\text{start}} &= \epsilon_i P, \\ \operatorname{div}(f_{i-1}^{\text{start}}) - 2\operatorname{div}(f_i^{\text{start}}) &= 2[T_i^{\text{start}}] - [T_{i-1}^{\text{start}}] + \epsilon_i [P] - (1+\epsilon_i)[O]. \end{aligned}$$

Dies hilft uns den finalen Wert von T zu berechnen:

$$\begin{aligned} T_0^{\text{end}} &= \epsilon_0 + 2T_0^{\text{start}} \\ &= \epsilon_0 P + \left(\sum_{i=1}^{t-1} 2^i (T_{i-1}^{\text{start}} - 2T_i^{\text{start}}) \right) + 2^t T_{i-1}^{\text{start}} \\ &= \epsilon_0 P + \sum_{i=1}^{t-1} 2^i \epsilon_i P + 2^t T_{t-1}^{\text{start}} \\ &= \sum_{i=0}^{t} 2^i \epsilon_i P \\ &= NP. \end{aligned}$$

Damit können wir den Divisor der vom Algorithmus berechneten Funktion angeben:

$$\begin{aligned} \operatorname{div}(f_0^{\text{end}}) &= 2\operatorname{div}(f_0^{\text{start}}) + 2[T_0^{\text{start}}] - [T_0^{\text{end}}] + \epsilon_0 [P] - (1+\epsilon_0)[O] \\ &= \left(\sum_{i=1}^{t-1} 2^i (\operatorname{div}(f_{i-1}^{\text{start}}) - 2\operatorname{div}(f_i^{\text{start}})) \right) \\ &\quad + 2[T_0^{\text{start}}] - [NP] + \epsilon_0 [P] - (1+\epsilon_0)[O] \\ &= \left(\sum_{i=1}^{t-1} 2^i (2[T_i^{\text{start}}] - [T_{i-1}^{\text{start}}] + \epsilon_i [P] - (1+\epsilon_i)[O]) \right) \\ &\quad + 2[T_0^{\text{start}}] - [NP] + \epsilon_0 [P] - (1+\epsilon_0)[O] \\ &= 2^t [T_{t-1}^{\text{start}}] + \sum_{i=0}^{t-1} 2^i \epsilon_i [P] - \sum_{i=0}^{t-1} 2^i (1+\epsilon_i)[O] - [NP] \\ &= N[P] - (N-1)[O] - [NP]. \end{aligned}$$

□

Ist jetzt $P \in E[n]$, erlaubt uns Millers Algorithmus eine Funktion f_P mit Divisor $\operatorname{div}(f_P) = n[P] - n[O]$ zu berechnen.

Seien also $P, Q \in E[n]$ und $S \in E(K)$ ein beliebiger Punkt, der nicht in der von P und Q erzeugten Untergruppe liegt. Seien $f_P \in K(E)$ mit $\operatorname{div}(f_P) = n[P] - n[O]$ und $f_Q \in K(E)$ mit $\operatorname{div}(f_Q) = n[Q] - n[O]$. Sei zusätzlich $f \in K(E)$ eine Funktion mit $\operatorname{div}(f) = n[P+S] - m[S]$.

Damit sind für f und f_Q die Voraussetzungen an Satz 5.1 erfüllt und das Weil-Pairing definiert. Somit gilt

$$\begin{aligned} e_n(P,Q) &= e_n((P+S)-S, Q-O) \\ &= \frac{f([Q]-[O])}{f_Q([P+S]-[S])} \\ &= \frac{f(Q)f_Q(S)}{f(O)f_Q(P+S)} \\ &= \frac{f_P(Q-S)f_Q(S)}{f_P(-S)f_Q(P+S)}. \end{aligned}$$

Letztere Gleichheit entsteht dadurch, dass die Nullstellen von f gerade die von f_P um S verschoben sind. Die letzte Formel kann dann mithilfe Millers Algorithmus ausgewertet werden.

5.2 Tate-Lichtenbaum-Pairing

Im letzten Abschnitt haben wir gesehen, wie wir das Weil-Pairing mithilfe von Millers Algorithmus berechnen können. Nach Bemerkung 4.65 können wir das Tate-Lichtenbaum-Pairing mithilfe des Weil-Pairings folgendermaßen ausdrücken:

$$\langle P,Q\rangle_n = e_n(P, R-\phi_q(R))^{\frac{1}{n}}$$

Um dies zu berechnen können wir dann einfach Millers Algorithmus benutzen und haben so eine einfache Art der Berechnung des Tate-Lichtenbaum-Pairings erhalten.

In diesem Abschnitt schauen wir uns noch eine zweite Art der Berechnung des Pairings an. Dabei nutzen wir das Paper [Sta07] von Katherine Stange. Sie präsentiert dort eine Berechnungsmöglichkeit mithilfe elliptischer Netze.

Dafür starten wir mit der Definition ellitptischer Netze.

Definition 5.3 *Sei A eine endlich erzeugte freie abelsche Gruppe und R ein Integritätsring. Dann ist eine Abbildung $W : A \to R$ ein elliptischen Netz, wenn für alle $p,q,r,s \in A$ gilt, dass*

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &+W(q+r+s)W(q-r)W(p+s)W(p) \\ &+W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned}$$

Die Menge der elliptischen Netze bezeichnen wir mit $\mathcal{EN}(A,R)$.

In unserem Fall wird A die Divisorengruppe, bzw. eine Untergruppe derer, und R ein endlicher Körper sein.

Wir halten zunächst ein einfaches Resultat über elliptische Netze fest.

Satz 5.4 *Sei $W : A \to R$ ein elliptisches Netz, $f : B \to A$ ein Homomorphismus freier abelscher Gruppen und $g : R \to S$ ein Homomorphismus zwischen Integritätsringen. Dann sind die folgenden Abbildungen ebenfalls elliptische Netze:*

a. $W \circ f : B \to R$

b. $g \circ W : A \to S$

Beweis Beide Behauptungen sieht man sofort durch Anwendung der Homomorphieeigenschaften.□

Unser Ziel ist zunächst, von einer elliptischen Kurve über den komplexen Zahlen $\mathbb{C}$ ein elliptisches Netz zu erzeugen. Dafür benötigen wir Eigenschaften elliptischer Kurven über $\mathbb{C}$. Wir folgen der kurzen Einführung in [Was08, Kapitel 9.1].

Definition 5.5 *Seien $\omega_1, \omega_2 \in \mathbb{C}$ zwei über $\mathbb{R}$ linear unabhängige komplexe Zahlen. Dann nennen wir*

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}.$$

ein komplexes Gitter. Die Menge

$$F = \{a_1\omega_1 + a_2\omega_2 | 0 \leq a_i < 1, i = 1, 2\}$$

nennen wir das fundamentale Parallelogramm von Λ.

Damit Funktionen auf $\mathbb{C}$ auch auf $\mathbb{C}/\Lambda$ Sinn ergeben, benötigen diese bestimmte Periodizitätseigenschaften. Besonders die der elliptischen Funktionen möchten wir hervorheben.

Definition 5.6 *Für ein komplexes Gitter Λ nennen wir eine meromorphe Funktion $f : \mathbb{C} \to \mathbb{C}$ mit*

$$f(z + \omega) = f(z)$$

für alle $z \in \mathbb{C}$ und $\omega \in \Lambda$ eine elliptische Funktion. Eine äquivalente Beschreibung ist, wenn

$$f(z + \omega_i) = f(z),\ i = 1, 2$$

gilt.

Definition 5.7 *Für ein komplexes Gitter Λ definieren wir die komplexe weierstraßsche Sigma Funktion $\sigma : \mathbb{C} \to \mathbb{C}$ durch*

$$\sigma(z; \Lambda) := z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{w} + \frac{1}{2}\left(\frac{z}{w}\right)^2},$$

die weierstraßsche Zeta Funktion $\zeta : \mathbb{C} \to \mathbb{C}$ durch

$$\zeta(z; \Lambda) := \frac{1}{z} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z - \omega)} - \frac{1}{\omega} + \frac{z}{\omega^2}\right),$$

die weierstraßsche Eta Funktion $\eta : \Lambda \to \mathbb{C}$ durch

$$\eta(\omega; \Lambda) := \zeta(z + \omega; \Lambda) - \zeta(z; \Lambda)$$

und die weierstraßsche P Funktion durch

$$\wp(z, \Lambda) := \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}\right).$$

Satz 5.8 *Die weierstraßsche Eta Funktion ist wohldefiniert, also tatsächlich von z unabhängig.*

Beweis Einen Beweis findet man in [AE06, Proposition 7.4]. □

Satz 5.9 *Die weierstraßsche P Funktion ist eine elliptische Funktion.*

Sei $\lambda : \Lambda \to \{\pm 1\}$ *definiert durch:*

$$\lambda(\omega) = \begin{cases} 1 & \text{für } \omega \in 2\Lambda, \\ -1 & \text{für } \omega \notin 2\Lambda. \end{cases}$$

Dann gilt für die weierstraßsche Sigma Funktion

$$\sigma(z+\omega;\Lambda) = \lambda(\omega) e^{\eta(\omega)(z+\frac{1}{2}\omega)} \sigma(z;\Lambda).$$

Beweis Einen Beweis für die P Funktion findet man in [Was08, Theorem 9.3].

Einen Beweis für die Sigma Funktion findet man in [AE06, Proposition 7.4]. □

Komplexe Gitter sind eng mit elliptischen Kurven verknüpft. Insbesondere sind diese auf gewisse Art isomorph. Dafür benötigen wir zunächst eine Definition.

Definition 5.10 *Sei* Λ *ein komplexes Gitter. Für natürliche Zahlen* $k \geq 3$ *definieren wir die Eisenstein Reihe als*

$$G_k = G_k(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-k}.$$

Außerdem setzen wir $g_2(\Lambda) = 60G_4$ *und* $g_3(\Lambda) = 140G_6$.

Satz 5.11 *a. Sei* Λ *ein komplexes Gitter und* $E(\mathbb{C})$ *die elliptische Kurve* $y^2 = 4x^3 - g_2 x - g_3$. *Dann ist die Abbildung*

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto O \end{aligned}$$

ein Gruppenisomorphismus.

b. Sei $y^2 = 4x^3 - Ax - B$ *eine elliptische Kurve* $E(\mathbb{C})$. *So existiert ein komplexes Gitter* Λ *mit*

$$g_2(\Lambda) = A \text{ und } g_3(\Lambda) = B.$$

Dann ist die Abbildung Φ *aus Teil a ein Isomorphismus der Gruppen* $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$.

Beweis Beweise findet man in [Was08, Theorem 9.10] und [Was08, Theorem 9.21]. □

Wir können also beliebig zwischen elliptischen Kurve und komplexen Gittern wechseln. Außerdem können wir elliptische Funktionen als Funktionen auf elliptischen Kurven betrachten. Als nächstes wollen wir ähnlich wie für elliptische Kurven den Begriff des Divisors für Gitter einführen. Dafür wiederholen wir zunächst Begriffe aus der Funktionentheorie.

Definition 5.12 *Es sei D eine nichtleere offene Teilmenge von $\mathbb{C}$ und $P_f \subset \mathbb{C}$ eine Teilmenge, welche nur aus isolierten Punkten besteht. Eine Funktion f heißt meromorph, wenn sie für Werte aus $D \backslash P_f$ definiert und komplex differenzierbar ist und für Werte aus P_f Pole hat.*

Definition 5.13 *Die Ordnung eines Pols einer meromorphen Funktion kann man an der Laurentreihe*

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z - z_0),$$

wobei $a_n \in \mathbb{C}$ und $z_0 \in \mathbb{C}$ der Entwicklungspunkt der Reihe ist, ablesen. Die Reihe bricht für eine meromorphe Funktion ab und nimmt die Form $\sum_{n=r}^{\infty} a_n (z - z_0)$ an. r kann dabei negativ, 0 oder positiv sein und wir definieren $r := \mathrm{ord}_{z_0} f$.

Damit können wir Divisoren definieren.

Definition 5.14 *Für ein komplexes Gitter Λ definieren wir einen Divisor D als eine endliche formale Summe von Punkten*

$$D = \sum_j a_j [z_j],$$

wobei $a_j \in \mathbb{Z}$ und $z_j \in F$.

Für eine Funktion f definieren wir den Divisor von f als

$$div(f) := \sum_{z \in F} \mathrm{ord}_z f [z].$$

Für diese Divisoren gelten die gleichen Rechenregeln wie für die für elliptische Kurven.

Mithilfe der weierstraßschen Funktionen können wir nun diejenige definieren, die uns zu den elliptischen Netzen führen wird.

Definition 5.15 *Sei Λ ein zu einer elliptischen Kurve $E(\mathbb{C})$ gehöriges Gitter. Für ein $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ definieren wir die Funktion Ψ_v:*

$$\begin{aligned} \Psi_v : \mathbb{C}^n &\to \mathbb{C} \\ z = (z_1, \ldots, z_n) &\mapsto \frac{\sigma\left(\sum_{i=1}^n v_i z_i; \Lambda\right)}{\prod_{i=1}^n \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}. \end{aligned}$$

Ist $v = 0$, so setzen wir $\Psi_v \equiv 0$.

Nach einem kleinen Hilfslemma zeigen wir, dass die Funktionen elliptisch sind.

Satz 5.16 *Sei Λ ein komplexes Gitter. Dann gilt für die weierstraßsche Eta Funktion*

$$\eta(n\omega) = n\eta(\omega)$$

für $n \in \mathbb{Z}$ und $\omega \in \Lambda$.

Beweis Sei zunächst $\lambda : \Lambda \to \{\pm 1\}$ definiert durch

$$\lambda(\omega) = \begin{cases} 1 & \text{für } \omega \in 2\Lambda, \\ -1 & \text{für } \omega \notin 2\Lambda. \end{cases}$$

Dann gilt $\frac{\lambda(n\omega)}{\lambda(\omega)^n} = 1$. Dafür unterscheiden wir verschiedene Fälle.

n gerade: Der Zähler ist gleich 1, da $n\omega \in 2\Lambda$ und der Nenner ebenfalls, da wir 1 oder -1 mit einer geraden Zahl potenzieren.

n ungerade und $\omega \in 2\Lambda$: Beide λ Funktionen sind bereits gleich 1.

n ungerade und $\omega \notin 2\Lambda$: Zähler und Nenner sind gleich -1, der Bruch dadurch gleich 1.

Zum Beweis des eigentlichen Satzes nutzen wir die Transformationsformel der weierstraßschen Sigma Funktion aus Satz 5.9. Wir behaupten, es gilt

$$\sigma(z + n\omega) = \lambda(\omega)^n e^{n\eta(\omega)(z+\frac{n}{2}\omega)}\sigma(z).$$

Wir führen einen Beweis durch Induktion.

Induktionsanfang: $n = 1$ ist einfach Satz 5.9.

Induktionsvorraussetzung: Für ein $n \in \mathbb{N}$ gelte $\sigma(z + n\omega) = \lambda(\omega)^n e^{n\eta(\omega)(z+\frac{n}{2}\omega)}\sigma(z)$.

Induktionsschluss: Wir nutzen die Transformationsformel für die Sigma Funktion und die Induktionsvorraussetzung.

$$\begin{aligned} \sigma(z + (n+1)\omega) &= \sigma((z + n\omega) + \omega) \\ &= \lambda(\omega) e^{\eta(\omega)(z+n\omega+\frac{1}{2}\omega)}\sigma(z + n\omega) \\ &= \lambda(\omega) e^{\eta(\omega)(z+n\omega+\frac{1}{2}\omega)}\lambda(\omega)^n e^{n\eta(\omega)(z+\frac{n}{2}\omega)}\sigma(z) \\ &= \lambda(\omega)^{n+1} e^{\eta(\omega)(z+nz+\frac{1}{2}\omega+n\omega+\frac{n^2}{2}\omega)}\sigma(z) \\ &= \lambda(\omega)^{n+1} e^{\eta(\omega)((n+1)z+\frac{(n+1)^2}{2}\omega)}\sigma(z) \end{aligned}$$

Dies beendet den Induktionsbeweis. Den gleichen Beweis kann man auch für negative n führen und außerdem ist die Aussage für $n = 0$ trivialerweise erfüllt, sodass die sie für ganz $\mathbb{Z}$ gilt.

Andererseits gilt mit Satz 5.9 auch

$$\sigma(z + n\omega) = \lambda(n\omega) e^{\eta(n\omega)(z+\frac{1}{2}n\omega)}\sigma(z).$$

Dies ist möglich, da $n\omega \in \Lambda$. Setzen wir die beiden Gleichungen nun gleich, erhalten wir mit der eben berechneten Identität für λ

$$\begin{aligned} &\lambda(\omega)^n e^{n\eta(\omega)(z+\frac{n}{2}\omega)}\sigma(z) = \lambda(n\omega) e^{\eta(n\omega)(z+\frac{1}{2}n\omega)}\sigma(z) \\ &\Leftrightarrow 1 = \frac{\lambda(n\omega)}{\lambda(\omega)^n} e^{\eta(n\omega)(z+\frac{1}{2}n\omega) - n\eta(\omega)(z+\frac{1}{2}n\omega)} \\ &\Leftrightarrow 1 = e^{(z+\frac{1}{2}n\omega)(\nu(n\omega) - n\nu(\omega))}. \end{aligned}$$

Damit diese Gleichung erfüllt ist, muss der Exponent 0 werden. Nachdem η von z unabhängig ist, können wir dies beliebig wählen. Wir wählen es also, sodass $z + \frac{1}{2}n\omega \neq 0$. Dann erhalten wir die gesuchte Behauptung und es gilt $\eta(n\omega) = n\eta(\omega)$. □

Satz 5.17 *Die Funktionen Ψ_v sind in jeder Variable elliptisch.*

Beweis Wir folgen dem Beweis in [Sta07, Proposition 1].

Ohne Beschränkung der Allgemeinheit betrachten wir die Variable z_1. Sei $\omega \in \Lambda$, $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ und $z = (z_1, \ldots, z_n), w = (\omega, 0, \ldots, 0) \in \mathbb{C}^n$. Wir schreiben vereinfachend $\sigma(z) := \sigma(z; \Lambda)$. Mithilfe der Definition, Satz 5.9 und Rechenregeln für die weierstraßsche Zeta Funktion berechnen wir zunächst die einzelnen Terme in $\Psi_v(z + w; \Lambda)$:

$$\sigma\left(\sum_{i=1}^{n} v_i(z_i + w_i)\right) = \lambda(v_1\omega)e^{\eta(v_1\omega)\left(\left(\sum_{i=1}^{n} v_i z_i\right)+\frac{1}{2}\omega v_1\right)}\sigma\left(\sum_{i=1}^{n} v_i z_i\right)$$

$$\begin{aligned}\prod_{i=1}^{n}\sigma(z_i + w_i)^{2v_i^2-\sum_{j=1}^{n} v_i v_j} &= \left(\lambda(\omega)e^{\eta(\omega)(z_1+\frac{1}{2}\omega)}\right)^{2v_1^2-\sum_{j=1}^{n} v_1 v_j}\prod_{i=1}^{n}\sigma(z_i;)^{2v_i^2-\sum_{j=1}^{n} v_i v_j} \\ &= \lambda(\omega)^{2v_i^2-\sum_{j=1}^{n} v_i v_j}e^{\eta(\omega)\left(z_1+\frac{1}{2}\omega\right)\left(2v_1^2-\sum_{j=1}^{n} v_1 v_j\right)}\prod_{i=1}^{n}\sigma(z_i;)^{2v_i^2-\sum_{j=1}^{n} v_i v_j}\end{aligned}$$

$$\begin{aligned}\prod_{1\le i<j\le n}\sigma(z_i + w_i + z_j + w_j)^{v_i v_j} &= \prod_{j=2}^{n}\lambda(\omega)^{v_1 v_j}e^{\eta(\omega)\left(z_1+z_j+\frac{1}{2}\omega\right)v_1 v_j}\prod_{1\le i<j\le n}\sigma(z_i + z_j)^{v_i v_j} \\ &= \lambda(\omega)^{\sum_{i=2}^{n} v_1 v_j}e^{\eta(\omega)\sum_{j=2}^{n}\left(z_1+z_j+\frac{1}{2}\omega\right)v_1 v_j}\prod_{1\le i<j\le n}\sigma(z_i + z_j)^{v_i v_j}\end{aligned}$$

Setzen wir dies nun ein und kürzen alle σ Terme, so erhalten wir mithilfe von Satz 5.16

$$\begin{aligned}H &= \frac{\Psi_v(z + w; \Lambda)}{\Psi_v(z; \Lambda)} \\ &= \frac{\lambda(v_1\omega)e^{\eta(v_1\omega)\left(\left(\sum_{i=1}^{n} v_I z_i\right)+\frac{1}{2}\omega v_1\right)}}{\lambda(\omega)^{2v_i^2-\sum_{j=1}^{n} v_i v_j}e^{\eta(\omega)\left(z_1+\frac{1}{2}\omega\right)\left(2v_1^2-\sum_{j=1}^{n} v_1 v_j\right)}\lambda(\omega)^{\sum_{i=2}^{n} v_1 v_j}e^{\eta(\omega)\sum_{j=2}^{n}\left(z_1+z_j+\frac{1}{2}\omega\right)v_1 v_j}} \\ &= \frac{\lambda(v_1\omega)}{\lambda(\omega)^{v_1^2}}e^{\eta(v_1\omega)\left(\sum_{i=1}^{n} v_i z_i+\frac{1}{2}\omega v_1\right)-\eta(\omega)\left(\sum_{i=1}^{n} v_1 v_i z_i+\frac{1}{2}\omega v_1^2\right)} \\ &= \frac{\lambda(v_1\omega)}{\lambda(\omega)^{v_1^2}}.\end{aligned}$$

Wir unterscheiden jetzt drei Fälle:

$\omega, v_1\omega \notin 2\Lambda$: Da $v_1\omega \notin 2\Lambda$, muss v_1 ungerade sein. Daher ist auch v_1^2 ungerade. Zähler und Nenner sind also beide gleich -1 und somit $H = 1$

$\omega \notin 2\Lambda, v_1\omega \in 2\Lambda$: Hier muss v_1 gerade sein, wodurch der Nenner zu 1 wird. Der Zähler ist es schon, weswegen $H = 1$.

$\omega \in 2\Lambda$: Jetzt ist automatisch $v_1\omega \in 2\Lambda$ und $H = 1$.

In allen Fällen ist also $H = 1$. Multiplizieren mit dem Nenner liefert die Behauptung. □

Bemerkung 5.18 *Wir können auf natürliche Weise die Abbildung Ψ_v auf elliptische Kurven fortsetzen. Dazu nutzen wir den Isomorphismus Φ aus Satz 5.11. Wir schreiben ebenso*

$$\begin{aligned}\Psi_v &: E(\mathbb{C})^n \to \mathbb{C}\\ P = (P_1, \ldots, P_n) &\mapsto \Psi_v((\Phi^{-1}(P_1), \ldots, \Phi^{-1}(P_n))).\end{aligned}$$

Implizit wählen wir dabei einen Repräsentanten eines Elements in $\mathbb{C}/\Lambda$. Dies bleibt aufgrund von Satz 5.17 wohldefiniert.

Satz 5.19 *Sei Λ ein zu einer elliptischen Kurve $E(\mathbb{C})$ gehöriges Gitter. Für ein $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ definieren wir die Funktion Ψ_v wie zuvor. Wir nehmen an, dass $z_i \notin \Lambda$ für alle $i = 1, \ldots, n$ und $z_i + z_j \notin \Lambda$ für alle $i \neq j$.Dann ist der Divisor der Funktion Ψ_v, betrachtet als Funktion in z_1, gegeben durch*

$$\left[\sum_{j=2}^{n}(-v_j)z_j\right] - \sum_{j=2}^{n} v_1 v_j[-z_j] - \left(v_1^2 - \sum_{j=2}^{n} v_1 v_j\right)[0].$$

Beweis Wir rechnen nach und schreiben vereinfachend $\sigma(z) := \sigma(z;\Lambda)$:

$$\begin{aligned}\operatorname{div}(\Psi_v(z_1)) &= \operatorname{div}\left(\frac{\sigma\left(\sum_{i=1}^{n} v_i z_i\right)}{\prod_{i=1}^{n}\sigma(z_i)^{2v_i^2-\sum_{j=1}^{n} v_i v_j}\prod_{1\le i<j\le n}\sigma(z_i+z_j)^{v_i v_j}}\right)\\ &= \operatorname{div}\left(\sigma\left(\sum_{i=1}^{n} v_i z_i\right)\right) - \left(2v_1^2 - \sum_{j=1}^{n} v_1 v_j\right)\operatorname{div}(\sigma(z_1)) - \operatorname{div}\left(\prod_{j=2}^{n}\sigma(z_1+z_j)^{v_1 v_j}\right)\\ &= \operatorname{div}\left(\sigma\left(\sum_{i=1}^{n} v_i z_i\right)\right) - \left(v_1^2 - \sum_{j=2}^{n} v_1 v_j\right)\operatorname{div}(\sigma(z_1)) - \sum_{j=2}^{n} v_1 v_j \operatorname{div}(\sigma(z_1+z_j))\\ &= \left[\sum_{j=2}^{n}(-v_j)z_j\right] - \left(v_1^2 - \sum_{j=2}^{n} v_1 v_j\right)[0] - \sum_{j=2}^{n} v_1 v_j[-z_j]\end{aligned}$$

Für die letzte Gleichheit betrachten wir die Nullstellen von $\sigma(z)$. Nach Definition wird diese an einem Punkt z_0 offensichtlich genau dann 0, wenn $z_0 \in \Lambda$. Sollte $\sum_{j=2}^{n}(-v_j)z_j$ nicht im fundamentalen Parallelogramm F von Λ liegen, so existiert aber dank Satz 5.17 eine entsprechende Nullstelle in F. □

Satz 5.20 *Sei T eine $n \times n$ Matrix mit Einträgen in $\mathbb{Z}$. Dann gilt für die Funktion Ψ_v folgende Transformationsformel:*

$$\Psi_v(T^{Tr}(z);\Lambda) = \frac{\Psi_{T(v)}(z;\Lambda)}{\prod_{i=1}^{n}\Psi_{T(e_i)}(z;\Lambda)^{2v_i-\sum_{j=1}^{n} v_i v_j}\prod_{1\le i<j\le n}\Psi_{T(e_i+e_j)}(z;\Lambda)^{v_i v_j}}$$

Beweis Der Beweis besteht nur aus Nachrechnen. Man findet ihn in [Akh12, Proposition 2.2.3] □

Für diese und die weierstraßschen Funktionen gibt es einige Identitäten.

Satz 5.21 *Seien $v, w, z \in \mathbb{C}^n$ und $x, a, b \in \mathbb{C}$. Dabei bezeichne $v \cdot z$ das Standardskalarprodukt von v und z. Seien außerdem $\wp$, σ und ζ die weierstraßschen P, Sigma und Zeta Funktionen für ein komplexes Gitter Λ. Dann gilt:*

$$\begin{aligned}
\wp(a) - \wp(b) &= -\frac{\sigma(a+b)\sigma(a-b)}{\sigma(a)^2\sigma(b)^2}, \\
\wp(v \cdot z) - \wp(w \cdot z) &= -\frac{\Psi_{v+w}(z)\Psi_{v-w}(z)}{\Psi_v(z)^2\Psi_w(z)^2}, \\
\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) &= \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)}, \\
\zeta(x+a+b) - \zeta(x+a) - \zeta(x+b) + \zeta(x) &= \frac{\sigma(2x+a+b)\sigma(a)\sigma(b)}{\sigma(x+a+b)\sigma(x+a)\sigma(x+b)\sigma(x)}
\end{aligned}$$

Beweis Einen Beweis findet man in [Akh12, Lemma 2.2.4 und Lemma 2.2.5]. Dieser nutzt einige Eigenschaften elliptischer Funktionen aus. □

Wir benötigen noch eine kleine Definition und Sätze, bevor wir unsere elliptisches Netz definieren können.

Definition 5.22 *Seien B, C abelsche Gruppen. Wir nennen eine Funktion $f : B \to C$ quadratische Funktion, wenn für alle $x, y, z \in B$ gilt, dass*

$$f(x+y+z) - f(x+y) - f(y+z) - f(x+z) + f(x) + f(y) + f(z) = 0.$$

Eine quadratische Funktion heißt quadratische Form, wenn $f(x) = f(-x)$ für alle $x \in B$ gilt.

Wie man schnell nachrechnet, ist auch die Summe quadratischer Formen eine quadratische Form.

Satz 5.23 *Eine quadratische Form $f : B \to C$ erfüllt die Parallelogrammgleichung*

$$f(x+y) + f(x-y) = 2f(x) + 2f(y).$$

Beweis Setzen wir $x = y = z = 0$, so erhalten wir direkt $f(0) = 0$. Setzen wir jetzt $z = -x$, so erhalten wir die gewünschte Gleichung. □

Satz 5.24 *Für eine quadratische Form : $B \to C$ gilt für $m \in \mathbb{Z}$ und $p, q \in B$*

$$f(mp) + f(q) - f(mp+q) = m(f(p) + f(q) - f(p+q)).$$

Beweis Wir führen einen Induktionsbeweis über m.

Induktionsanfang $m = 1$: Es gilt offensichtlich

$$f(1 \cdot p) + f(q) - f(1 \cdot p + q) = 1 \cdot (f(p + f(q) - f(p+q))).$$

Induktionsvoraussetzung: Für ein $N \in \mathbb{N}$ gelte $f(mp) + f(q) - f(mp+q) = m(f(p) + f(q) - f(p+q))$ für alle $m \leq N$.

Induktionsschluss: Wir nutzen die Parallelogrammgleichung und die Induktionsvoraussetzung zwei mal und berechnen

$$\begin{aligned} f((m+1)p) + f(q) - f((m+1)p+q) &= f(mp+p) + f(q) - f(mp+p+q) \\ &= 2f(mp) + 2f(p) - f((m-1)p) + f(q) \\ &\quad - 2f(mp+q) - 2f(p) + f((m-1)p+q) \\ &= 2(f(mp) + f(q) - f(mp+q)) \\ &\quad - (f((m-1)p) + f(q) - f((m-1)p+q)) \\ &= 2m(f(p) + f(q) - f(p+q)) \\ &\quad - (m-1)(f(p) + f(q) - f(p+q)) \\ &= (m+1)(f(p) + f(q) - f(p+q)). \end{aligned}$$

Für $m = 0$ ist die Behauptung trivialerweise erfüllt. Außerdem kann der gleiche Beweis für negative m geführt werden, weswegen die Behauptung für ganz $\mathbb{Z}$ gilt. □

Dies führt zur Definition unseres elliptischen Netzes.

Definition 5.25 *Sei $E(\mathbb{C})$ eine elliptische Kurve und $\phi : \mathbb{Z}^n \to E(\mathbb{C})$ ein Homomorphismus, sodass die Bilder der Basisvektoren $\pm e_i$ alle unterschiedlich und nicht Null sind. Dann definieren wir $W_\phi : \mathbb{Z}^n \to \mathbb{C}$ durch*

$$W_\phi(v) = \Psi_v((\phi(e_1), \phi(e_2), \ldots, \phi(e_n)); E(\mathbb{C})).$$

Satz 5.26 *W_ϕ ist ein elliptisches Netz.*

Beweis Wir folgen dem Beweis in [Akh12, Theorem 2.2.6].

Mit der Bedingung, dass die Bilder der Basisvektoren $\pm e_i$ unter ϕ alle unterschiedlich und nicht Null sind, stellen wir sicher, dass wir Ψ_v nicht an einer Polstelle auswerten.

Nach Definition, ist $\Psi_v = 0$, wenn $v = 0$. Wenn andersrum $\Psi_v = 0$ ist, bedeutet das, dass $\sigma(v \cdot z) = 0$ für alle z. Also muss $v = 0$ sein.

Wir wollen zeigen, dass die Gleichung in Definition 5.3 für alle $p, q, r, s \in \mathbb{Z}^n$ erfüllt ist. Dafür sei zunächst $p = 0$, also auch $W(p) = 0$. Da die weierstraßsche Sigma Funktion ungerade ist, wie schnell ersichtlich ist, gilt $W(-v) = -W(v)$ für alle $v \in \mathbb{Z}^n$. Damit können wir die Bedingung an Definition 5.3 nachrechnen:

$$W(q+s)W(-q)W(r+s)W(r) + W(r+s)W(r)W(q+s)W(q) = 0$$

Nachdem die Gleichung in Definition 5.3 in p, q und r symmetrisch ist, können wir annehmen, dass keiner davon Null ist. Wie wir bereits gezeigt haben, ist das äquivalent damit, dass keine der Funktionen Ψ_p, Ψ_q und Ψ_r Null ist. Mit Satz 5.21 erhalten wir

$$\frac{\Psi_{p+q}(z)\Psi_{p-q}(z)}{\Psi_p(z)^2\Psi_q(z)^2} = \wp(q \cdot z) - \wp(p \cdot z).$$

Wir können das gleiche auch für die Paare (q, r) und (r, p) machen. Das liefert uns

$$\frac{\Psi_{p+q}(z)\Psi_{p-q}(z)}{\Psi_p(z)^2\Psi_q(z)^2} + \frac{\Psi_{q+r}(z)\Psi_{q-r}(z)}{\Psi_q(z)^2\Psi_r(z)^2} + \frac{\Psi_{r+p}(z)\Psi_{r-p}(z)}{\Psi_r(z)^2\Psi_p(z)^2} = 0.$$

Bringen wir alles auf einen gemeinsamen Nenner, so erhalten wir

$$\Psi_{p+q}(z)\Psi_{p-q}(z)\Psi_r(z)^2 + \Psi_{q+r}(z)\Psi_{q-r}(z)\Psi_p(z)^2 + \Psi_{r+p}(z)\Psi_{r-p}(z)\Psi_q(z)^2 = 0.$$

Das ist für $s = 0$ genau die Gleichung, die wir zeigen müssen:

$$W(p+q)W(p-q)W(r)^2 + W(q+r)W(q-r)W(p)^2 + W(r+p)W(r-p)W(q)^2 = 0$$

Für den allgemeinen Fall, in dem $s \neq 0$ ist, nutzen wir, dass die Exponenten im Nenner der Funktion $\Psi_v(z)$ quadratische Formen sind, was man aufwendig nachrechnen kann. Dann gilt mit Satz 5.21, wobei wir die Abhängigkeit von z der Einfachheit weglassen,

$$\begin{aligned}\frac{\Psi_{p+q+s}\Psi_{p-q}\Psi_s}{\Psi_{p+s}\Psi_p\Psi_{q+s}\Psi_q} &= \frac{\sigma((p+q+s)\cdot z)\sigma((p-q)\cdot z)\sigma(s\cdot z)}{\sigma((p+s)\cdot z)\sigma(p\cdot z)\sigma((q+s)\cdot z)\sigma(q\cdot z)} \\ &= \zeta((p+s)\cdot z) - \zeta(p\cdot z) - \zeta((q+s)\cdot z) + \zeta(q\cdot z).\end{aligned}$$

Damit gilt also

$$\frac{\Psi_{p+q+s}\Psi_{p-q}\Psi_s}{\Psi_{p+s}\Psi_p\Psi_{q+s}\Psi_q} + \frac{\Psi_{q+r+s}\Psi_{q-r}\Psi_s}{\Psi_{q+s}\Psi_q\Psi_{r+s}\Psi_r} + \frac{\Psi_{r+p+s}\Psi_{r-p}\Psi_s}{\Psi_{r+s}\Psi_r\Psi_{p+s}\Psi_p} = 0,$$

oder wenn wir alles wieder auf einen Nenner bringen

$$\Psi_{p+q+s}\Psi_{p-q}\Psi_{r+s}\Psi_r + \Psi_{q+r+s}\Psi_{q-r}\Psi_{p+s}\Psi_p + \Psi_{r+p+s}\Psi_{r-p}\Psi_{q+s}\Psi_q = 0,$$

was genau die gewünschte Gleichung ist. □

Da wir aber an Kryptographie interessiert sind, benötigen wir ein elliptisches Netz für eine elliptische Kurve über einem endlichen Körper. Dies schaffen wir, indem wir das oben eingeführte elliptische Netz auf einen endlichen Körper reduzieren. Dafür benötigen wir zunächst ein paar algebraische Definitionen.

Definition 5.27 *Zahlkörper: Ein algebraischer Zahlkörper ist eine endliche Körpererweiterung L von $\mathbb{Q}$.*

Ganzheitsring: Sei L ein algebraischer Zahlkörper. Dann ist der Ganzheitsring R von L definiert als die Teilmenge derjenigen $x \in L$, die eine Gleichung der Form

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$$

mit $c_i \in \mathbb{Z}$ erfüllen.

Primelement: Ein Element p eines kommutativen Ringes R mit Eins heißt Primelement, falls p weder 0 noch eine Einheit ist und für alle $a, b \in R$ gilt: Teilt p das Produkt $a\dot{b}$, dann teilt p auch a oder b.

Primelement mit guter Reduktion: *Sei $p \in R$ ein Primelement und E_L eine elliptische Kurve über einem Zahlkörper. Dann heißt p Primelement mit guter Reduktion, wenn p die Diskriminante $\Delta(E) = -16(4A^3 + 27B^2)$ nicht teilt.*

Sei L ein Zahlkörper enthalten in $\mathbb{C}$ und E_L eine elliptische Kurve definiert über L. Sei außerdem R der Ganzheitsring von L. Sei $p \in R$ ein Primelement mit guter Reduktion für E_L. Sei k_p der entsprechende Restklassenkörper modulo p und E_{k_p} die reduzierte elliptische Kurve. Zuletzt seien $\delta : E_L(L) \to E_{k_p}(k_p)$ und $\delta : \mathbb{P}^1(L) \to \mathbb{P}(k_p)$ die kanonischen Surjektionen, hier genannt Reduktionsabbildungen, welche Elemente über dem Zahlkörper L auf die entsprechenden über den Restklassenkörper abbildet. Damit können wir das gewünschte elliptische Netz finden.

Satz 5.28 *Seien $P_1, \ldots, P_n \in E_L(L)$, sodass die Reduktionen modulo p der $\pm P_i$ alle unterschiedlich und nicht Null sind. Dann existiert für jedes $v \in \mathbb{Z}^n$ eine Funktion Ω_v, sodass folgendes Diagramm kommutiert:*

$$\begin{array}{ccc} E_L^n(L) & \xrightarrow{\Psi_v} & \mathbb{P}^1(L) \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ E_{k_p}^n(k_p) & \xrightarrow{\Omega_v} & \mathbb{P}^1(k_p) \end{array}$$

Abbildung 5.1: Kommutierendes Diagramm

Beweis Den Beweis findet man in [Sta08, Kapitel 6]. □

Das Theorem liefert uns die Definition für das gesuchte elliptische Netz.

Definition 5.29 *Sei $\phi : \mathbb{Z}^n \to E_{k_p}$ ein Homomorphismus, sodass die Bilder der Einheitsvektoren $\pm e_i$ unter ϕ alle verschieden und nicht Null sind. Sei Ω_v wie in Satz 5.28 definiert. Dann definiere $W_\Phi : \mathbb{Z}^n \to k_p$ durch*

$$W_\phi(v) = \Omega_v(\phi(e_1), \phi(e_2), \ldots, \phi(e_n)).$$

Satz 5.30 *Angenommen K ist entweder ein Zahlkörper oder endlicher Körper und $E(K)$ ein elliptische Kurve definiert über K. Sei $\phi : \mathbb{Z}^n \to E(K)$ ein Homomorphismus. Dann ist W_ϕ ein elliptisches Netz.*

Beweis Für den Beweis folgen wir [Sta07, Theorem 4].

Ist K ein Zahlkörper, so folgt die Behauptung aus Satz 5.26. Ist K hingegen ein endlicher Körper, so folgt die Behauptung aus Satz 5.28, da ein elliptisches Netz, welches mit einem Homomorphismus verknüpft wird, wieder ein elliptisches Netz ist. □

Angenommen wir wählen n Punkte P_i, wobei alle $\pm P_i$ unterschiedlich und nicht Null sind, so nennen wir für die Abbildung $\phi : \mathbb{Z}^n \to E(K)$, definiert durch $\phi(e_i) = P_i$, $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, K)$ das zu $E, P_1, \ldots, P_n$ assoziierte elliptische Netz. Wir müssen jetzt aufpassen, da wir elliptische Netze nicht als Abbildung der Punkte auf elliptischen Kurven sehen dürfen. Dafür folgen dem Beispiel in

[Akh12, Kapitel 4.3.1]. Es kann passieren, dass $W_v(\phi(e_1), \ldots, \phi(e_n)) \neq W_{v'}(\phi'(e_1), \ldots, \phi'(e_n))$, selbst wenn

$$\sum_{i=1}^{n} v_i \phi(e_i) = \sum_{i=1}^{n} v_i' \phi'(e_i).$$

Beispielsweise betrachten wir die elliptische Kurve $E : y^2 + y = x^3 + x^2 - 2x$ und die Punkte $P = (0, 0)$ und $Q = (1, 0)$. Wir entnehmen die Formeln zur Berechnung [Sta08, Proposition 6.1.2]. Dann können wir

$$\Omega_{(1,-1)}(2P, Q) = x_2 - x_1 = 1,$$
$$\Omega_{(2,1)}(P, -Q) = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2 = 2$$

berechnen. Ebenso sei W das elliptische Netz assoziiert mit einer elliptischen Kurve und Punkt $E(K), P$, wobei $P \in E[m]$. Dann können wir nicht davon ausgehen, dass $W(k) = W(m + k)$. Um diese Probleme anzugehen, führen wir den Begriff äquivalenter elliptischer Netze ein.

Dafür sei K ab jetzt immer ein endlicher Körper.

Definition 5.31 *Seien $W_1, W_2 \in \mathcal{EN}(A, K)$. Angenommen es existieren $\alpha, \beta \in K^*$ und $f : A \to \mathbb{Z}$ eine quadratische Form, sodass*

$$W_1(v) = \alpha \beta^{f(v)} W_2(v),$$

für alle $v \in A$, so sagen wir W_1 ist äquivalent zu W_2 und schreiben $W_1 \sim W_2$. Außerdem schreiben wir

$$\mathcal{EN}_0(A, K) := \mathcal{EN}(A, K)/\sim .$$

Satz 5.32 *Die Relation aus Definition 5.31 ist eine Äquivalenzrelation.*

Beweis Reflexivität: Seien $\alpha = \beta = 1$ und f eine beliebige quadratische Form. Dann gilt

$$W_1(v) = 1 \cdot 1^{f(v)} W_1(v) = \alpha \beta^{f(v)} W_1(v).$$

Symmetrie: Seien $\alpha, \beta \in K^*$ und f eine quadratische Form, sodass $W_1(v) \alpha \beta^{f(v)} W_2(v)$. Mit $\alpha' = \alpha^{-1}$ und $\beta' = \beta^{-1}$ gilt dann

$$W_2(v) = \alpha^{-1} \beta^{-f(v)} W_1(v) = \alpha' \beta'^{f(v)} W_1(v).$$

Transitivität: Seien $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K^*$ und f_1, f_2 quadratische Formen, sodass $W_1(v) = \alpha_1 \beta_1^{f_1(v)} W_2(v)$ und $W_2(v) = \alpha_2 \beta_2^{f_2(v)} W_3(v)$. Da K ein endlicher Körper ist, wird die multiplikative Gruppe K^* von einem Element $a \in K^*$ erzeugt. Es existieren also $n_1, n_2 \in \mathbb{N}$ mit $\beta_i = a^{n_i}, i = 1, 2$. Dann gilt mit $\alpha = \alpha_1 \cdot \alpha_2$, $\beta = a$ und $f(v) = n_1 f_1(v) + n_2 f_2(v)$

$$\begin{aligned} W_1(v) &= \alpha_1 \beta_1^{f_1(v)} W_2(v) = W_1(v) \\ &= \alpha_1 \beta_1^{f_1(v)} \alpha_2 \beta_2^{f_2(v)} W_3(v) \\ &= \alpha (a^{n_1})^{f_1(v)} (a^{n_2})^{f_2(v)} W_3(v) \\ &= \alpha a^{n_1 f_1(v) + n_2 f_2(v)} W_3(v) \\ &= \alpha \beta^{f(v)} W_3(v). \end{aligned}$$

□

Wir nehmen uns jetzt die Divisorengruppe $\mathrm{div}(E)$ zusammen mit der Summenabbildung

$$\mathrm{sum} : \mathrm{div}(E) \to E_K(K)$$

zur Hand. Sei $\hat{\Gamma} \approx \mathbb{Z}^n$ eine Untergruppe von $\mathrm{div}(E)$ und $\Gamma = \mathrm{sum}(\hat{\Gamma})$. Wir wählen einen surjektiven Homomorphismus $\phi : \mathbb{Z}^n \to \Gamma$, sodass ein Lift $\hat{\phi} : \mathbb{Z}^n \to \hat{\Gamma}$ existiert, welcher ein Isomorphismus ist. Solch ein Homomorphismus ϕ existiert. Beispielsweise sei $\{P_1, \dots P_m\}$ eine erzeugende Menge von Γ und $\phi(e_i) := P_i$. Dann gilt für $\hat{\phi}(e_i) := [P_i]$, dass $\hat{\phi} \circ \mathrm{sum} = \phi$ und $\hat{\phi}$ ist ein Isomorphismus. Damit definieren wir

$$V_\phi = W_\phi \circ \hat{\phi}^{-1}.$$

Nach einem kleinen Hilfslemma können wir zwei Eigenschaften dieses elliptischen Netzes zeigen.

Satz 5.33 *Sei W_ϕ ein elliptisches Netz und $T : \mathbb{Z}^n \to \mathbb{Z}^n$ ein Isomorphismus, so dass $W_{\phi\circ T}$ wohldefiniert ist. Das bedeutet, dass die Bilder von $\pm e_i$ alle unterschiedlich und nicht Null sind. Dann gilt*

$$W_{\phi\circ T} \sim W_\phi \circ T.$$

Beweis Wir folgen dem Beweis in [Akh12, Lemma 4.3.2].

Nach Definition gilt

$$W_\phi \circ T(v) = \Omega_{Tv}(\phi(e_1), \phi(e_2), \dots, \phi(e_n)).$$

Außerdem gilt

$$\begin{aligned} W_{\phi\circ T}(v) &= \Omega_v(\phi(Te_1), \dots, \phi(Te_n)) \\ &= \Omega_v(T^{\mathrm{Tr}}(\phi(e_1), \dots, \phi(e_n))^{\mathrm{Tr}}). \end{aligned}$$

Dadurch erhalten wir mit der Transformationsformel aus Satz 5.20

$$\frac{\Omega_{Tv}(\phi(e_1), \dots, \phi(e_n))}{\prod_{i=1}^n \Omega_{T(e_i)}(\phi(e_1), \dots, \phi(e_n))^{2v_i^2 - \sum_j v_i v_j} \prod_{1\le i<j\le n} \Omega_{T(e_i+e_j)}(\phi(e_1), \dots, \phi(e_n))^{v_i v_j}}.$$

Da T ein Isomorphismus ist, wissen wir, dass Ω_{Te_i} und $\Omega_{T(e_i+e_j)}$ nicht die Nullabbildung sind. Außerdem wissen wir, dass die $\phi(e_i)$ nicht Null und paarweise nicht negativ voneinander sind. Mit Definition 5.15 folgt dann, dass Ω_{Tv}, $\Omega_{T(e_i)}$ und $\Omega_{T(e_i+e_j)}$ nicht an Polstellen ausgewertet wird.

Um zu zeigen, dass $\Omega_{T(e_i)}(\phi(e_1), \dots, \phi(e_n)) \neq 0$ ist für alle $i = 1, \dots, n$, betrachten wir den Zähler von $\Psi_{T(e_i)}$. Dieser ist $\sigma(\sum_{j=1}^n T(e_i)_j \cdot \phi(e_j))$. Die weierstraßsche Sigma Funktion wird genau dann Null, wenn die Punkte sich zum Punkt im Unendlichen aufaddieren. Für das Argument gilt aber

$$\begin{aligned} \sum_{j=1}^n T(e_i)_j \cdot \phi(e_j) &= \phi(\sum_{j=1}^n T(e_i)_j \cdot e_j) \\ &= \phi(Te_i) \\ &= (\phi \circ T)(e_i). \end{aligned}$$

Für diese Funktion haben wir allerdings angenommen, dass das Bild der Basisvekoren ungleich des Punkts im Unendlichen ist. Die Behauptung überträgt sich mit den Bedingungen an Satz 5.28 auf $\Omega_{T(e_i)}$. Für die Faktoren $\Omega_{T(e_i+e_j)}$ erhält man mit gleicher Rechnung für das Argument im Zähler $(\phi \circ T)(e_i) + (\phi \circ T)(e_j)$. Nach Annahme sind die Bilder der Einheitsvektoren nicht negativ voneinander und die Summe somit ungleich des Punkts im Unendlichen.

Mithilfe der Eigenschaft, dass Summen quadratischer Formen wieder quadratische Formen sind, rechnet man nach, dass die Exponenten im Nenner eben solche sind. Wir können außerdem $\mathbb{P}^1(k_p)$ mit k_p identifizieren. Da dies ein endlicher Körper ist, wird die multiplikative Gruppe des Körpers von einem Element a erzeugt. Mit $\Omega_{T(e_i)}(\phi(e_1), \ldots, \phi(e_n)) = a^{n_i}$ und $\Omega_{T(e_i+e_j)}(\phi(e_1), \ldots, \phi(e_n)) = a^{n_{i,j}}$ für $n_i, n_{i,j} \in \mathbb{N}$ können wir den Nenner umschreiben zu

$$\prod_{i=1}^{n} (a^{n_i})^{2v_i^2 - \sum_j v_i v_j} \prod_{1 \le i < j \le n} (a^{n_{i,j}})^{v_i v_j} = a^{\sum_{i=1}^{n} \left(n_i \left(2v_i^2 - \sum_j v_i v_j\right)\right) + \sum_{1 \le i < j \le n} n_{i,j} v_i v_j}.$$

Dieser besteht nun aus konstanten Vielfachen und Summen von quadratischen Formen, also einer quadratischen Form. Das beweist den Satz. □

Satz 5.34 *$V_\phi \in \mathcal{EN}(\hat{\Gamma}, K)$ und die Äquivalenzklasse von V_ϕ ist unabhängig von der Wahl der Surjektion $\phi : \mathbb{Z}^n \to \Gamma$.*

Beweis Wir folgen dem Beweis in [Sta07, Theorem 5].

Durch die Linearität von $\hat{\phi}^{-1}$ ist sofort ersichtlich, dass V_ϕ ein elliptisches Netz ist.

Sei nun $\phi' : \mathbb{Z}^n \to \Gamma$ eine zweite surjektive Abbildung. Dann existiert ein Isomorphismus $T : \mathbb{Z}^n \to \mathbb{Z}^n$, sodass $\hat{\phi} \circ T = \hat{\phi}'$ und $\phi \circ T = \phi'$. Damit gilt

$$V_{\phi'} = W_{\phi'} \circ \hat{\phi}'^{-1} = W_{\phi \circ T} \circ T^{-1} \circ \hat{\phi}^{-1} \sim W_\phi \circ \hat{\phi}^{-1} = V_\phi \qquad \square$$

Definition 5.35 *Wir bezeichnen mit $\mathcal{W}_{\mathrm{Div}(E)}$ die Äquivalenzklasse $[V_\phi] \in \mathcal{EN}(\hat{\Gamma}, K)$.*

Satz 5.36 *Sei $W \in \mathcal{W}_{\mathrm{Div}(E)}$. Dann impliziert $W(p) = 0$, dass $\mathrm{sum}(p) = 0$.*

Beweis Ist $W(p) = 0$, so gilt nach Definition $\Omega_v(P) = 0$ für ein v und P, sodass $v_1 P_1 + \cdots + v_n P_n = \mathrm{sum}(p)$. Aber die Nullstellen P von Ψ_v sind genau die Punkte P, sodass $v_1 P_1 + \cdots + v_n P_n = 0$. □

Mithilfe dieser Netze können wir nun die Verknüpfung zum Tate-Lichtenbaum Pairing herstellen.

Satz 5.37 *Sei $m \in \mathbb{Z}$ positiv. Sei $E(K)$ eine elliptische Kurve über einem Körper, der die m-ten Einheitswurzeln enthält. Seien $Q \in E(K)$ und $P \in E[m]$. Wähle $S \in E(K)$, sodass $S \notin \{O, -Q\}$ und $p, q, s \in \mathrm{Div}(E)$, sodass $\mathrm{sum}(p) = P, \mathrm{sum}(q) = Q$ und $\mathrm{sum}(s) = S$. Sei $W \in \mathcal{W}_{\mathrm{Div}(E)}$. Dann ist*

$$T_m(P, Q) = \frac{W(s + mp + q)W(s)}{W(s + mp)W(s + q)}$$

eine wohldefinierte Funktion $T_m : E[m] \times E(K)/mE(K) \to K^*/(K^*)^m$. Außerdem gilt $T_m(P, Q) = \langle P, Q \rangle_m$.

Beweis Wir folgen dem Beweis in [Sta07, Theorem 6].

Nach Satz 5.36 und den Annahmen an S wird keiner der vier Terme von W Null werden.

Für die Wohldefiniertheit von T_m müssen wir zeigen, dass T_m unabhängig von der Wahl von des Repräsentanten aus $\mathcal{W}$ ist. Seien also $W_1, W_2 \in \mathcal{W}$. Dann ist $W_2(V) = \alpha\beta^{f(v)}W_1(v)$ für $\alpha, \beta \in K^*$ und eine quadratische Form f. Damit gilt

$$\begin{aligned}\frac{W_1(s+mp+q)W_1(s)W_2(s+mp)W_2(s+q)}{W_1(s+mp)W_1(s+q)W_2(s+mp+q)W_2(s)} &= \frac{\beta^{f(s+mp)+f(s+q)}}{\beta^{f(s+mp+q)+f(s)}} \\ &= \beta^{f(s+mp)+f(s+q)-f(s+mp+q)-f(s)} \\ &= \beta^{f(mp)+f(q)-f(mp+q)} \\ &= \beta^{m(f(p)+f(q)-f(p+q))}.\end{aligned}$$

Dies zeigt die Wohldefiniertheit.

Sei $\Gamma \subset E_K(K)$ die Untergruppe erzeugt von S, P und Q. Sei

$$f_P = \frac{\Omega_{1,0,0}(-S,P,Q)}{\Omega_{1,m,0}(-S,P,Q)}.$$

Betrachten wir f_P als eine Funktion in S, können wir mithilfe von Satz 5.19 ihren Divisor bestimmen:

$$\operatorname{div}(f_P) = -[mP] + (1-m)[O] + m[P] = m[P] - m[O].$$

Sei $D_Q = [-S] - [-S-Q]$. Diese beiden Divisoren sind genau die, die wir auch in der Definition des Tate-Lichtenbaum Pairings genutzt haben, weswegen $\langle P, Q\rangle_m = f_P(D_Q)$ gilt. Mithilfe mühsamen Nachrechnens mit Satz 5.20 erhalten wir

$$\begin{aligned}f_P(D_Q) &= \frac{\Omega_{1,0,0}(S,P,Q)\Omega_{1,m,0}(S+Q,P,Q)}{\Omega_{1,m,0}(S,P,Q)\Omega_{1,0,0}(S+Q,P,Q)} \\ &= \frac{\Omega_{1,0,0}(S,P,Q)\Omega_{1,m,1}(S,P,Q)}{\Omega_{1,m,0}(S,P,Q)\Omega_{1,0,1}(S,P,Q)}.\end{aligned}$$

Nachdem wir für die Abbildung $\phi : \mathbb{Z}^3 \to \Gamma$ freie Wahl haben, wählen wir sie, sodass $\phi(1,0,0) = S, \phi(0,1,0) = P$ und $\phi(0,0,1) = Q$. So haben wir $W_\phi(v) = \Omega_v(S,P,Q) \in \mathcal{EN}(\mathbb{Z}^3, K)$ und damit

$$\langle P, Q\rangle_m = f_P(D_Q) = \frac{V_\phi(s+mp+q)V_\phi(s)}{V_\phi(s+mp)V_\phi(s+q)} = T_m(P,Q). \qquad \square$$

Satz 5.38 *Sei $E(K)$ eine elliptische Kurve, $m \in \mathbb{Z}$ positiv, $P \in E[m]$ und $Q \in E(K)$. Wenn W das elliptische Netz assoziiert mit E, P ist, dann gilt*

$$\langle P, P\rangle_m = \frac{W_P(m+2)W_P(1)}{W_P(m+1)W_P(2)}.$$

Ist $W_{P,Q}$ das mit E, P, Q assoziierte Netz, so gilt

$$\langle P, Q\rangle_m = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)}$$

Beweis Wir folgen dem Beweis in [Sta07, Korollar 1].

Für die erste Formel wählen wir $p = q$ und $s = 2p$, womit wir

$$T_m(P,P) = \frac{W((m+2)p)W(p)}{W((m+1)p)W(2p)}$$

erhalten.

Für die zweite Formel wählen wir $s = p$ und erhalten

$$T_m(P,Q) = \frac{W((m+1)p+q)W(p)}{W((m+1)p)W(p+q)}.$$ □

Bemerkung 5.39 *Die eben hergeleiteten elliptischen Netze können auch dazu verwendet werden, das Weil-Pairing zu berechnen. Sei dafür $E(K)$ eine elliptische Kurve und $m \in \mathbb{Z}$ positiv, welche nicht von der Charakteristik von K geteilt wird. Dann gilt für zwei Punkte $P, Q \in E[m]$ und beliebiges $S \in E(K)$*

$$e_m(P,Q) = \frac{W(mp+q+s)W(p+s)W(mq+s)}{W(mp+s)W(q+s)W(p+mq+s)}.$$

Einen Beweis dafür findet man in [Sta08, Theorem 17.2.2].

5.2.1 Berechnung elliptischer Netze

Nachdem wir gesehen haben, wie wir ein elliptisches Netz nutzen können, um das Tate-Lichtenbaum Pairing zu berechnen, stellt sich noch die Frage, wie wir die Werte des Netzes berechnen können. Dafür stellt Stange einen Algorithmus vor.

Der folgende Algorithmus wird dafür genutzt werden, die Werte $W(m,0)$ und $W(m,1)$ eines elliptisches Netzes mit $W(1,0) = W(0,1) = 1$ zu berechnen. Dafür definieren wir einen Block zentriert um k als die Werte $W(k-3,0), \ldots, W(k+4,0), W(k-1,1), \ldots W(k+1,1)$. Für einen solchen Block definieren wir zwei Funktionen:

Double: Gegeben einen Block V zentriert um k, berechne den Block zentriert um $2k$.

DoubleAndAdd: Gegeben einen Block V zentriert um k, berechne den Block zentriert um $2k+1$.

Für $i = k-1, \ldots, k+3$ können wir folgende Formeln zur Berechnung der Funktionen nutzen:

$$\begin{aligned}
W(2i-1,0) &= W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3 \\
W(2i,0) &= \frac{W(i,0)W(i+2,0)W(i-1,0)^2 - W(i,0)W(i-2,0)W(i+1,0)^2}{W(2,0)} \\
W(2k-1,1) &= \frac{W(k+1,1)W(k-1,1)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k,1)^2}{W(1,1)} \\
W(2k,1) &= W(k-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2 \\
W(2k+1,1) &= \frac{W(k-1,1)W(k+1,1)W(k+1,0)^2 - W(k,0)W(k+2,0)W(k,1)^2}{W(-1,1)} \\
W(2k+2,1) &= \frac{W(k+1,0)W(k+3,0)W(k,1)^2 - W(k-1,1)W(k+1,1)W(k+2,0)^2}{W(2,-1)}
\end{aligned}$$

Algorithmus 5.2 Elliptic Net Algorithm

1: Setze $a = W(2,0), b = W(3,0), c = W(4,0), d = W(2,1), e = W(-1,1), f = W(2,-1), g = W(1,1)$ und $m = (d_k d_{k-1} \dots d_1)_2$ mit $d_k = 1$ die Binärdarstellung von m
2: $V \leftarrow [[-a, -1, 0, 1, a, b, c, a^3c - b^3]; [1, g, d]]$
3: **for** $i = k - 1$ to 1 **do**
4: **if** $d_i = 0$ **then**
5: $V \leftarrow \text{Double}(V)$
6: **else**
7: $V \leftarrow \text{DoubleAndAdd}(V)$
8: **end if**
9: **end forreturn** $V[0,3]$ und $V[1,1]$

Diese Formeln entstehen direkt aus der Definition elliptischer Netze.

Der Algorithmus, welcher $W(m,0)$ und $W(m,1)$ berechnet, ist in Algorithmus 5.2 dargestellt.

Um den Algorithmus nun für das Tate-Lichtenbaum Pairing anzuwenden, müssen wir die Startwerte berechnen. Sei dafür $E(F_q)$ eine elliptische Kurve und $P, Q \in E(F_q)$ mit $Q \neq \pm P$. Nun erhalten wir mithilfe der Funktion Ψ_v aus Definition 5.15:

$$
\begin{aligned}
W(1,0) &= 1 \\
W(2,0) &= 2y_1 \\
W(3,0) &= 3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2 \\
W(4,0) &= 4y_1(x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - 8B^2 - A^3) \\
W(0,1) &= W(1,1) = 1 \\
W(2,1) &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \\
W(-1,1) &= x_1 - x_2 \\
W(2,-1) &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2
\end{aligned}
$$

Für eine genaue Herleitung dieser Formeln siehe [Sta08, Proposition 6.1.2].

Bemerkung 5.40 *Beide Algorithmen, Millers und der Elliptic Net Algorithmus, basieren auf der gleichen Struktur. Beide sind ein „Double and Add“ Algorithmus, weswegen sie die gleiche Komplexität haben und linear in m sind. Dies ist leicht zu sehen, da die „Double“ und „DoubleAndAdd“ Funktionen jeweils eine konstante Anzahl an Rechenschritten haben. Die Laufzeitunterschiede liegen dann in den benötigten Rechenoperationen dieser Funktionen. Für eine genaue Analyse der benötigten Additionen, Multiplikationen und Invertierungen siehe [Sta07, Kapitel 5.2].*

6 Schluss

Nachdem wir in Kapitel 2 Pairings definiert haben, haben wir verschiedene Anwendungsfälle für diese gesehen. Dabei haben wir uns einen Schlüsselaustausch mit drei Parteien, welcher nur eine Runde benötigt, angeschaut, wie man mit Pairings ein Signaturschema kreieren kann und ein Verfahren zur Identity Based Encryption gesehen.

Um ein Pairing zu definieren, benötigten wir zunächst einige Theorie. Da unsere Pairings auf elliptischen Kurven leben, haben wir diesen das dritte Kapitel gewidmet. Dabei haben wir zunächst affine und projektive Kurven eingeführt und dabei insbesondere definiert, was es bedeutet, wenn diese singulär sind. Elliptische Kurven wurden dann als nicht singuläre projektive Kurven mit der Weierstraß Gleichung definiert. Auf diesen haben wir auf geometrische Weise eine Gruppenoperation hergeleitet.

Im vierten Kapitel haben wir uns der Theorie gewidmet, die speziell für die Definition unserer Pairings notwendig ist. Einen kurzen Blick haben wir dabei auf die Untergruppe, auf denen die Pairings definiert sind, die Torsionspunkte, geworfen. Danach folgte eine ausführliche Untersuchung von Funktionen auf elliptischen Kurven. Dabei haben wir Normalformen für sie gefunden und ihre Null- und Polstellen untersucht. Außerdem haben wir den Frobenius Endomorphismus eingeführt. Dieses Wissen haben wir in eine andere Sprache gebracht und die Divisoren eingeführt. Dabei haben wir gesehen, dass ein bestimmter Quotient dieser isomorph zu den Punkten der elliptischen Kurve ist. Somit konnten wir ab da mit Divisoren statt auf der elliptischen Kurve rechnen. Mit diesem Werkzeug war es uns möglich das Weil-Pairing zu definieren und zentrale Eigenschaften dessen zu beweisen. Ebenso sind wir mit dem Tate-Lichtenbaum-Pairing verfahren.

Das letzte Kapitel drehte sich um die Berechnung der beiden Pairings. Bei der Einführung dieser haben wir gesehen, dass diese nicht in einer geschlossenen Form gegeben sind, weswegen wir noch Algorithmen zur Berechnung brauchten. Dafür haben wir zuerst Millers Algorithmus vorgestellt, welcher Funktionen mit Divisor $n[P] - [nP] - (n-1)[P]$ berechnen kann und damit insbesondere das Weil-Pairing. Da das Tate-Lichtenbaum mithilfe des Weil-Pairings ausgedrückt werden kann, kann auch jenes durch Millers Algorithmus berechnet werden. Zuletzt haben wir noch einen zweiten Algorithmus zur Berechnung des Tate-Lichtenbaum Pairings vorgestellt, welcher auf elliptischen Netzen beruht. Dafür haben wir zunächst noch einige Vorarbeit in komplexer Funktionentheorie tätigen müssen.

In dieser Arbeit haben wir zwei Pairings auf elliptischen Kurven gesehen und wie diese berechnet werden können. Weiterführend kann man noch andere Pairings untersuchen und weitere Algorithmen zur Berechnung finden. Auch haben wir in dieser Arbeit nicht untersucht, welche Kurven sich besonders gut für die Berechnung von Pairings eignen. Mit weiteren Algorithmen könnte sich auch diese Klasse von Kurven vergrößern.

Literaturverzeichnis

[AE06] J. V. Armitage, W. F. Eberlein. *Elliptic functions*. 1. publ. Bd. 67. London Mathematical Society student texts. Cambridge: Cambridge Univ. Press, 2006. ISBN: 978-0521785631 (zitiert auf S. 69).

[Akh12] M. Akhim. „Elliptic nets and their use in Cryptography“. Masterarbeit. Katholieke Universiteit Leuven, 2012 (zitiert auf S. 73–75, 78, 79).

[BF01] D. Boneh, M. Franklin. „Identity-Based Encryption from the Weil Pairing“. In: *Advances in Cryptology — CRYPTO 2001*. Hrsg. von G. Goos, J. Hartmanis, J. van Leeuwen, J. Kilian. Bd. 2139. Lecture notes in computer science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, S. 213–229. ISBN: 978-3-540-42456-7 (zitiert auf S. 11).

[BLS01] D. Boneh, B. Lynn, H. Shacham. „Short Signatures from the Weil Pairing“. In: *Advances in Cryptology — ASIACRYPT 2001*. Hrsg. von C. Boyd. Bd. 2248. Springer eBook Collection Computer Science. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2001, S. 514–532. ISBN: 978-3-540-45682-7 (zitiert auf S. 10).

[BSS04] I. F. Blake, G. Seroussi, N. P. Smart, Hrsg. *Advances in elliptic curve cryptography*. Bd. 317. London Mathematical Society lecture note series. Cambridge: Cambridge University Press, 2004. ISBN: 978-0-521-60415-4 (zitiert auf S. 47, 57).

[DKR13] V. Diekert, M. Kufleitner, G. Rosenberger. *Diskrete algebraische Methoden: Arithmetik, Kryptographie, Automaten und Gruppen*. De Gruyter Studium. Berlin: De Gruyter, 2013. ISBN: 978-3-11-031260-7 (zitiert auf S. 48).

[Gal12] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge: Cambridge University Press, 2012. ISBN: 9781139012843 (zitiert auf S. 57).

[Har77] R. Hartshorne. *Algebraic Geometry*. Bd. 52. New York, NY: Springer New York, 1977. ISBN: 978-1-4419-2807-8 (zitiert auf S. 41).

[Jou04] A. Joux. „A One Round Protocol for Tripartite Diffie–Hellman“. In: *Journal of Cryptology* 17.4 (2004), S. 263–276. ISSN: 0933-2790 (zitiert auf S. 9, 10).

[Men] A. Menezes. *An Introduction to Pairing-Based Cryptography*. URL: https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf (zitiert auf S. 9, 11).

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. second edition. Bd. 106. Graduate texts in mathematics. Dordrecht u. a.: Springer, 2009. ISBN: 978-0-387-09493-9 (zitiert auf S. 21, 23, 48, 50, 64).

[Sta07] K. E. Stange. „The Tate Pairing Via Elliptic Nets“. In: *Pairing-based cryptography - Pairing 2007*. Bd. 4575. Lecture notes in computer science. Berlin: Springer, 2007, S. 329–348. ISBN: 978-3-540-73489-5 (zitiert auf S. 7, 67, 72, 77, 80–83).

[Sta08] K. E. Stange. „Elliptic Nets and Elliptic Curves“. PhD thesis. Providence, Rhode Island: Brown University, 2008 (zitiert auf S. 77, 78, 82, 83).

[Wal10] L. A. Wallenborn. „Elliptic Curves, Divisors and Lines“. 2010. URL: https://www.wallenborn.net/download/Talk-Algebraic-Methods-in-Computation-Complexity-Elliptic-Curves-Divisors-and-Lines.pdf (zitiert auf S. 27, 29, 31–36).

[Was08] L. C. Washington. *Elliptic curves: Number theory and cryptography*. 2. ed. Bd. 50. A Chapman & Hall book. Boca Raton, Fla.: Chapman & Hall/CRC, 2008. ISBN: 9781420071467 (zitiert auf S. 23, 26, 37, 39–43, 46, 47, 50, 53, 55, 57–60, 68, 69).

[Wer02] A. Werner. *Elliptische Kurven in der Kryptographie*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. ISBN: 978-3-540-42518-2 (zitiert auf S. 12, 14, 16–21, 23).

Alle URLs wurden zuletzt am 23. 10. 2022 geprüft.

Erklärung

Ich versichere, diese Arbeit selbstständig verfasst zu haben. Ich habe keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet. Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens. Ich habe diese Arbeit bisher weder teilweise noch vollständig veröffentlicht. Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Ort, Datum, Unterschrift