Die Weil-Paarung auf elliptischen Kurven und ihre Anwendung in der Kryptographie

Diplomarbeit im Fachbereich Mathematik

der Universität Bremen

vorgelegt von

Tim Nikolayzik

August 2007

1. Gutachter Prof. Dr. Michael Hortmann
2. Gutachter Prof. Dr. Jens Gamst

Inhaltsverzeichnis

Einleitung

Elliptische Kurven spielen eine wichtige Rolle in der Zahlentheorie und Kryptographie. Mitte der 1980er Jahre machten Koblitz und Miller den Vorschlag elliptische Kurven in der Kryptographie einzusetzen. Inzwischen hat sich die Kryptographie mit elliptischen Kurven etabliert. Die Sicherheit beruht dabei auf der Schwierigkeit des diskreten Logarithmus-Problems (siehe Kapitel 4). Viele Verfahren, die zum Lösen des diskreten Logarithmus-Problems in endlichen Körpern entwickelt wurden, sind nicht auf elliptische Kurven übertragbar. Daraus ergibt sich der Vorteil von Kryptosystemen mit elliptischen Kurven, bei gleicher Sicherheit, Schlüssel von deutlich geringerer Länge als bei anderen Verfahren nehmen zu können. Ein 163 Bit ECC (Elliptic Curve Cryptosystem) Schlüssel besitzt dieselbe Sicherheit wie ein 1024 Bit RSA-Schlüssel [24]. Für weitere Vergleiche siehe zum Beispiel [8]. Damit ist es also möglich, Rechenzeit und Speicherplatz zu sparen. Die Kryptographie mit elliptischen Kurven ist also besonders dort interessant, wo man wenig Rechenleistung und Speicherplatz zur Verfügung hat, zum Beispiel auf Chipkarten. Öffentlich gebrochen wurde bisher nur das diskrete Logarithmus-Problem für elliptische Kurven für 109 bit Schlüssellänge [23]. Um diesen Schlüssel zu berechnen, haben 10000 Computer 549 Tage gebraucht. Das Problem einen 163 Bit Schlüssel zu berechnen ist laut Vanstone [23] etwa um den Faktor 10^8 aufwändiger als das gelöste Problem. Nach Lenstra und Verheul [20] sind die heute standardmäßig genutzten 163 Bit ECC-Schlüssel sicher bis mindestens 2020.

Elliptische Kurven werden auch in anderen Bereichen der Kryptographie eingesetzt, zum Beispiel bei Primzahltests oder zur Faktorisierung ganzer Zahlen. Da die Kryptographie mit elliptischen Kurven viele Vorteile bietet, ist man natürlich auch an eventuellen Angriffspunkten interessiert, insbesondere bei der Lösung des diskreten Logarithmus-Problems. In diesem Fall möchte man also Angriffe auf das diskrete Logarithmus-Problem über endlichen Körpern auf das diskrete Logarithmus-Problem auf elliptischen Kurven übertragen. An diesem Punkt setzt diese Arbeit an. Als Motivation dient ein Artikel von Menezes, Vanstone und Okamoto. Diese zeigten 1991 in [22], dass mit Hilfe der Weil-Paarung das diskrete Logarithmus-Problem auf elliptischen Kurven in ein diskretes Logarithmus-Problem in einem endlichen Körper zurückgeführt werden kann. Da dieses Problem schon sehr ausführlich untersucht wurde, gibt es viele Verfahren die man nun an dieser Stelle ansetzen kann. Hierbei hängt es von der Größe und Charakteristik des endlichen Körpers ab, in welcher Zeit das diskrete Logarithmus-Problem lösbar ist.

In Kapitel 1 werden wir zunächst einige Grundlagen aus der kommutativen Algebra behandeln. Im weiteren Verlauf des Kapitels werden Grundbegriffe der algebraischen

Geometrie eingeführt. Diese werden wir benutzen, um einige Sätze über Varietäten darzustellen. Diese Sätze legen den theoretischen Grundstein für das Kapitel 2. In ihm werden wir zuerst den Zusammenhang zwischen projektiven Varietäten und elliptischen Kurven herstellen. Auf der Ebene der elliptischen Kurven werden dann einige Sätze behandelt, die es ermöglichen, den Hauptsatz des Kapitels, Theorem 2.2.16, zu beweisen. Mit Hilfe dieses Theorems werden wir in Kapitel 3 die Weil-Paarung definieren. Weiter werden wir ihre Eigenschaften vorstellen und ein Verfahren zur Berechnung präsentieren. In Kapitel 4 wird zuerst ein Kryptosystem mit elliptischen Kurven vorgestellt. Mit dem Verfahren aus [22] ist es dann unter bestimmen Umständen möglich, ein solches Krpytosystem anzugreifen. Zum Schluss werden wir noch einige weitere Anwendungen der Weil-Paarung in der Kryptographie behandeln.

1. Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen für die weiteren Kapitel gelegt. Zuerst werden wir ein paar Ergebnisse aus der kommutativen Algebra kennen lernen, die wir brauchen, um uns einige Grundbegriffe der algebraischen Geometrie anzueignen.

1.1. Kommutative Algebra

Wir werden jetzt einige Ergebnisse der kommutativen Algebra zusammenfassen. Zuerst wird ein Einblick in die Modultheorie gegeben. Dieser orientiert sich an [19]. Dann werden wir uns mit Bewertungen und Bewertungsringen auseinander setzen, hierbei orientieren wir uns an [3].

Im Folgenden sei R ein kommutativer Ring mit Eins.

Lemma 1.1.1. *Sei R Integritätsring mit Quotientenkörper K. Dann gilt*

$$\bigcap_{P \text{ max. Ideal}} R_P = R.$$

Beweis. Wir wollen R und R_P als Unterringe des Quotientenkörpers K auffassen. Sei $r/s \in \cap_P R_P$, dabei durchlaufe im Folgenden P immer alle maximalen Ideale. Wir definieren die Menge

$$I := \{a \in R : ra \in sR\}.$$

Man kann leicht nachprüfen, dass I ein Ideal in R ist. Wir wollen nun annehmen, dass es ein maximales Ideal P gibt mit $I \subseteq P$. Da $r/s \in \cap_P R_P$, existiert $r' \in R$ und $s' \notin P$ mit

$$rs' = r's.$$

Nach der Definition von I folgt somit, dass $s' \in I$. Da wir $I \subseteq P$ angenommen hatten, folgt $s' \in P$, was ein Widerspruch ist. Damit ist $I = (1)$ und somit können wir $r \in sR$ folgern und es gilt $r/s \in R$. □

Das Jacobson-Radikal $J(R)$ des Ringes R ist definiert als der Durchschnitt aller maximalen Ideale in R. Es gilt die folgende Charakterisierung:

Lemma 1.1.2. *Ist R ein Ring, so gilt $x \in J(R)$ genau dann, wenn $1 - xy$ für alle $y \in R$ eine Einheit in R ist.*

Beweis. Sei $x \in J(R)$. Angenommen es existiert ein $y \in R$, so dass $1-xy$ keine Einheit in R ist. Dann existiert ein maximales Ideal $\mathfrak{m}$ in dem $1-xy$ enthalten ist. Da $x \in J(R) \subseteq \mathfrak{m}$ gilt, ist $yx \in \mathfrak{m}$ und damit folgt insgesamt $1 \in \mathfrak{m}$, was ein Widerspruch ist.

Sei nun $x \in R$ mit der Eigenschaft, dass $1 - xy$ für alle $y \in R$ eine Einheit in R ist. Wir nehmen an, dass $x \notin J(R)$ gilt. Es existiert also ein maximales Ideal $\mathfrak{m}$ mit $x \notin \mathfrak{m}$. Dann wird R von x und $\mathfrak{m}$ erzeugt und daher gibt es Elemente $u \in \mathfrak{m}$ und $y \in R$ mit $u+xy = 1$. Damit ist $1-xy \in \mathfrak{m}$ und somit ist $1-xy$ keine Einheit, was ein Widerspruch zu unserer Voraussetzung ist. □

Bevor wir nun das nächste Ergebnis formulieren, wollen wir an die Definition eines Moduls erinnern. Ein R-Modul ist eine abelsche Gruppe M, zusammen mit einer Multiplikation

$$R \times M \to M,\ (a, x) \mapsto a \cdot x,$$

mit den Eigenschaften

$$\begin{aligned} a \cdot (x + a) &= a \cdot x + a \cdot y, \\ (a + b) \cdot x &= a \cdot x + b \cdot x, \\ a \cdot (b \cdot x) &= (ab) \cdot x, \\ 1 \cdot x &= x, \end{aligned}$$

für $a, b \in R,\ x, y \in M$. Eine Familie $(x_i)_{i \in I}$ von Elementen eines R-Moduls M heißt ein Erzeugendensystem von M, wenn $M = \sum_{i \in I} Rx_i$ gilt. Besitzt M ein endliches Erzeugendensystem, so heißt M endlich erzeugt. Ein Untermodul N von M ist eine additive Gruppe mit der Eigenschaft, dass $RN \subseteq N$ gilt. Es ist klar, dass N auch wieder ein R-Modul ist. Sind M und M' zwei R-Module, so heißt eine Abbildung

$$f : M \to M'$$

Modulhomomorphismus, wenn f ein Homomorphismus der additiven Gruppen ist und

$$f(rm) = rf(m),\ r \in R,\ m \in M$$

gilt. Sei zum Beispiel M ein R-Modul und N ein Untermodul von M, so ist M/N wieder ein R-Modul und die kanonische Abbildung $f : M \to M/N$ ein Modulhomomorphismus. Ist $f : M \to M'$ ein Modulhomomorphismus und seien N, N' Untermodule von M beziehungsweise M' so kann man leicht nachprüfen, dass $ker(f)$ sowie $f(N)$ und $f^{-1}(N')$ Untermodule sind. Wir können nun das folgende Lemma formulieren:

Lemma 1.1.3. *(Lemma von Nakayama)*
Sei M ein endlich erzeugter R-Modul und $\mathfrak{a}$ ein Ideal von R, das im Jacobson-Radikal $J(R)$ von R enthalten ist. Gilt $\mathfrak{a}M = M$, so folgt $M = 0$.

Beweis. Wir nehmen an, dass $M \neq 0$ gilt. Sei $u_1, \ldots, u_n$ ein minimales Erzeugendensystem von M. Es ist $u_n \in \mathfrak{a}M = M$. Dann existieren $a_i \in \mathfrak{a}, i = 1 \ldots n$, mit

$$u_n = a_1u_1 + \ldots + a_nu_n.$$

Damit erhalten wir

$$(1 - a_n)u_n = a_1u_1 + \ldots + a_{n-1}u_{n-1}.$$

Da $a_n \in J(R)$ folgt mit $y = 1$ aus Lemma 1.1.2, dass $1 - a_n$ eine Einheit in R ist. Daher liegt u_n in dem von $u_1, \ldots, u_{n-1}$ erzeugten Untermodul von M. Dies ist jetzt aber ein Widerspruch dazu, dass $u_1, \ldots, u_n$ ein minimales Erzeugendensystem von M war. □

Wir wollen zeigen, haben wir einen noetherschen Ring R und ist M ein endlich erzeugter R-Modul, so sind alle Untermodule von M endlich erzeugt. Wird die Voraussetzung, dass R noethersch ist, fallen gelassen, so gibt es Gegenbeispiele.

Beispiel 1.1.4. Sei $R = \mathbb{Z}[X]$. Wir setzen dann

$$M := \left\{ \sum a_i X^i : 2|a_i,\ i > 0 \right\} \text{ und } M' := \left\{ \sum a_i X^i : 2|a_i,\ i \geq 0 \right\}.$$

M ist nun ein endlich erzeugter M-Modul, da $\{1\}$ eine Basis von M ist. M' ist zwar ein Untermodul von M, aber M' ist nicht endlich erzeugt.

Um jetzt diese Aussage zu beweisen, müssen wir wissen, wann ein Modul noethersch ist.

Satz 1.1.5. *Sei M ein R-Modul. Dann heißt M noethersch, wenn M eine der drei folgenden Bedingungen erfüllt:*

i. Jedes Untermodul von M ist endlich erzeugt.

ii. Jede aufsteigende Folge von Untermodulen von M

$$M_1 \subset M_2 \subset \ldots$$

wird stationär.

iii. Jede nichtleere Menge S von Untermodulen von M hat ein maximales Element, das heißt es existiert ein Untermodul M_0 so, dass für jedes Element $N \in S$ mit $N \supseteq M_0$ folgt $N = M_0$.

Beweis. Zu zeigen ist, dass die drei Bedingungen äquivalent sind.

i.⇒ii. : Sei

$$M_1 \subset M_2 \subset \ldots$$

eine beliebige aufsteigende Folge von Untermodulen von M. Wir setzen $N := \cup_i M_i$. N ist somit ein Untermodul von M und daher endlich erzeugt. Seien $x_1, \ldots, x_r$ die Erzeuger von N. Dann liegen alle x_i in einem M_j und es existiert ein $j_0 \in \mathbb{N}$ mit $x_1, \ldots, x_r \in M_{j_0}$. Es folgt

$$\langle x_1, \ldots, x_r \rangle \subseteq M_{j_0} \subseteq N = \langle x_1, \ldots, x_r \rangle.$$

Daher wird die aufsteigende Folge von Untermodulen stationär.

ii.⇒iii. : Sei S eine beliebige Menge von Untermodulen von M und $N \in S$ beliebig. Ist N maximales Element so ist die Behauptung bewiesen. Ist N hingegen nicht maximal, so gibt es ein Untermodul $N_1 \in S$, so dass $N \subset N_1$ gilt. Ist nun N_1 nicht maximal, so existiert wieder ein Untermodul $N_2 \in S$, so dass $N_1 \subset N_2$ gilt. Würde S kein maximales Element besitzen, so könnten wir auf diese Weise eine aufsteigende Folge von Untermodulen konstruieren, deren Länge nicht endlich wäre. Dies ist aber ein Widerspruch zur Voraussetzung.

iii.⇒i. : Sei N ein beliebiges Untermodul von M und $a_0 \in N$. Gilt $\langle a_0 \rangle \neq N$, so existiert $a_1 \in N$ mit $a_1 \notin \langle a_0 \rangle$. Auf diese Weise erhalten wir eine aufsteigende Folge von Untermodulen

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \dots .$$

Diese Menge von Untermodulen hat ein maximales Element, gegeben durch $\langle a_1, \dots, a_r \rangle$. Es folgt sofort, dass $\langle a_1, \dots, a_r \rangle = N$ gilt. Somit ist N endlich erzeugt. □

Satz 1.1.6. *Sei M ein R-Modul und N ein Untermodul von M. Sind N und M/N noethersch, so ist auch M noethersch.*

Beweis. Für Untermodule L von M definieren wir die Abbildung

$$L \mapsto (L \cap N, (L + N)/N),$$

dabei sind $L \cap N$ und $(L + N)/N$ wieder Module. Sind E, F zwei Untermodule von M mit $E \subseteq F$, für die

$$(E \cap N, (E + N)/N) = (F \cap N, (F + N)/N)$$

gilt, so folgt bereits $E = F$. Sei $x \in F$. Da $(E + N)/N = (F + N)/N$ gilt, existieren $u, v \in N$ und $y \in E$ mit $y + u = x + v$. Damit erhalten wir

$$x - y = u - v \in F \cap N = E \cap N.$$

Da $y \in E$ folgt, dass $x \in E$ gilt und somit insgesamt $E = F$. Sei jetzt

$$E_1 \subset E_2 \subset \dots$$

eine beliebige aufsteigende Folge von Untermodulen in M. Dann bilden die $E_i \cap N$ und $(E_i + N)/N$ eine aufsteigende Folge von Untermodulen von N beziehungsweise M/N. Diese Folgen werden aber stationär, da N und M/N noethersch sind. Also existiert ein $j \in \mathbb{N}$ mit

$$E_i \cap N = E_j \cap N \text{ und } (E_i + N)/N = (E_j + N)/N,\ i \geq j.$$

Mit Hilfe unser vorherigen Überlegung folgt $E_i = E_j,\ i \geq j$ und somit ist M noethersch. □

Aus dem Satz folgt:

Corollar 1.1.7. *Sei M ein R-Modul und N, N' Untermodule. Sind N und N' noethersch und gilt $M = N+N'$, so ist auch M noethersch. Weiter gilt dann, dass die endliche direkte Summe von noetherschen Modulen wieder noethersch ist.*

Beweis. Da $(N \times N')/N \cong N'$ ist und nach Voraussetzung N und N' noethersch sind, folgt nach Satz 1.1.6, dass auch $N \times N'$ noethersch ist. Wir definieren einen surjektiven Modulhomomorphismus durch

$$\begin{aligned} f : N \times N' &\to M \\ (x, x') &\mapsto x + x'. \end{aligned}$$

Sei nun

$$M_1 \subset M_2 \subset \dots$$

eine beliebige aufsteigende Folge von Untermodulen. Wir setzen $N_i := f^{-1}(M_i)$. Die N_i sind Untermodule von $N \times N'$. Da f surjektiv ist, sind diese nicht leer und es gilt

$$N_1 \subset N_2 \subset \dots \ .$$

Da $N \times N'$ noethersch ist, wird diese aufsteigende Folge stationär, das heißt es existiert ein N_j mit $N_i = N_j,\ i \geq j$. Da $f(N_i) = M_i$ gilt, folgt $M_i = M_j,\ i \geq j$ und somit ist M noethersch. Per Induktion folgt nun, dass das endliche Produkt noetherscher Module und die endliche Summe noetherscher Module wieder noethersch ist. □

Jetzt ist es möglich, unsere ursprüngliche Aussage zu beweisen.

Satz 1.1.8. *Ist R ein noetherscher Ring und M ein endlich erzeugtes R-Modul, dann ist M noethersch.*

Beweis. Seien $x_1, \dots, x_n$ die Erzeuger von M. Wir definieren einen surjektiven Modulhomomorphismus, vom n-fachen Produkt des Ringes R nach M, durch

$$f : R \times R \times \dots \times R \to M,\ (a_1, \dots, a_n) \mapsto a_1x_1 + \dots a_nx_n.$$

Nach Corollar 1.1.7 ist $R \times R \times \dots \times R$ noethersch und wie im Beweis vom Corollar 1.1.7 folgt, mit Hilfe des Modulhomomorphismus f, dass M noethersch ist. □

In der Arbeit werden keine weiteren Ergebnisse aus der Modultheorie benötigt und wir wenden uns daher jetzt den Bewertungen zu.

Definition 1.1.9. Sei K ein Körper und G eine total geordnete abelsche Gruppe bezüglich der Addition. Eine Abbildung $\nu : K - \{0\} \to G$ heißt Bewertung von K mit Werten

in G, wenn für alle $x, y \in K,\ x, y \neq 0$ gilt:

$$\nu(xy) = \nu(x) + \nu(y),$$
$$\nu(x+y) \geq \min\{\nu(x), \nu(y)\},\ x+y \neq 0.$$

Ist G eine total geordnete Gruppe bezüglich der Multiplikation, so ändert sich die erste Bedingung zu

$$\nu(xy) = \nu(x)\nu(y).$$

Wir können in der Definition einer Bewertung auch den Körper K durch einen Integritätsring R ersetzen, denn ist $\nu : R - \{0\} \to G$ eine Bewertung auf R, so erhalten wir durch $\nu'(r/s) := \nu(r) - \nu(s)$ eine Bewertung auf dem Quotientenkörper von R.

Ist $\nu : K - \{0\} \to G$ eine Bewertung eines Körpers K, dann ist die Menge

$$R_\nu := \{x \in K - \{0\} |\ \nu(x) \geq 0\} \cup \{0\}$$

ein Ring und wird der Ring der Bewertung von ν genannt.

Proposition 1.1.10. *Sei K ein Körper. Ein Unterring $R \subseteq K$ist genau dann der Ring einer Bewertung auf K, wenn für alle $x \in K - \{0\}$ entweder $x \in R$ oder $x^{-1} \in R$ gilt.*

Beweis. Sei $\nu : K^* = K - \{0\} \to G$ eine Bewertung, so dass $R = R_\nu$ gilt. Da G total geordnet ist, gilt für alle $x \in K^*$ entweder $\nu(x) \geq 0$ oder $\nu(x) \leq 0$. Aus letzterem ergibt sich $\nu(x^{-1}) = -\nu(x) \geq 0$. Damit ist $x \in R_\nu$ oder $x^{-1} \in R_\nu$.

Für die Rückrichtung konstruieren wir eine Bewertung und zeigen, dass R der Ring dieser Bewertung ist. Sei $\nu : K^* \to K^*/R^*$ der kanonische Homomorphismus. Zuerst brauchen wir eine totale Ordnung auf K^*/R^*, dazu definieren wir für $xR^*, yR^* \in K^*/R^*$

$$xR^* \leq yR^* :\iff yx^{-1} \in R.$$

Die Wohldefiniertheit der Ordnung ergibt sich, da $xR^* = yR^*$ äquivalent zu $xy^{-1} \in R^*$ ist. Für xR^*, yR^*, zR^* mit $xR^* \leq yR^*$ und $yR^* \leq zR^*$ gilt $zx^{-1} = zy^{-1}yx^{-1} \in R$ und damit ist $xR^* \leq zR^*$. Ist $xR^* \leq yR^*$ und $yR^* \leq xR^*$ für $xR^*, yR^* \in K^*/R^*$, so folgt $yx^{-1} \in R^*$ und damit erhalten wir $xR^* = yR^*$. Unsere Ordnung ist also reflexiv, antisymmetrisch und transitiv. Nach Voraussetzung gilt, aus $x, y \in K^*$ mit $x \neq y$ folgt $yx^{-1} \in R$ oder $xy^{-1} \in R$. Weiter gilt für $xR^*, yR^*, zR^* \in K^*/R^*$ mit $xR^* \leq yR^*$, dass $(zy)(zx)^{-1} = yx^{-1} \in R$ ist, das heißt $zxR^* \leq zyR^*$. Damit ist $(K^*/R^*, \cdot, \leq)$ eine total geordnete Gruppe. Es bleibt also zu zeigen, dass $\nu : K^* \to K^*/R^*,\ x \mapsto xR^*$ eine Bewertung ist und R der Ring der Bewertung. Im Folgenden sei $x, y \in K^*$. Wir sehen, dass

$$\nu(xy) = xyR^* = xR^*yR^* = \nu(x)\nu(y)$$

gilt. Ohne Einschränkung wollen wir $xR^* \leq yR^*$ annehmen. Dann gilt $yx^{-1} \in R$ und damit ist $1 + yx^{-1} = (x+y)x^{-1} \in R$. Nach Definition der Ordnung erhalten wir

$$\min\{\nu(x), \nu(y)\} = \nu(x) = xR^* \leq (x+y)R^* = \nu(x+y).$$

Damit ist also ν eine Bewertung von K^* mit Werten in K^*/R^*. Weiter gilt genau dann $\nu(x) = 0$, wenn $x \in R^*$ ist. Ebenso gilt genau dann $\nu(x) \geq 1$, wenn $x \in R$. Also ist $R = R_\nu$ und damit ist die Behauptung gezeigt. □

Mit dieser Proposition können wir nun den Begriff Bewertungsring definieren.

Definition 1.1.11. Sei K ein Körper und $R \subseteq K$ ein Unterring. R heißt Bewertungsring von K, wenn für alle $x \in K - \{0\}$ folgt, dass $x \in R$ oder $x^{-1} \in R$ gilt. Ein Integritätsring R heißt Bewertungsring, wenn R Bewertungsring seines Quotientenkörpers ist.

Wir werden uns nur für Bewertungen mit Werten in $\mathbb{Z}$ interessieren. Diese Bewertungen heißen diskrete Bewertungen.

Definition 1.1.12. Ein Integritätsring R heißt diskreter Bewertungsring, wenn es eine diskrete Bewertung ν im Quotientenkörper von R gibt, so dass R ein Bewertungsring von ν ist.

Proposition 1.1.13. *Sei R ein noetherscher, lokaler Integritätsring mit maximalem Ideal $\mathfrak{m}$. Gilt $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$, so ist R ein diskreter Bewertungsring.*

Beweis. Sei $p \in \mathfrak{m} - \mathfrak{m}^2$ beliebig. Da $p \neq 0$ in $\mathfrak{m}/\mathfrak{m}^2$ und $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$ ist, existiert für $x \in \mathfrak{m}/\mathfrak{m}^2$ ein $r \in R$ mit $x = \overline{rp}$. Daher gilt $(p) + \mathfrak{m}^2 = \mathfrak{m}$. Es folgt

$$\mathfrak{m}\left(\mathfrak{m}/(p)\right) = \left(\mathfrak{m}^2 + (p)\right)/(p) = \mathfrak{m}/(p).$$

Mit Lemma 1.1.3 ergibt sich, dass $\mathfrak{m} = (p)$ ist. Sei nun $I \subset R$ ein beliebiges von 0 verschiedenes Ideal. Es existiert dann ein maximales $q \in \mathbb{N}_0$, so dass $I \subseteq \mathfrak{m}^q$ gilt. Wir wählen nun $r \in I - \mathfrak{m}^{q+1}$, dann existiert $t \in R - \mathfrak{m}$, das heißt $t \in R^*$, mit der Eigenschaft, dass

$$r = p^q t$$

gilt. Es ergibt sich also

$$I \supseteq (r) = (p^q) = \mathfrak{m}^q \supseteq I$$

und damit $I = (p^q)$. Wir haben jetzt gezeigt, dass für alle $x \in R - \{0\}$ ein eindeutiges $k \in \mathbb{N}_0$ existiert, so dass

$$(x) = (p^k)$$

gilt. Wir definieren dann $\nu(x) := k$ und können ν durch $\nu(ab^{-1}) := \nu(a) - \nu(b)$ auf dem Quotientenkörper von R fortsetzen. ν ist eine diskrete Bewertung und weiter ist R der Bewertungsring von ν, denn für $x \in R - \{0\}$ ist $\nu(x) \geq 0$ und ebenso ergibt sich aus $\nu(x) \geq 0$, dass $x \in R - \{0\}$ ist. □

1.2. Algebraische Geometrie

Wir wollen in diesem Abschnitt die Grundlagen der Algebraischen Geometrie behandeln. Dabei werden wir uns mit affinen und projektiven Varietäten beschäftigen. Im letzten Teil des Abschnittes werden wir ein paar grundlegende Ergebnisse formulieren und beweisen. Als Vorlage dieses Abschnittes dient das Buch von Hartshorne [11].

1.2.1. Affine Varietäten

Im weiteren Verlauf sei K ein fester, algebraisch abgeschlossener Körper. Die folgende Theorie kann auch an einem nicht algebraisch abgeschlossen Körper K' durchgeführt werden, wenn man K durch einen festen algebraisch Abschluss $\overline{K'}$ von K' ersetzt. Gibt es für diesen Fall Besonderheiten, wird dies an den entsprechenden Stellen bemerkt.

Definition 1.2.1. Wir definieren den n-dimensionalen affinen Raum $\mathbb{A}^n$ durch

$$\mathbb{A}^n := \mathbb{A}^n(K) := \{P = (x_1, \ldots, x_n) : x_i \in K,\ i = 1, \ldots n\}.$$

Bemerkung 1.2.2. Ist K' nicht algebraisch abgeschlossen, so ist die Menge der K'-rationalen Punkte $\mathbb{A}^n(K')$ in $\mathbb{A}^n = \mathbb{A}^n(\overline{K'})$ definiert durch

$$\mathbb{A}^n(K') := \left\{P = (x_1, \ldots, x_n) : x_i \in K',\ i = 1, \ldots n\right\}.$$

Sei $T \subseteq K[X_1, \ldots, X_n]$ eine beliebige Teilmenge, dann definieren wir die Nullstellenmenge $Z(T)$ von T als die Menge aller gemeinsamen Nullstellen von Elementen aus T, das heißt

$$Z(T) := \{P \in \mathbb{A}^n : f(P) = \text{ für alle } f \in T\}.$$

Ist $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ das von T erzeugte Ideal, so gilt $Z(\mathfrak{a}) = Z(T)$. Da $K[X_1, \ldots, X_n]$ ein noetherscher Ring ist, hat $\mathfrak{a}$ eine endliche Menge von Erzeugern $f_1, \ldots, f_r$. Also ist $Z(T)$ gleich der Menge der gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_r$.

Definition 1.2.3. Eine Menge $V \subseteq \mathbb{A}^n$ heißt algebraische Menge, wenn es eine Menge $T \subseteq K[X_1, \ldots, X_n]$ gibt mit $V = Z(T)$.

Man kann nun zeigen, dass die Vereinigung von zwei algebraischen Mengen und der Schnitt einer Familie algebraischer Mengen wieder eine algebraische Menge ist. Ebenso sind die leere Menge und der ganze Raum algebraische Mengen. Damit können wir uns nun auf $\mathbb{A}^n$ eine Topologie, die Zariski-Topologie, definieren, indem wir als abgeschlossene Mengen die algebraischen Mengen nehmen.

Beispiel 1.2.4. Nehmen wir uns als Beispiel den eindimensionalen affinen Raum $\mathbb{A}^1$ mit der zugehörigen Zariski-Topologie. Ist $V \subset \mathbb{A}^1$ mit $V \neq \emptyset$ eine algebraische Menge, so existiert ein Ideal $\mathfrak{a} \subseteq K[X]$, so dass $V = Z(\mathfrak{a})$ gilt. Da jedes Ideal in $K[X]$ ein Hauptideal

ist, existiert $f \in K[X]$, $f \neq 0$ mit $V = Z(f)$. Da K algebraisch abgeschlossen ist, f zerfällt vollständig, somit existieren also $c, a_1, \ldots, a_n \in K$ mit

$$f = c(X - a_1) \cdot \ldots \cdot (X - a_n).$$

Damit gilt $V = \{a_1, \ldots, a_n\}$. Somit sind die algebraischen Mengen in $\mathbb{A}^1$ gerade die endlichen Mengen, inklusive der leeren Menge und $\mathbb{A}^1$. Die offenen Mengen sind also die leere Menge, $\mathbb{A}^1$ und die Komplemente von endlichen Mengen.

Definition 1.2.5. Sei V eine nichtleere Teilmenge eines topologischen Raumes X. V heißt irreduzibel, wenn es keine nichtleeren V-abgeschlossenen Teilmengen V_1 und V_2 gibt mit $V = V_1 \cup V_2$.

Beispiel 1.2.6. $\mathbb{A}^1$ ist irreduzibel, denn nach Beispiel 1.2.4 sind die einzigen echten abgeschlossen Teilmengen von $\mathbb{A}^1$ endlich. Da aber K algebraisch abgeschlossen ist, besitzt $\mathbb{A}^1$ unendlich viele Elemente. Weiter ergibt sich, dass die einzigen abgeschlossen irreduziblen Teilmengen von $\mathbb{A}^1$ die einpunktigen Mengen sind.

Bemerkung 1.2.7. Sei X ein irreduzibler topologischer Raum. So gilt, dass jede nichtleere, offene Teilmenge $U \subseteq X$ dicht in X liegt und irreduzibel ist.

Dies können wir leicht nachprüfen. Ist $U \subseteq X$ eine nichtleere, offene Teilmenge, so erhalten wir eine Zerlegung $X = U^c \cup \overline{U}$ in abgeschlossene Mengen. Da X irreduzibel ist, folgt $\overline{U} = X$. Nehmen wir nun an, dass U reduzibel ist, so existieren $A, B \subseteq X$ abgeschlossen mit $U = A \cup B$. Daraus erhalten wir

$$X = \overline{U} = \overline{A \cup B} = \overline{A} \cup \overline{B} = A \cup B$$

und somit folgt $U \subseteq A$ oder $U \subseteq B$.

Bemerkung 1.2.8. Sei X ein topologischer Raum und $Y \subseteq X$ eine Teilmenge die irreduzibel bezüglich ihrer Relativtopologie ist. Dann ist die abgeschlossene Hülle $\overline{Y}$ von Y irreduzibel.

Auch diese Bemerkung wollen wir beweisen. Angenommen es existieren $A, B \subseteq X$ abgeschlossen mit $\overline{Y} = A \cup B$. Wir erhalten damit $Y = (A \cap Y) \cup (B \cap Y)$. Da Y irreduzibel bezüglich der Relativtopologie ist, gilt $Y \subseteq A$ oder $Y \subseteq B$ und somit nach Definition der abgeschlossenen Hülle $\overline{Y} \subseteq A$ oder $\overline{Y} \subseteq B$.

Definition 1.2.9. Eine irreduzible abgeschlossene Teilmenge des $\mathbb{A}^n$ heißt affine (algebraische) Varietät. Eine offene Teilmenge einer affinen Varietät heißt quasi-affine Varietät.

Wir haben bereits zu einer Menge T von Polynomen die zugehörige Menge der Nullstellen $Z(T)$ definiert. Nun wollen wir zu einer beliebigen Teilmenge des $\mathbb{A}^n$ das Ideal

der Funktionen erklären, die auf der Teilmenge null sind. Sei also $V \subseteq \mathbb{A}^n$ eine beliebige Teilmenge. Wir definieren das Verschwindungsideal von V in $K[X_1, \ldots, X_n]$ durch

$$I(V) := \{f \in K[X_1, \ldots, X_n] : f(P) = 0 \text{ für alle } P \in V\}.$$

Bemerkung 1.2.10. Ist K' nicht algebraisch abgeschlossen, so heißt eine algebraische Menge V definiert über K', wenn ihr Verschwindungsideal $I(V)$ von Polynomen aus $K'[X]$ erzeugt wird. Die K'-rationalen Punkten von V, bezeichnet mit $V(K')$, sind gegeben durch:

$$V(K') = V \cap \mathbb{A}^n(K').$$

Durch die Abbildungen Z und I haben wir nun eine Beziehung zwischen den Mengen von $\mathbb{A}^n$ und Idealen in $K[X_1, \ldots, X_n]$. Es kann gezeigt werden, dass Z und I zueinander inverse, inklusionsumkehrende Bijektionen zwischen den algebraischen Mengen in $\mathbb{A}^n$ und den reduzierten Idealen in $K[X_1, \ldots, X_n]$ sind. Weiter gilt:

Proposition 1.2.11. *Eine algebraische Menge in $\mathbb{A}^n$ ist genau dann irreduzibel, wenn ihr Ideal in $K[X_1, \ldots, X_n]$ ein Primideal ist.*

Beweis. Sei $V \subseteq \mathbb{A}^n$ eine algebraische Menge und $f \cdot g \in I(V)$. Dann gilt

$$V \subseteq Z(f \cdot g) = Z(f) \cup Z(g).$$

Also ist

$$V = (Z(f) \cap V) \cup (Z(g) \cap V).$$

Dabei sind $Z(f) \cap V$ und $Z(g) \cap V$ abgeschlossene Mengen. Da V irreduzibel ist, folgt nun $V = Z(f) \cap V$ oder $V = Z(g) \cap V$. Also ist $V \subseteq Z(f)$ oder $V \subseteq Z(g)$ und damit gilt $f \in I(V)$ oder $g \in I(V)$.

Sei nun umgekehrt $\mathfrak{p}$ ein Primideal in $K[X_1, \ldots, X_n]$. Wir nehmen nun an, dass algebraische Mengen $V_1, V_2 \subseteq \mathbb{A}^n$ mit $Z(\mathfrak{p}) = V_1 \cup V_2$ existieren. Es folgt $\mathfrak{p} = I(V_1) \cap I(V_2)$ und, da $\mathfrak{p}$ ein Primideal ist, gilt $\mathfrak{p} = V_1$ oder $\mathfrak{p} = V_2$. Also ist insgesamt $Z(\mathfrak{p}) = V_1$ oder $Z(\mathfrak{p}) = V_2$ und daher ist $Z(\mathfrak{p})$ irreduzibel. □

Beispiel 1.2.12. Für $n \in \mathbb{N}$ ist $\mathbb{A}^n$ irreduzibel, denn $Z(\mathbb{A}^n) = (0)$ und das Nullideal ist ein Primideal.

Betrachten wir nun ein maximales Ideal $\mathfrak{m} \subseteq K[X_1, \ldots, X_n]$. Nach Proposition 1.2.11 wissen wir, dass dieses Ideal einer minimalen irreduziblen algebraischen Menge in $\mathbb{A}^n$, das heißt einem Punkt $P = (a_1, \ldots, a_n)$, entspricht. Damit ergibt sich, dass jedes maximale Ideal von $K[X_1, \ldots, X_n]$ von der Form $\mathfrak{m} = (a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in K$ ist.

Definition 1.2.13. Sei $V \subseteq \mathbb{A}^n$ eine affine algebraische Menge, dann heißt

$$K[V] := K[X_1, \ldots, X_n]/I(V)$$

der affine Koordinatenring der Varietät V.

Bemerkung 1.2.14. Jede endlich erzeugte K-Algebra B, die ein Integritätsring ist, ist ein affiner Koordinatenring einer affinen Varietät.

Da B eine endlich erzeugte K-Algebra ist, existiert ein Epimorphismus

$$\Phi : K[X_1, \ldots, X_n] \to B.$$

Es gilt dann $B \cong K[X_1, \ldots, X_n]/\ker(\Phi)$. Da B ein Integritätsring ist, ist $\mathfrak{a} = \ker(\Phi)$ ein Primideal und $V := Z(\mathfrak{a})$ nach Proposition 1.2.11 eine Varietät.

Definition 1.2.15. Sei X ein topologischer Raum. Wir definieren die Dimension von X, bezeichnet mit $\dim X$, als das Supremum der Längen n aller Ketten

$$X_0 \subset X_1 \subset \ldots \subset X_n$$

von nichtleeren, abgeschlossenen, irreduziblen Teilmengen $X_i \subset X$.

Als Dimension einer affinen Varietät definieren wir die Dimension der Varietät als topologischen Raum.

Beispiel 1.2.16. Nach Beispiel 1.2.6 sind die einzigen echten irreduziblen, abgeschlossen Teilmengen von $\mathbb{A}^1$ die einpunktigen Mengen und somit hat $\mathbb{A}^1$ die Dimension eins.

Proposition 1.2.17. *Sei X ein topologischer Raum mit $X = \cup_i U_i$ und U_i, $i \in I$, offen. Dann gilt* $\dim X = \sup_i \dim U_i$.

Beweis. Sei $U_i \subset X$ beliebig und $Y_0 \subseteq Y_1 \subseteq \ldots \subseteq Y_n$ eine aufsteigende Kette von abgeschlossenen, irreduziblen Teilmengen in U_i. Nach Bemerkung 1.2.8 ist dann

$$\overline{Y_0} \subseteq \overline{Y_1} \subseteq \ldots \subseteq \overline{Y_n}$$

eine aufsteigende Kette von abgeschlossenen, irreduziblen Teilmengen in X und wir erhalten

$$\sup_i \dim U_i \leq \dim X.$$

Für die andere Richtung betrachten wir eine Kette $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n$ von abgeschlossenen, irreduziblen Teilmengen in X. Dabei können wir ohne Einschränkung annehmen, dass X_0 aus einem Punkt besteht. Dann existiert $i_0 \in I$ mit $X_0 \in U_{i_0}$. Dann ist nach Bemerkung 1.2.7 $X_i \cap U_{i_0}$ dicht in X_i und somit gilt $X_i \cap U_{i_0} \not\subseteq X_{i-1}$. Daher erhalten wir also eine aufsteigende Kette

$$X_0 \cap U_{i_0} \subseteq X_1 \cap U_{i_0} \subseteq \ldots \subseteq X_n \cap U_{i_0}$$

von abgeschlossenen, irreduziblen Teilmengen in U_{i_0}. Somit gilt

$$\dim X \leq \dim U_{i_0} \leq \sup_i \dim U_i.$$

□

Definition 1.2.18. Sei R ein Ring. Die Krulldimension von R ist definiert als das Supremum der Längen n aller Primidealketten

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n.$$

Mit Hilfe von Definition 1.2.18 können wir die Dimension des affinen Koordinatenringes einer Varietät bestimmen. Es drängt sich nun die Frage auf, ob es einen Zusammenhang zwischen dieser Dimension und der Dimensionen der Varietät gibt. Die folgende Proposition wird dies beantworten.

Proposition 1.2.19. *Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät. Dann ist die Dimension von V gleich der Dimension ihres affinen Koordinatenringes $K[V]$.*

Beweis. Sei V eine affine algebraische Menge in $\mathbb{A}^n$, dann gilt nach Proposition 1.2.11, dass die abgeschlossenen, irreduziblen Teilmengen von V genau den Primidealen in $K[X_1, \ldots, X_n]$ und damit den Primidealen in $K[V]$ entsprechen. Also ist $\dim V$ gleich der Länge der längsten Primidealkette in $K[V]$ und damit gleich $\dim K[V]$. □

1.2.2. Projektive Varietäten

Wie im vorherigen Abschnitt sei auch in diesem Abschnitt K ein fester, algebraisch abgeschlossener Körper. Unser Vorgehen wird dabei ähnlich sein wie bei den affinen Varietäten, jedoch mit dem Unterschied, dass wir uns im projektiven Raum befinden. Wie in Abschnitt 1.2.1 kann diese Theorie auch auf einen nicht algebraischen Körper K' angewandt werden.

Definition 1.2.20. Der projektive Raum der Dimension n, bezeichnet mit $\mathbb{P}^n$, ist die Menge aller $(n+1)$-Tupel

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1},\ x_i \neq 0 \text{ für mindestens ein } i,$$

modulo der Äquivalenzrelation die durch

$$(x_0, \ldots, x_0) \sim (y_0, \ldots, y_n) : \Longleftrightarrow\ \exists \lambda \in K - \{0\} \text{ mit } x_i = \lambda y_i,\ i = 1, \ldots n,$$

gegeben ist. Eine Äquivalenzklasse wird mit $[x_0 : \ldots : x_n]$ bezeichnet und $x_0, \ldots, x_n$ werden homogene Koordinaten für den zugehörigen Punkt $P \in \mathbb{P}^n$ genannt.

Bemerkung 1.2.21. Ist K' nicht algebraisch abgeschlossen, so ist die Menge der K'-rationalen Punkte $\mathbb{P}^n(K')$ in $\mathbb{P}^n = \mathbb{P}^n(\overline{K'})$ definiert durch

$$\mathbb{P}^n(K') := \left\{[x_0 : \ldots : x_n] \in \mathbb{P}^n : x_i \in K',\ i = 0, \ldots n\right\}.$$

Wir wollen $K[X_0, \ldots, X_n]$ als graduierten Ring auffassen und rufen uns daher die Definition eines graduierten Ringes und ein paar weitere damit zusammenhängende Definitionen in Erinnerung.

Ein graduierter Ring ist ein Ring S zusammen mit einer Zerlegung $S = \bigoplus_{d\geq 0} S_d$ in direkte Summen von abelschen Gruppen S_d, mit der Eigenschaft

$$S_d \cdot S_e \subseteq S_{d+e},\ d, e \geq 0.$$

Die Elemente von S_d heißen homogene Elemente vom Grad d und jedes Element $f \in S$ lässt sich als endliche Summe von homogenen Elementen darstellen. Es gilt also

$$f = \sum_q f_q,$$

mit $f_q \in S_q$, wobei die f_q homogene Komponenten von f heißen. Ein Ideal $\mathfrak{a} \subseteq S$ heißt homogenes Ideal, wenn aus $f \in \mathfrak{a}$ folgt, dass auch die homogenen Komponenten von f in $\mathfrak{a}$ liegen.

Proposition 1.2.22. *$\mathfrak{a} \subseteq S$ ist genau dann ein homogenes Ideal, wenn $\mathfrak{a}$ von homogenen Elementen erzeugt wird.*

Beweis. Sei $\mathfrak{a}$ ein homogenes Ideal und $\{f_i\}$, $i \in I$, ein Erzeugendensystem von $\mathfrak{a}$. Es folgt, dass die homogenen Komponenten aller f_i wieder in $\mathfrak{a}$ liegen. Damit erzeugen auch die f_{i_q} das Ideal $\mathfrak{a}$.

Sei nun $\mathfrak{a}$ ein Ideal in S mit einem Erzeugendensystem $\{g_i\}$ von homogenen Elementen und $f = \sum_q f_q \in \mathfrak{a}$ beliebig. Dann existiert eine Darstellung $f = \sum_i h_i g_i$, $p_i \in S$. Ist $h_i = \sum_q h_{i_q}$ die Zerlegung von h_i in die homogenen Komponenten, so ist

$$f = \sum_i \sum_q h_{i_q} g_i.$$

Daraus können wir nun schließen, dass

$$f_k = \sum_{q+\deg g_i = k} h_{i_q} g_i \in \mathfrak{a}$$

gilt und somit $\mathfrak{a}$ ein homogenes Ideal ist. □

Weiter gilt, dass auch die Summe, das Produkt, der Schnitt und das Radikalideal eines homogenen Ideals wieder homogen sind. Wenn wir prüfen wollen, ob ein homogenes Ideal $\mathfrak{a}$ ein Primideal ist, reicht es, die Bedingung

$$f \cdot g \in \mathfrak{a} \implies f \in \mathfrak{a} \text{ oder } g \in \mathfrak{a},$$

für homogene Elemente f und g, nachzuweisen. Diese Beweise wollen wir aber nicht führen und verweisen für den interessierten Leser auf Zariski-Samuel [32]. Nun können wir also aus dem Polynomring $K[X_1, \ldots, X_n]$ einen graduierten Ring machen, indem wir

$$S_d := \left\langle X_0^{\alpha_0} \cdot \ldots \cdot X_n^{\alpha_n} : \sum \alpha_i = d \right\rangle, \ d \geq 0$$

setzen. Die S_d bestehen also aus allen Linearkombinationen von Monomen mit Gesamtgrad d.

Ist $f \in K[X_1, \ldots, X_n]$ ein Polynom, so können wir mit f keine Funktion auf dem projektiven Raum definieren. Da die homogenen Koordinaten nicht eindeutig sind, hätten wir ein Problem, den Wert der Funktion in einem Punkt zu definieren. Für homogene Polynome können wir dieses Problem allerdings umgehen. Ist f ein homogenes Polynom vom Grad d, so gilt

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^n f(x_0, \ldots, x_n).$$

Daher ist es jetzt sinnvoll, davon zu reden, ob f an einem Punkt 0 ist oder nicht. Wir können nun mit f eine Funktion auf $\mathbb{P}^n$ durch

$$\tilde{f} : \mathbb{P}^n \to \{0, 1\}, \ P \mapsto \begin{cases} 0, & f(P) = 0, \\ 1, & f(P) \neq 0, \end{cases}$$

definieren. Jetzt können wir für eine beliebige Teilmenge $T \subset S$ von homogenen Polynomen die Nullstellenmenge $Z(T)$ von T definieren durch

$$Z(T) := \{P \in \mathbb{P}^n | f(P) = 0 \text{ für alle } f \in T\}.$$

Sei $\mathfrak{a} \subseteq S$ ein homogenes Ideal. Dann definieren wir die Nullstellenmenge $Z(\mathfrak{a})$ durch $Z(\mathfrak{a}) := Z(T)$, wobei T die Menge der homogenen Elemente von $\mathfrak{a}$ ist. Da S ein noetherscher Ring ist, gibt es homogene Elemente $f_1, \ldots, f_r$ in T, so dass $Z(T) = Z(f_1, \ldots, f_r)$ ist.

Definition 1.2.23. Eine Teilmenge $V \subseteq \mathbb{P}^n$ heißt algebraische Menge, wenn eine Menge $T \subseteq S$ von homogenen Elementen existiert, so dass $Z(T) = V$ ist.

Wie im vorherigen Abschnitt ist es möglich, zu zeigen, dass die Vereinigung von zwei algebraischen Mengen und der Schnitt einer Familie algebraischer Mengen wieder eine algebraische Menge ist. Ebenso sind die leere Menge und der ganze Raum algebraische Mengen. Damit können wir nun wieder die Zariski-Topologie definieren, diesmal auf $\mathbb{P}^n$, indem wir als abgeschlossene Mengen die algebraischen Mengen nehmen. Wir haben also einen topologischen Raum und können jetzt, mit Hilfe der Definitionen 1.2.5 und 1.2.15, analog zu den affinen Varietäten eine projektive Varietät definieren.

Definition 1.2.24. Eine irreduzible, abgeschlossene Teilmenge des $\mathbb{P}^n$ heißt projektive (algebraische) Varietät. Eine offene Teilmenge einer projektiven Varietät heißt quasiprojektive Varietät. Die Dimension der projektiven Varietät ist ihre Dimension als topologischer Raum.

Sei $V \subseteq \mathbb{P}^n$ beliebig. Dann definieren wir das homogene Ideal von V in S, bezeichnet mit $I(V)$, durch

$$I(V) := \{f \in S : f \text{ ist homogen und } f(P) = 0 \text{ für alle } P \in V\}.$$

Den homogene Koordinatenring $S(V)$ einer algebraischen Menge V definieren wir als

$$S(V) := S/I(V).$$

Bemerkung 1.2.25. Ist, wie in Bemerkung 1.2.10, K' ein nicht algebraisch abgeschlossener Körper, so heißt eine algebraische Menge V definiert über K', wenn ihr Verschwindungsideal $I(V)$ von homogenen Polynomen aus $K'[X]$ erzeugt wird. Die K'-rationalen Punkten von V, bezeichnet mit $V(K')$, sind gegeben durch:

$$V(K') = V \cap \mathbb{P}^n(K').$$

Als nächstes wollen wir einen Zusammenhang zwischen den projektiven und den affinen Varietäten herstellen. Dazu werden wir zuerst eine offene Überdeckung des $\mathbb{P}^n$ benötigen. Mit H_i bezeichnen wir die Nullstellenmenge des Polynoms X_i und setzen $U_i := \mathbb{P}^n - H_i$. Die U_i sind nach Konstruktion offene Mengen und es gilt

$$\mathbb{P}^n = \bigcup_{i=1}^{n} U_i,$$

denn für $P \in \mathbb{P}^n$ mit $P = (a_0, \ldots, a_n)$ gilt $a_i \neq 0$ für mindestens ein i und somit ist $P \in U_i$. Nun definieren wir eine Abbildung $\varphi_i : U_i \to \mathbb{A}^n$ durch

$$\varphi_i(P) = \varphi_i(a_0, \ldots, a_n) = \left(\frac{a_0}{a_i}, \ldots, \frac{a_i - 1}{a_i}, \frac{a_i + 1}{a_i}, \ldots, \frac{a_n}{a_i}\right).$$

φ_i ist wohldefiniert, denn für $P \in U_i$ mit $P = (a_1, \ldots, a_n) = (b_1, \ldots, b_n)$ existiert ein $\lambda \in K - \{0\}$ mit $a_j = \lambda b_j,\ j = 1, \ldots, n$, und daraus folgt

$$\frac{b_j}{b_i} = \frac{\lambda a_j}{\lambda a_i} = \frac{a_j}{a_i},\ j = 1 \ldots, n.$$

Satz 1.2.26. *Für $i = 1, \ldots, n$ ist die Abbildung φ_i ein Homöomorphismus zwischen U_i und $\mathbb{A}^n$. Dabei trägt U_i die von $\mathbb{P}^n$ induzierte Relativtopologie und $\mathbb{A}^n$ die Zariski Topologie.*

Beweis. Es ist klar, dass die φ_i bijektive Abbildungen sind. Es bleibt also zu zeigen, dass sie auch offene und stetige Abbildungen sind. Ohne Einschränkung wollen wir jetzt den Fall $i = 0$ betrachten und werden φ und U anstatt φ_0 und U_0 schreiben. Mit S^h hingegen wollen wir die Menge der homogenen Elemente des Polynomringes S bezeichnen. Weiter definieren wir zwei Abbildungen

$$\alpha : S^h \to K[Y_1, \ldots, Y_n],\ f \mapsto f(1, Y_1, \ldots, Y_n)$$

und

$$\beta : K[Y_1, \ldots, Y_n] \to S^h,\ g \mapsto X_0^{\deg g} g\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right).$$

Als erstes werden wir zeigen, dass φ eine offene Abbildung ist. Dazu werden wir zeigen, dass abgeschlossene Mengen unter φ wieder auf abgeschlossene Mengen abgebildet werden. Da φ bijektiv ist, ist dieses äquivalent zu der Bedingung, dass offene Mengen auf offene Mengen abgebildet werden. Sei nun $V \subseteq U$ eine beliebige in U abgeschlossene Menge und $\overline{V}$ ihr Abschluß in $\mathbb{P}^n$. Dann ist, nach Definition der Zariski Topologie, $\overline{V}$ eine algebraische Menge und daher existiert eine Teilmenge $T \subseteq S^h$ mit $Z(T) = \overline{V}$. Wir setzen dann $T' := \alpha(T)$ und erhalten damit $\varphi(V) = Z(T')$. Also ist $\varphi(V)$ abgeschlossen in $\mathbb{A}^n$. Es fehlt jetzt noch die Stetigkeit von φ. Diese werden wir nachweisen, indem wir zeigen, dass φ^{-1} eine offene Abbildung ist. Sei dazu $W \subseteq \mathbb{A}^n$ eine beliebige abgeschlossene Menge. Nach Definition der Topologie existiert dann eine Menge $D \subset K[Y_1, \ldots, Y_n]$ mit $Z(D) = W$. Setzen wir $D' := \beta(D)$, so erhalten wir, dass $\phi^{-1}(W) = Z(D') \cap U$ gilt. Damit ist $\phi^{-1}(W)$ abgeschlossen in U. Insgesamt ist jetzt also φ eine bijektive, stetige und offene Abbildung und somit ein Homöomorphismus. □

Es ist uns jetzt möglich eine projektive Varietät durch offene Mengen zu überdecken, die homöomorph zu affinen Varietäten sind.

Corollar 1.2.27. *Ist V eine projektive Varietät, so gilt*

$$V = \bigcup_{i=0}^{n} V \cap U_i.$$

Dabei sind die $V \cap U_i,\ i = 1, \ldots n$, unter φ_i homöomorph zu einer affinen Varietät.

Wir können aber auch die Homöomorphismen φ_i dazu benutzen, eine affine Varietät projektiv zu sehen. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät. Durch φ_0 betrachten wir $\mathbb{A}^n$ als eine offene Menge $U_0 \subseteq \mathbb{P}^n$. Dann heißt die abgeschlossene Hülle $\overline{V}$ von V in $\mathbb{P}^n$ der projektive Abschluß von V. Nach Bemerkung 1.2.8 ist $\overline{V}$ eine projektive Varietät und für ihr Verschwindungsideal gilt:

Proposition 1.2.28. *$I(\overline{V})$ wird erzeugt von $\beta\,(I(V))$, dabei ist β die Abbildung aus dem Beweis von Satz 1.2.26.*

Beweis. Sei $f \in I(V)$. Dann folgt unmittelbar, dass $\beta(f) \in I(\overline{V})$ gilt.

Ist nun umgekehrt $h \in I(\overline{V})$ ein homogenes Polynom vom Grad d. Dann existiert $n \in \mathbb{N}$ mit $h = X_0^n \cdot H$, dabei teilt X_0^n nicht H. Wir setzen dann

$$g(X_1, \ldots, X_n) := H(1, X_1, \ldots, X_n).$$

Es folgt $g \in I(V)$ und $\beta(g) = H$ und damit die Behauptung. □

1.2.3. Sätze über Varietäten

Definition 1.2.29. Sei V eine affine Varietät. Eine Funktion $f : V \to K$ heißt regulär im Punkt $P \in V$, wenn es eine offene Umgebung U mit $P \in U \subseteq V$ gibt, sowie Polynome $g, h \in K[X_1, \ldots, X_n]$ mit $h(P) \neq 0,\ P \in U$, so dass $f = g/h$ auf U gilt. Eine Funktion heißt regulär auf V, wenn sie regulär in allen Punkten von V ist.

Proposition 1.2.30. *Ist $f : V \to K$ eine reguläre Funktion, so ist f stetig, wenn man K mit $\mathbb{A}^1$, versehen mit der Zariski-Topologie, identifiziert.*

Beweis. Wir zeigen, dass das Urbild abgeschlossener Mengen wieder abgeschlossen ist. Die abgeschlossenen Mengen in $\mathbb{A}^1$ sind, wie wir schon im Beispiel 1.2.4 gesehen haben, die endlichen Mengen, $\emptyset$ und K. Es reicht also zu zeigen, dass für $a \in K$ beliebig die Menge $f^{-1}(a)$ abgeschlossen ist. Dazu merken wir an, dass eine Teilmenge W eines topologischen Raumes genau dann abgeschlossen ist, wenn W von offenen Mengen W_i überdeckt wird und für jedes W_i die Menge $W \cap W_i$ in W_i abgeschlossen ist. Sei $U \subseteq V$ eine offene Menge, so dass $g, h \in K[X_1, \ldots, X_n]$ existieren mit

$$f = g/h \text{ und } h \neq 0 \text{ auf } U.$$

Dann ist

$$f^{-1}(a) \cap U = \{P \in U : g(P)/h(P) = a\}.$$

Es gilt genau dann $g(P)/h(P) = a$, wenn $(g - ah)(P) = 0$ ist. Daraus erhalten wir

$$f^{-1}(a) \cap U = Z(g - ah) \cap U.$$

Damit ist $f^{-1}(a) \cap U$ in U abgeschlossen und da f regulär auf V ist, folgt nun, nach unserer Vorbemerkung, dass $f^{-1}(a)$ abgeschlossen in V ist. □

Definition 1.2.31. Sei V eine projektive Varietät. Eine Funktion $f : V \to K$ heißt regulär im Punkt $P \in V$, wenn es eine offene Umgebung U mit $P \in U \subseteq V$ gibt, sowie homogene Polynome $g, h \in K[X_0, \ldots, X_n]$ vom selben Grad mit $h(P) \neq 0,\ P \in U$, so dass $f = g/h$ auf U gilt. Eine Funktion heißt regulär auf V, wenn sie regulär in allen Punkten von V ist.

Wie in Proposition 1.2.30 ergibt sich, dass reguläre Funktionen auf projektiven Varietäten stetig sind.

Bezeichnung 1.2.32. Die Menge aller regulären Funktionen auf einer Varietät V bezeichnen wir mit $\mathcal{O}(V)$.

Proposition 1.2.33. *Sei V eine Varietät und $f, g \in \mathcal{O}(V)$. Existiert eine nichtleere, offene Menge $U \subseteq V$, so dass $f = g$ auf U gilt, so folgt $f = g$ auf ganz V.*

Beweis. Sei V eine Varietät, $f, g \in \mathcal{O}(V)$ und es existiere eine nichtleere, offene Menge U auf der $f = g$ ist. Nach Bemerkung 1.2.7 ist U dicht in V. Weiter wissen wir, dass U aus der Menge der Punkte besteht, für die $f - g = 0$ gilt. Da $f, g \in \mathcal{O}(V)$, ist $f - g$ stetig und damit $U = (f - g)^{-1}(0)$ abgeschlossen. Insgesamt ist U also eine dichte, abgeschlossene Teilmenge von V und somit gleich V. □

Betrachten wir das folgende Beispiel:

Beispiel 1.2.34. Sei $V \subseteq \mathbb{A}^2$ gegeben durch $Z(Y^2 - X^3)$ und $f = Y/X$. Wir setzen $V' := V \setminus \{(0,0)\}$ und stellen fest, dass f eine reguläre Funktion auf V' ist. Weiter sei $g = f^2$, dann ist auch g auf V' regulär und es gilt

$$g(X,Y) = \frac{Y^2}{X^2} = \frac{X^3}{X^2} = X.$$

Wir setzen $g(0,0) = 0$ und somit ist g regulär auf V. f lässt sich aber nicht auf V regulär fortsetzen, denn ansonsten würde es eine offene Umgebung W von $(0,0)$ und $u, v \in K[X,Y]$ geben, so dass in allen Punkten von W

$$\frac{Y}{X} = \frac{u(X,Y)}{v(X,Y)} \tag{1.1}$$

gilt. Dabei ist $v(0,0) \neq 0$. Wir können annehmen, da $Y^2 = X^3$ gilt, dass u und v von der Gestalt

$$u(X,Y) = u_0(X) + Yu_1(X),\ v(X,Y) = v_0(X) + Yv_1(X)$$

sind. Durch Einsetzen in (1.1) und Ausmultiplizieren erhalten wir

$$Yv_0(X) + X^3v_1(X) = Xu_0(X) + XYu_1(X). \tag{1.2}$$

Die Gleichheit gilt auf der nichtleeren, offenen Menge W und damit nach Proposition 1.2.33 auch auf V. Somit gilt (1.2) auch modulo des Ideals $(Y^2 - X^3)$ und damit ebenso modulo des größeren Ideals (X^2, XY, Y^2), wodurch wir

$$v_0(X)Y \equiv u_0(X)X \mod (X^2, XY, Y^2)$$

folgern können. Damit ist

$$v_0(0)Y \equiv u_0(0)0 \equiv 0 \mod (X^2, XY, Y^2).$$

Es folgt $v_0(0) = 0$. Dies ist ein Widerspruch zu $v(0,0) \neq 0$. Wir können also f nicht regulär auf V fortsetzen.

Mit Hilfe von regulären Funktionen können wir die Kategorie der Varietäten definieren. Die Objekte sind dabei die Varietäten. Die Morphismen sind gegeben durch stetige

Abbildungen $\phi : A \to B$ mit der Eigenschaft, dass für alle offenen Teilmengen $U \subseteq B$ und jede reguläre Funktion $f : U \to K$ die Funktion $f \circ \phi : \phi^{-1}(U) \to K$ regulär ist. Zwei Varietäten A, B sind nun isomorph, wenn zwei Morphismen $\phi : A \to B$ und $\psi : B \to A$ mit $\phi \circ \psi = \mathrm{id}_B$ und $\psi \circ \phi = \mathrm{id}_A$ existieren. Dabei reicht es nicht aus, dass ϕ eine bijektive Abbildung ist, wie in der Kategorie der Mengen, oder ein Homöomorphismus, wie in der Kategorie der topologischen Räume.

Beispiel 1.2.35. Sei $\phi : \mathbb{A}^1 \to \mathbb{A}^2,\ t \mapsto (t^2, t^3)$. Dann ist ϕ ein Morphismus und die Umkehrabbildung ist gegeben durch

$$\psi : Z(X^2 - Y^3) \to \mathbb{A}^1,\ (x, y) \mapsto \begin{cases} \frac{y}{x} & ,\ (x, y) \neq (0, 0), \\ 0 & ,\ (x, y) = (0, 0). \end{cases}$$

ψ ist eine stetige Abbildung und damit ein Homöomorphismus. ψ ist aber kein Morphismus auf $Z(Y^2 - X^3)$, denn ansonsten wäre ψ eine reguläre Fortsetzung auf $Z(Y^2 - X^3)$. Diese kann es aber nicht geben, wie wir im Beispiel 1.2.34 gesehen haben.

Proposition 1.2.36. *Sei $U_i \subseteq \mathbb{P}^n$ die offene Menge, die durch $X_i \neq 0$ definiert wird. Dann ist die Abbildung $\phi_i : U_i \to \mathbb{A}^n$ aus Satz 1.2.26 ein Isomorphismus von Varietäten.*

Beweis. In Satz 1.2.26 haben wir schon nachgewiesen, dass ϕ_i ein Homöomorphismus ist. Sei $f : \mathbb{A}^n \to K$ eine reguläre Funktion, dann müssen wir nun zeigen, dass auch $f \circ \phi_i : \phi_i^{-1}(\mathbb{A}^n) = U_i \to K$ eine reguläre Funktion ist. Für $g \in K[X_1, \ldots, X_n]$ ist $g \circ \phi_i$ ein homogenes Polynom vom Grad 0. Daraus erhalten wir, dass $f \circ \phi_i$ ein Quotient von homogenen Polynomen desselben Grades und somit regulär ist. Also ist ϕ_i ein Morphismus. Es bleibt nun noch zu zeigen, dass auch die Umkehrabbildung, die durch

$$\psi_i : \mathbb{A}^n \to U_i,\ (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_i, 1, a_{i+1}, \ldots, a_n)$$

gegeben ist, ein Morphismus ist. Dazu müssen wir nur noch zeigen, dass für eine reguläre Funktion $h : U_i \to K$ auch die Funktion $h \circ \psi_i : \psi_i^{-1}(U_i) = \mathbb{A}^n \to K$ regulär ist. Dieses ist aber trivial und somit ist ϕ_i ein Isomorphismus. □

Definition 1.2.37. Sei V eine Varietät und $P \in V$. Dann definieren wir den lokalen Ring der Varietät V in P, bezeichnet mit $\mathcal{O}_{V,P}$, durch

$$\mathcal{O}_{V,P} := \{(U, f) :\ U \subseteq V \text{ offen},\ P \in U,\ \text{f ist regulär auf } U\}.$$

Dabei ist $(U, f) \sim (W, g)$ wenn $f = g$ auf $U \cap W$ gilt.

Wie in Proposition 1.2.33, folgt aus $(U, f) \sim (W, g)$, dass $f = g$ auf ganz V gilt. Somit erhalten wir, dass $\sim$ eine Äquivalenzrelation ist. $\mathcal{O}_{V,P}$ ist tatsächlich ein lokaler Ring, das heißt er besitzt nur ein maximales Ideal. Ist nämlich $\mathfrak{m}_P$ die Menge aller Äquivalenzklassen, die in P null sind, so ist $\mathfrak{m}_P$ ein Ideal und für $f \in \mathcal{O}_{V,P} - \mathfrak{m}_P$ gilt $f(P) \neq 0$. Damit

existiert eine Umgebung U von P auf der $1/f$ regulär ist. Also sind alle Elemente aus $\mathcal{O}_{V,P} - \mathfrak{m}_P$ Einheiten und somit ist $\mathcal{O}_{V,P}$ ein lokaler Ring.

Gibt es einen Isomorphismus zwischen zwei Varietäten, so wollen wir einen Zusammenhang zwischen ihren lokalen Ringen herstellen. Seien V, W zwei beliebige Varietäten und $\phi : V \to W$ ein Morphismus. Dann definieren wir für $P \in V$ die Abbildung ϕ_P^* durch

$$\phi_P^* : \mathcal{O}_{\phi(P),W} \to \mathcal{O}_{P,V}, \ f \mapsto f \circ \phi.$$

Diese Abbildung ist wohldefiniert, denn ϕ ist ein Morphismus. Weiter ist ϕ_P^* ein Homomorphismus und es gilt die folgende Proposition.

Proposition 1.2.38. *Seien V, W zwei Varietäten. Dann ist die Abbildung $\phi : V \to W$ genau dann ein Isomorphismus, wenn ϕ ein Homöomorphismus ist und die Abbildung ϕ_P^* ein Isomorphismus ist für alle $P \in V$.*

Beweis. Sei ϕ ein Isomorphismus und $P \in V$ beliebig. Es bleibt zu zeigen, dass ϕ_P^* ein Isomorphismus ist. Da die regulären Funktionen in P einen Ring bilden, müssen wir zeigen, dass ϕ_P^* bijektiv ist. Seien dazu $f, g \in \mathcal{O}_{\phi(P),W}$ mit $\phi_P^*(f) = \phi_P^*(g)$, das heißt es gilt $f \circ \phi = g \circ \phi$. Da ϕ ein Isomorphismus ist, folgt daraus $f = g$ und damit ist ϕ_P^* injektiv. Um die Surjektivität zu beweisen, betrachten wir eine beliebige reguläre Funktion $h \in \mathcal{O}_{P,V}$. Dann setzen wir $f := h \circ \phi^{-1}$. Da ϕ^{-1} ein Morphismus ist, folgt $f \in \mathcal{O}_{\phi(P),W}$. Damit erhalten wir

$$\phi_P^*(f) = f \circ \phi = h \circ \phi^{-1} \circ \phi = h.$$

Also ist ϕ_P^* auch surjektiv und damit ein Isomorphismus.

Sei nun umgekehrt ϕ ein Homöomorphismus und für alle $P \in V$ ϕ_P^* ein Isomorphismus. Wir müssen jetzt lediglich zeigen, dass ϕ und ϕ^{-1} Morphismen sind. Sei $U \subseteq W$ offen und $f : U \to K$ regulär. Dann gilt für alle $Q \in U$, dass f ein Element des Ringes $\mathcal{O}_{Q,W}$ ist. Daraus folgt, mit Hilfe der Surjektivität von ϕ, dass

$$\phi_P^*(f) = f \circ \phi \in \mathcal{O}_{\phi^{-1}(Q),V}$$

gilt. Damit ist $f \circ \phi$ in allen Punkten $P \in \phi^{-1}(U)$ regulär und somit ist ϕ ein Morphismus. Völlig analog erhalten wir, dass ϕ^{-1} ein Morphismus ist und insgesamt ist damit ϕ ein Isomorphismus. □

Definition und Satz 1.2.39. *Sei V eine Varietät. Wir definieren den Körper der Funktionen $K(V)$ von V durch*

$$K(V) := \{(U, f) : \ U \subseteq V \text{ offen und } f \text{ ist regulär auf } U\}.$$

Dabei ist wieder $(U, f) \sim (W, g)$, wenn $f = g$ auf $U \cap W$ gilt. Die Elemente von $K(V)$ heißen rationale Funktionen.

Beweis. Sei V eine Varietät. Wir müssen zeigen, dass $K(V)$ tatsächlich ein Körper ist. Wenn $A, B \subseteq V$ zwei nichtleere, offene Mengen sind, müssen sie einen gemeinsamen Schnitt haben, ansonsten hätten wir durch $V = A^c \cup B^c$ eine Zerlegung von V in echte, abgeschlossene Teilmengen. Dieses ist aber ein Widerspruch zur Irreduziblität. Wir können jetzt also Addition und Multiplikation von zwei Elementen aus $K(V)$ auf dem Schnitt ihrer Mengen erklären. Damit ergibt sich, dass $K(V)$ ein Ring ist. Es bleibt die Existenz von Inversen zu zeigen. Sei dazu $(U, f) \in K(V)$ mit $f \neq 0$. Wir definieren jetzt die Menge $W := U - U \cap Z(f)$. W ist offen und $1/f$ ist regulär auf W. Damit ist $(W, 1/f) \in K(V)$. □

Bemerkung. Ersetzen wir die Varietät V durch eine isomorphe Varietät, so sind die entsprechenden Ringe ebenfalls isomorph, siehe zum Beispiel Proposition 1.2.38. Die Ringe $\mathcal{O}(V), \mathcal{O}_{V,P}$ und $K(V)$ sind also bis auf Isomorphie invariant unter der Varietät V und dem Punkt P.

Theorem 1.2.40. *Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät mit Koordinatenring $K[V]$. Dann gilt:*

i. $\mathcal{O}(V) \cong K[V]$

ii. für jeden Punkt $P \in V$ sei $\mathfrak{m}_P \subseteq K[V]$ das Ideal der Funktionen, die in P null sind. Dann ist durch $P \mapsto \mathfrak{m}_P$ eine bijektive Abbildung zwischen den Punkten von V und den maximalen Idealen von $K[V]$ gegeben.

iii. für alle $P \in V$ ist $\mathcal{O}_{V,P} \cong K[V]_{\mathfrak{m}_P}$ und $\dim \mathcal{O}_{V,P} = \dim V$

iv. $K(V)$ ist isomorph zum Quotientenkörper von $K[V]$

Beweis. Jedes Polynom $f \in K[X_1, \ldots, X_n]$ ist nach Definition eine reguläre Funktion auf V. Daher erhalten wir einen Homomorphismus $K[X_1, \ldots, X_n] \to \mathcal{O}(V)$ und die Elemente des Kerns bestehen aus den Elementen von $I(V)$. Wir erhalten also einen injektiven Homomorphismus

$$\alpha : K[V] \to \mathcal{O}(V).$$

Nach Proposition 1.2.11 wissen wir bereits, dass eine bijektive Abbildung zwischen den Punkten von V und den maximalen Idealen in $K[X_1, \ldots, X_n]$, die $I(V)$ enthalten, existiert. Zwischen diesen maximalen Idealen und den maximalen Idealen in $K[V]$ gibt es auch eine bijektive Abbildung. Mit Hilfe von α können wir nun Elemente aus $K[V]$ als Funktionen identifizieren und wir erhalten, dass die zugehörigen maximalen Ideale gerade $\mathfrak{m}_P = \{f \in K[V] : f(P) = 0\}$ entsprechen, womit *ii.* bewiesen ist.

Um die Aussage *iii.* zu beweisen, konstruieren wir eine ähnliche Abbildung wie α. Jedes Element aus $K[X_1, \ldots, X_n]_{\mathfrak{m}_P}$ ist eine reguläre Funktion in P. Wir erhalten also einen Homomorphismus $K[X_1, \ldots, X_n]_{\mathfrak{m}_P} \to \mathcal{O}_{V,P}$. Nach Definition einer regulären Funktion in P ist dieser Homomorphismus surjektiv. Die Elemente des Kerns sind gerade die Elemente

aus $I(V)_{\mathfrak{m}_P}$. Damit erhalten wir also einen bijektiven Homomorphismus $K[V]_{\mathfrak{m}_P} \to \mathcal{O}_{V,P}$, womit wir die Behauptung bewiesen haben.

Aus *iii.* folgt, dass der Quotientenkörper von $K[V]$ isomorph zum Quotientenkörper der $\mathcal{O}_{V,P}$ ist und zwar für alle $P \in V$. Dieser hingegen ist gleich $K(V)$, denn jede rationale Funktion liegt in einem $\mathcal{O}_{V,P}$ und damit ist *iv.* bewiesen.

Jetzt müssen wir nur noch *i.* beweisen. Es gilt

$$\mathcal{O}(V) \subseteq \bigcap_{P \in V} \mathcal{O}_{V,P}.$$

Nach *ii.* und *iii.* folgt dann

$$K[V] \subseteq \mathcal{O}(V) \subseteq \bigcap_{\mathfrak{m}} K[V]_{\mathfrak{m}},$$

dabei durchläuft $\mathfrak{m}$ alle maximalen Ideale von $K[V]$. Da nach Lemma 1.1.1

$$K[V] = \cap_{\mathfrak{m}} K[V]_{\mathfrak{m}}$$

gilt, folgt die Behauptung. □

Wir wollen nun das äquivalente Resultat für die projektiven Varietäten formulieren. Dafür benötigen wir einige zusätzliche Bezeichnungen.

Sei S ein graduierter Ring, $\mathfrak{p}$ ein homogenes Primideal und T die Menge, die aus allen homogenen Elementen von S, die nicht aus $\mathfrak{p}$ sind, besteht. Mit $S_{(\mathfrak{p})}$ bezeichnen wir die Menge aller homogenen Elemente vom Grad 0 aus der Lokalisierung von S bezüglich der Menge T. Ist $a \in T^{-1}S$, so gilt $a = f/g$, wobei $f \in S$ homogen ist und $g \in T$. Mit $\deg(a) = \deg(f) - \deg(g)$ wird $T^{-1}S$ wieder zu einem graduierten Ring. Weiter ist $S_{(\mathfrak{p})}$ ein lokaler Ring mit maximalem Ideal $(\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}$. Dies wollen wir nachweisen, denn für $f/g \in S_{(\mathfrak{p})}$ mit $f/g \notin (\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}$ gilt $f \in T$ und somit

$$(f/g)^{-1} = g/f \in S_{(\mathfrak{p})}.$$

Damit sind alle Elemente aus $S_{(\mathfrak{p})} - ((\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})})$ Einheiten, was $S_{(\mathfrak{p})}$ zu einem lokalen Ring mit maximalem Ideal $(\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}$ macht. Für $\mathfrak{p} = (0)$ erhalten wir sogar, dass $S_{((0))}$ ein Körper ist. Für ein homogenes Element $f \in S$ bezeichnen wir ebenso mit $S_{(f)}$ die Menge aller homogenen Elemente vom Grad 0 aus der Lokalisierung S_f.

Lemma 1.2.41. *Sei $U_i \subseteq \mathbb{P}^n$ die offene Menge mit $X_i \neq 0$, V eine projektive Varietät und $V_i := V \cap U_i$. Ist $V_i \neq \emptyset$, so gilt $S(V)_{(X_i)} \cong K[V_i]$.*

Beweis. Nach Proposition 1.2.36 ist ϕ_i ein Isomorphismus und somit ist V_i isomorph zu einer affinen Varietät. Wir wollen jetzt den Isomorphismus

$$\nu : K[V_i] \to S(V)_{(X_i)}$$

konstruieren. Dabei wollen wir uns auf den Fall $i = 0$ beschränken, das heißt wir nehmen an, dass $V_0 \neq \emptyset$ gilt. Um diese Abbildung zu konstruieren, benötigen wir zuerst die Abbildung

$$\phi_0^* : K[Y_1, \ldots, Y_n] \to K[X_0, \ldots, X_n]_{(X_0)},$$

die durch

$$f(Y_1, \ldots, Y_n) \mapsto f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$$

gegeben ist. Wir betrachten jetzt ϕ_0^* etwas genauer. Ist $f \in K[Y_1, \ldots, Y_n]$ durch

$$f(Y_1, \ldots, Y_n) = \sum a_{\alpha_1, \ldots \alpha_n} Y_1^{\alpha_1} \cdot \ldots \cdot Y_n^{\alpha_n}$$

gegeben, so gilt

$$\begin{aligned}
\phi_0^*(f) &= \sum a_{\alpha_1, \ldots \alpha_n} \left(\frac{X_1}{X_0}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{X_n}{X_0}\right)^{\alpha_n} \\
&= \sum a_{\alpha_1, \ldots \alpha_n} \left(\frac{X_1}{X_0}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{X_n}{X_0}\right)^{\alpha_n} \cdot \left(\frac{X_0}{X_0}\right)^{\deg(f) - \sum_i \alpha_i} \\
&= \frac{1}{X_0^{\deg(f)}} \sum a_{\alpha_1, \ldots, \alpha_n} X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n} \cdot X_0^{\deg(f) - \sum_i \alpha_i}.
\end{aligned}$$

Damit können wir nun nachrechnen, dass ϕ_0^* ein Isomorphismus ist. Nach Proposition 1.2.28 gilt für ein homogenes Polynom $f \in S$, dass f genau dann in $I(V)$ liegt, wenn ein $g \in I(V_0)$ und $d \in \mathbb{N}$ mit $d \geq \deg g$ existiert, so dass

$$f(X_0, \ldots, X_n) = X_0^n \cdot \phi_0^*(g(X_1, \ldots, X_n)) \tag{1.3}$$

gilt. Ist nun $f \in I(V)_{(X_0)}$, so existiert $h \in I(V)$ mit $f = h/X_0^{\deg h}$. Mit (1.3) erhalten wir, dass ein Polynom $g \in I(V_0)$ und $n \in \mathbb{N}$ existiert mit $h = X_0^n \phi_0^*(g)$. Weiter ist $X_0 \notin I(V)$, da $V_0 \neq \emptyset$. Da $I(V)$ ein Primideal ist, können wir daraus $\phi_0^*(g) \in I(V)$ folgern. Weiter erkennen wir, dass für $g \in I(V_0)$, $\phi_0^*(g) \in I(V)_{(X_0)}$ folgt. Insgesamt erhalten wir also $\phi_0^*(I(V_0)) = I(V)_{(X_0)}$. Nun definieren wir die Abbildung $\nu : K[V_0] \to S(V)_{(X_0)}$ durch

$$\nu(\overline{f}) := \pi(\phi_0^*(f)),\ \overline{f} \in K[Y_1, \ldots, Y_n]/I(V_0).$$

Dabei bezeichnen wir mit $\pi : K[X_0, \ldots, X_n]_{(X_0)} \to K[X_0, \ldots, X_n]_{(X_0)}/I(V)_{(X_0)}$ die kanonische Projektion. Wir müssen zunächst zeigen, dass ν wohldefiniert ist. Gilt $\overline{f} = \overline{g}$, so existiert $h \in I(V_0)$ mit $g = f + h$ und es folgt

$$\nu(\overline{g}) = \pi(\phi_0^*(g)) = \pi(\phi_0^*(f) + \phi_0^*(h)) = \pi(\phi_0^*(f)) = \nu(\overline{f}).$$

Da ϕ_0^* ein Isomorphismus ist, ist auch ν ein Isomorphismus. □

Nun können wir das Resultat für die projektiven Varietäten formulieren:

Theorem 1.2.42. *Sei $V \subseteq \mathbb{P}^n$ eine projektive Varietät mit homogenen Koordinatenring $S(V)$. Dann gilt*

i. $\mathcal{O}(V) = K$

ii. $K(V) \cong S(V)_{((0))}$

iii. $\dim S(V) = \dim V + 1$.

Beweis. Wir wollen zuerst die Aussage *ii.* beweisen. Es gilt $K(V) = K(V_i)$. Nach Theorem 1.2.40 ist $K(V_i)$ der Quotientenkörper von $K[V_i]$. Mit Lemma 1.2.41 folgt damit insgesamt:

$$K(V) = S(V)_{((0))}.$$

Als nächstes wollen wir *i.* beweisen. Sei dazu $f \in \mathcal{O}(V)$. Dann gilt $f \in \mathcal{O}(V_i)$ für alle i und somit gilt nach Theorem 1.2.40 $f \in K[V_i]$. Nach Lemma 1.2.41 gilt $K[V_i] \cong S(V)_{(X_i)}$ und daher existiert $g_i \in S(V)$ homogen vom Grad N_i, so dass

$$f = \frac{g_i}{X_i^{N_i}}$$

gilt. Sei L der Quotientenkörper von $S(V)$. Mit *i.* können wir die Ringe $\mathcal{O}(V), K(V)$ und $S(V)$ als Unterringe von L auffassen. Wir können nun

$$X_i^{N_i} \cdot f \in S(V)_{N_i}$$

folgern. Als nächstes wählen wir $N \in \mathbb{N}$ mit $N \geq \sum_i N_i$. Da $S(V)_N$ von den Monomen vom Grad N in $X_0, \ldots, X_n$ aufgespannt wird, gibt es in jedem Monom mindestens ein X_i mit $\deg(X_i) \geq N_i$. Für alle i existiert, wie wir eben gezeigt haben, eine Darstellung $f = g_i/X_i^{N_i}$ und daher gilt

$$S(V)_N \cdot f \subseteq S(V)_N.$$

Daraus erhalten wir

$$S(V)_N \cdot f^k \subseteq S(V)_N,\ k \in \mathbb{N}.$$

Insbesondere gilt dann

$$X_0^N \cdot f^k \in S(V),\ k \in \mathbb{N}.$$

Damit ist der Unterring $S(V)[f]$ von L in $X_0^{-N}S(V)$ enthalten, denn für $a \in S(V)[f]$ gilt

$$a = \sum_k a_k f^k = \sum_k a_k X_0^{-N} X_0^N f^k = X_0^{-N} \sum_k a_k X_0^N f^k$$

und da $a_k \in S(V)$ ist, folgt nun $\sum_k a_k X_0^N f^k \in S(V)$. $X_0^{-N}S(V)$ ist ein endlich erzeugter $S(V)$-Modul und $S(V)$ ein noetherscher Ring, also folgt nach Satz 1.1.8, dass $X_0^{-N}S(V)$ noethersch ist. Wir haben eben gezeigt, dass $S(V)[f]$ ein Untermodul von $X_0^{-N}S(V)$ ist

und daher ist nun $S(V)[f]$ endlich erzeugt. Es folgt, dass f ganz über $S(V)$ ist (siehe zum Beispiel [1]), das heißt es existieren $a_0, \ldots, a_{m-1} \in S(V)$ mit

$$f^m + a_{m-1}f^{m-1} + \ldots + a_0 = 0.$$

Daraus folgt, dass auch die homogenen Komponenten von $f^m + a_{m-1}f^{m-1} + \ldots + a_0$ alle gleich 0 sind. Weil f homogen vom Grad 0 ist, besitzt $a_j f^j,\ j = 1, \ldots, m-1$ eine homogene Komponente vom Grad 0. Da $S(V)_0 = K$ gilt, erhalten wir eine Gleichung

$$f^m + b_{m-1}f^{m-1} + \ldots + b_0 = 0,$$

mit Koeffizienten $b_0, \ldots, b_{m-1} \in K$. Also ist f algebraisch über K. K ist aber algebraisch abgeschlossen und somit folgt $f \in K$.

Zum Schluß wollen wir Aussage *iii.* beweisen. Ähnlich wie im Beweis zu Lemma 1.2.41 konstruieren wir einen Isomorphismus $\rho : K[V_i][X_i, X_i^{-1}] \to S(V)_{X_i}$. Sei $X_i^n \cdot \overline{f} \in K[V_i][X_i, X_i^{-1}]$. Dann ist $\rho\left(X_i^n \cdot \overline{f}\right) := \pi\left(X_i^n \cdot \phi_i^*(f)\right)$. Dabei ist

$$\pi : K[X_0, \ldots, X_n]_{(X_i)} \to K[X_0, \ldots, X_n]_{(X_i)}/I(V)_{(X_i)}$$

wieder die kanonische Projektion. Wir wissen nach Proposition 1.2.28, dass f genau dann ein Element von $I(V)_{X_i}$ ist, wenn $k \in \mathbb{Z}$ und $g \in I(V_i)$ existieren mit $f = X_i^k \phi_i^*(g)$. Durch eine ähnliche Rechnung wie im Beweis von Lemma 1.2.41 erkennen wir, dass ρ wohldefiniert ist. Durch eine weitere leichte Rechnung erhalten wir die Injektivität und da ϕ_i^* ein Isomorphismus ist, ist ρ auch surjektiv. Ist K ein Körper und B ein Integritätsbereich, der eine endliche erzeugte K-Algebra ist, dann ist die Dimension von B gleich dem Transzendenzgrad des Quotientenkörpers von B über K. Einen Nachweis hierfür findet man in [21]. Sei $F := \mathrm{Quot}(K[V_i])$, dann ist $F(X_i)$ der Quotientenkörper von $K[V_i][X_i, X_i^{-1}]$. Durch ρ erhalten wir $F(X_i) = \mathrm{Quot}(S(V)_{X_i})$ und $F(X_i) = \mathrm{Quot}(S(V))$. Damit erhalten wir mit Theorem 1.2.40

$$\dim S(V) = \mathrm{transgrad}(F(X_i)) = \mathrm{transgrad}(F) + 1 = \dim K[V_i] + 1 = \dim V_i + 1.$$

Nach Proposition 1.2.17 folgt

$$\dim S(V) = \sup_i \dim S(V) = \sup_i \dim V_i + 1 = \dim V + 1.$$

□

Corollar 1.2.43. *Sei V eine projektive Varietät und $V_i := U_i \cap V$. Ist $V_i \neq \emptyset$, so gilt* $\dim V_i = \dim V$.

Beweis. Dies haben wir bereits im Beweis von Theorem 1.2.42 *iv.* gezeigt. □

Definition 1.2.44. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät und $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ die Erzeugenden des Verschwindungsideals. Dann heißt V nichtsingulär in $P \in V$, wenn der Rang der Matrix

$$J = (\partial f_i/\partial x_j)_{i,j}$$

$n - \dim V$ ist. V heißt nichtsingulär, wenn V in jedem Punkt nichtsingulär ist.

Wir wollen zeigen, dass diese Definition wohldefiniert ist. Dazu wollen wir nur minimale Erzeugendensysteme von $I(V)$ betrachten. Sei also $(f_1, \ldots, f_t)$ so ein System und $P \in V$ ein beliebiger Punkt. Wir definieren die Abbildung

$$\theta : K[X_1, \ldots, X_n] \to K^n,\ f \mapsto \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P) \right).$$

Dann ist V nichtsingulär in P, wenn $(\theta(f_1), \ldots, \theta(f_t))$ ein $(n - \dim V)$-dimensionaler Untervektorraum von K^n ist. Sei nun $(g_1, \ldots, g_t)$ ein zweites minimales Erzeugendensystem von $I(V)$. Dann existiert eine invertierbare Matrix $A = (a_{ij})_{i,j},\ a_{ij} \in K[X]$, mit

$$g_i = \sum a_{ij} f_j,\ i = 1, \ldots, t.$$

Mit $f_j \in I(V)$ erhalten wir für $i = 1, \ldots, t$

$$\begin{aligned} \theta(g_i) &= \theta\left(\sum a_{ij} f_j \right) = \sum \left(\theta(a_{ij}) f_j(P) + a_{ij}(P) \theta(f_j) \right) \\ &= \sum a_{ij}(P) \theta(f_j). \end{aligned}$$

Da die Matrix $A(P) := (a_{ij}(P))_{i,j}$ invertierbar ist, folgt, dass $\theta(g_1), \ldots, \theta(g_t)$ auch ein $(n - \dim V)$-dimensionaler Unterraum ist und damit ist die Wohldefiniertheit gezeigt.

Wir benötigen noch eine andere Charakterisierung und dafür brauchen wir die folgende Definition.

Definition 1.2.45. Sei A ein noetherscher, lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper $K = A/\mathfrak{m}$. A heißt regulärer lokaler Ring, wenn $\dim_K \mathfrak{m}/\mathfrak{m}^2 = \dim A$ gilt.

Anhand der folgenden Charakterisierung können wir unsere Definition 1.2.44 auf beliebige Varietäten ausdehnen, indem wir sagen, dass eine Varietät im Punkt P nichtsingulär ist, wenn $\mathcal{O}_{V,P}$ ein regulärer lokaler Ring ist.

Satz 1.2.46. *Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät und $P \in V$ ein Punkt. Dann ist V genau dann nichtsingulär in P, wenn der lokale Ring $\mathcal{O}_{V,P}$ ein regulärer lokaler Ring ist.*

Beweis. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät und $P \in V$. Dann existieren $a_i \in K,\ i = 1, \ldots, n$, mit $P = (a_1, \ldots, a_n)$. Zu P gehört dann das maximale Ideal $\mathfrak{a}_P = (x_1 - a_1, \ldots, x_n - a_n)$ in $K[X_1, \ldots, X_n]$. Sei θ wieder gegeben durch

$$\theta : K[X_1, \ldots, X_n] \to K^n,\ f \mapsto \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P) \right).$$

Es ist $\theta(x_i - a_i) = e_i$ und somit bilden die $\theta(x_i - a_i),\ i = 1, \ldots, n$, eine Basis des K^n. Unsere Abbildung, eingeschränkt auf das Ideal $\mathfrak{a}_P$, ist demzufolge bereits surjektiv. Wir sehen, dass ein Element $g \in K[X_1, \ldots, X_n]$ unter θ genau dann auf 0 abgebildet wird,

wenn g mindestens eine doppelte Nullstelle in P hat, das heißt es gilt $\ker\theta = \mathfrak{a}_{\mathrm{P}}^2$. Wir erhalten damit einen Isomorphismus $\theta' : \mathfrak{a}_{\mathrm{P}}/\mathfrak{a}_{\mathrm{P}}^2 \to K^n$. Insbesondere gilt nun

$$\dim(\mathfrak{a}_{\mathrm{P}}/\mathfrak{a}_{\mathrm{P}}^2) = \dim(K^n) = n.$$

Sei $\{f_1, \ldots, f_l\}$ ein Erzeugendensystem von $I(V)$. Dann ist der Rang der Jacobimatrix J gleich der Dimension des Bildes von $I(V)$ unter θ. Unter Zuhilfenahme von θ' sehen wir, dass dies gleich der Dimension des Unterraumes $(I(V)+\mathfrak{a}_{\mathrm{P}})/\mathfrak{a}_{\mathrm{P}}^2$ von $\mathfrak{a}_{\mathrm{P}}/\mathfrak{a}_{\mathrm{P}}^2$ ist. Sei $\mathfrak{m}$ das maximale Ideal des lokalen Ringes $\mathcal{O}_{V,P}$. Dann gilt für $f/g \in \mathcal{O}_{V,P}$, da $1/g$ eine Einheit in $\mathcal{O}_{V,P}$ ist, dass $f/g \in \mathfrak{m}$ genau dann gilt, wenn $f \in \mathfrak{m}$. Damit können wir nachrechnen, dass $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{a}_{\mathrm{P}}/(I(V)+\mathfrak{a}_{\mathrm{P}}^2)$ gilt. Mit Hilfe der Dimensionsformel für Quotientenräume von endlichdimensionalen Vektorräumen erhalten wir dann

$$\begin{aligned}
\dim \mathfrak{m}/\mathfrak{m}^2 &= \dim \mathfrak{a}_{\mathrm{P}}/(I(V)+\mathfrak{a}_{\mathrm{P}}^2) \\
&= \dim \mathfrak{a}_{\mathrm{P}} - \dim(I(V)+\mathfrak{a}_{\mathrm{P}}^2) \\
&= n + \dim \mathfrak{a}_{\mathrm{P}}^2 - \dim(I(V)+\mathfrak{a}_{\mathrm{P}}^2) \qquad (1.4)\\
&= n + \dim \mathfrak{a}_{\mathrm{P}}^2 - \dim((I(V)+\mathfrak{a}_{\mathrm{P}}^2)/\mathfrak{a}_{\mathrm{P}}^2) - \dim \mathfrak{a}_{\mathrm{P}}^2 \\
&= n - \text{Rang } J.
\end{aligned}$$

Ist jetzt $\mathcal{O}_{V,P}$ ein regulärer, lokaler Ring, so ist $\dim \mathfrak{m}/\mathfrak{m}^2 = \dim \mathcal{O}_{V,P}$ und mit Theorem 1.2.40 und (1.4) folgt Rang $J = n - \dim V$.

Ist umgekehrt V singulär, so gilt Rang $J = n - \dim V$ und es folgt wiederum mit Theorem 1.2.40 und (1.4), dass $\dim \mathfrak{m}/\mathfrak{m}^2 = \dim V$ gilt. Damit ist $\mathcal{O}_{V,P}$ ein regulärer lokaler Ring. □

2. Vorbereitungen für die Weil-Paarung

In diesem Kapitel schlagen wir den Bogen von der Theorie aus Kapitel 1 zu den elliptischen Kurven und schaffen die Voraussetzungen für die Konstruktion der Weil-Paarung.

2.1. Elliptische Kurven als projektive Varietäten

Sei K ein beliebiger Körper und $\overline{K}$ ein fester algebraischer Abschluss von K. Unter einer Kurve verstehen wir im Folgenden eine projektive Varietät der Dimension 1.

Proposition 2.1.1. *Ist C eine Kurve und $P \in C$ ein nichtsingulärer Punkt, so ist $\mathcal{O}_{C,P}$ ein diskreter Bewertungsring.*

Beweis. Sei $V_i = V \cap U_i$, so dass $P \in V_i$ gilt. Wir erhalten mit Theorem 1.2.40 und Corollar 1.2.43

$$\dim \mathfrak{m}/\mathfrak{m}^2 = \dim \mathcal{O}_{V,P} = \dim \mathcal{O}_{V_i,P} = \dim V_i = \dim V = 1.$$

Nach Proposition 1.1.13 folgt dann, dass $\mathcal{O}_{V,P}$ ein diskreter Bewertungsring ist. □

Definition 2.1.2. Sei C eine Kurve, $P \in C$ ein nichtsingulärer Punkt und $\mathfrak{m}_{\mathrm{P}}$ das maximale Ideal von $\mathcal{O}_{C,P}$. Die Bewertung von $\mathcal{O}_{C,P}$ ist gegeben durch

$$\mathrm{ord}_P : \mathcal{O}_{C,P} \to \mathbb{N}_0 \cup \{\infty\},\ \mathrm{ord}_P(f) = \max\left\{d \in \mathbb{N}_0 : f \in \mathfrak{m}_{\mathrm{P}}^d\right\}.$$

Wir setzen $\mathrm{ord}_P(f/g) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$. Damit können wir ord_P auf $\overline{K}(C)$ fortsetzen und erhalten

$$\mathrm{ord}_P : \overline{K}(C) \to \mathbb{Z} \cup \{\infty\}.$$

Erzeugt $u \in \overline{K}(C)$ das Ideal $\mathfrak{m}_{\mathrm{P}}$, das heißt gilt $\mathrm{ord}_P(u) = 1$, so wollen wir u eine Ortsuniformisierende von C im Punkt P nennen.

Proposition 2.1.3. *Sei C eine nichtsinguläre Kurve und $f \in \overline{K}(C)$. Besitzt f keine Polstellen auf C, so folgt, dass f konstant ist.*

Beweis. Da f keine Polstellen besitzt, existieren $g, h \in \overline{K}[C]$ mit $h(P) \neq 0$ für alle $P \in C$, so dass

$$f = \frac{g}{h}$$

gilt. Daraus können wir $f \in \mathcal{O}(C)$ folgern und somit folgt nach Theorem 1.2.42, dass f konstant ist. □

Aus dieser Proposition folgt unmittelbar, indem wir $1/f$ betrachten:

Corollar 2.1.4. *Sei C eine nichtsinguläre Kurve und $f \in \overline{K}(C)$. Besitzt f keine Nullstellen auf C so folgt, dass f konstant ist.*

Definition 2.1.5. Die Gruppe der Divisoren einer Kurve C, bezeichnet mit $\mathrm{Div}(C)$, ist die freie abelsche Gruppe, die von den Punkten von C erzeugt wird. Ein Divisor $D \in \mathrm{Div}(C)$ ist also gegeben durch

$$D = \sum_{P \in C} n_P[P],\ n_P \in \mathbb{Z}.$$

Dabei gilt $n_P = 0$ bis auf endliche viele $P \in C$. Der Grad von D wird definiert durch

$$\deg(D) = \sum_{P \in C} n_P.$$

Die Divisoren vom Grad 0 bilden eine Gruppe, die wir mit $\mathrm{Div}^0(C)$ bezeichnen. Einen Divisor $D = \sum n_P[P] \in \mathrm{Div}(C)$ nennen wir positiv, bezeichnet mit $D \geq 0$, wenn $n_P \geq 0$ für alle $P \in C$ gilt. Sind $D_1, D_2 \in \mathrm{Div}(C)$ mit $D_1 - D_2 \geq 0$, so bezeichnen wir diese mit $D_1 \geq D_2$.

Sei nun C eine nichtsinguläre Kurve. Dann können wir mit Proposition 2.1.1 und Definition 2.1.5 für $f \in \overline{K}(C)^*$ den Divisor von f durch

$$\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(f)[P] \tag{2.1}$$

erklären. Diese Divisoren werden Hauptdivisoren genannt. Für den Beweis, dass es sich hierbei um eine endliche Summe handelt, sei auf [11] verwiesen.

Definition 2.1.6. Sei $D \in \mathrm{div}(C)$. Wir definieren

$$\mathscr{L}(D) := \left\{ f \in \overline{K}(C)^* : \mathrm{div}(f) \geq -D \right\} \cup \{0\}.$$

Man kann zeigen [27], dass $\mathscr{L}(D)$ ein endlich dimensionaler $\overline{K}$-Vektorraum ist und setzt

$$\ell(D) := \dim_{\overline{K}} \mathscr{L}(D).$$

Theorem 2.1.7. *(Riemann-Roch) Sei C eine nichtsinguläre Kurve, dann existieren eine ganze Zahl g, genannt das Geschlecht von C, und ein Divisor $\mathcal{K}$, so dass*

$$\ell(D) - \ell(\mathcal{K} - D) = \deg(D) - g + 1$$

für alle Divisoren $D \in Div(C)$ gilt.

Beweis. Siehe Theorem 1.3. in Kapitel IV in [11]. □

Definition 2.1.8. Eine elliptische Kurve ist ein Paar (E, O), wobei E eine nichtsinguläre Kurve vom Geschlecht 1 und $O \in E$ ein spezieller Punkt auf der Kurve ist. Die elliptische Kurve E ist definiert über K, wenn E als Kurve über K definiert ist und $O \in E(K)$ gilt.

Theorem 2.1.9. *Sei E eine elliptische Kurve definiert über K. Dann gilt*

i. Es existieren Funktionen $x, y \in K(E)$, so dass die Abbildung

$$\phi : E \to \mathbb{P}^2,\ P \mapsto \begin{cases} [x(P) : y(P) : 1] & , \text{ für } P \neq O, \\ [0 : 1 : 0] & , \text{ für } P = O, \end{cases}$$

ein Isomorphismus von E auf $\phi(E) \subseteq \mathbb{P}^2$ ist. Dabei ist $\phi(E)$ die durch die Weierstrass'sche Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.2}$$

mit $a_1, \ldots, a_6 \in K$ gegebene Kurve. Die Funktionen x, y werden Weierstrass'sche Koordinatenfunktionen von E genannt.

ii. Jede nichtsinguläre Kurve, die durch eine Weierstrass'sche Gleichung (2.2) gegeben ist, ist eine elliptische Kurve über K.

Beweis. Siehe Proposition 3.1 in [27]. □

Corollar 2.1.10. *Ist E eine elliptische Kurve definiert über K und seien x, y die Weierstrass'schen Koordinatenfunktionen. Dann gilt*

$$K(E) = K(x, y).$$

Beweis. Siehe Corollar 3.1.1 in [27]. □

2.2. Funktionen und Divisoren auf elliptischen Kurven

Im Folgenden werden wir einige grundlegende Tatsachen über elliptische Kurven voraussetzen, zum Beispiel, dass die Punkte auf einer elliptischen Kurve eine Gruppe bezüglich der Addition bilden, mit O als neutrales Element. Die Addition von zwei Punkten kann mit Hilfe expliziter Formeln ausgerechnet werden, siehe zum Beispiel [30].

Sei E eine elliptische Kurve über einem algebraisch abgeschlossenen Körper K mit char $\neq 2, 3$. Dann können wir aus (2.2) eine vereinfachte Weierstrass'sche Normalform erzeugen, das heißt E ist gegeben durch

$$Y^2 = X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3), \tag{2.3}$$

mit $A, B, e_1, e_2, e_3 \in K$. Weiter seien x, y die Weierstrass'schen Koordinatenfunktionen. Man kann leicht nachweisen, dass eine Kurve der Gestalt (2.3) genau dann nichtsingulär ist, wenn e_1, e_2 und e_3 paarweise verschieden sind. Um dieses zu prüfen, schauen wir uns die Diskriminante des Polynoms $(X - e_1)(X - e_2)(X - e_3)$ an. Durch Nachrechnen erhalten wir

$$\triangle = ((e_1 - e_2)(e_1 - e_3)(e_2 - e_3))^2 = -(4A^3 + 27B^2).$$

Gilt $4A^3 + 27B^2 \neq 0$, so ist (2.3) eine nichtsinguläre Kurve. Für elliptische Kurven folgt also aus Definition 2.1.8 also $4A^3 + 27B^2 \neq 0$. Wir wollen jetzt Funktionen auf elliptischen Kurven betrachten, dabei orientieren wir uns an [6] und [30]. Mit Hilfe von Hauptdivisoren können wir dann den Hauptsatz dieses Abschnittes formulieren.

Definition 2.2.1. Ein Polynom auf E ist ein Element des Ringes $K[x, y]$. Die Elemente von $K(E) = K(x, y)$ heißen rationale Funktionen.

Ist $f \in K[x, y]$, so existieren $v, w \in K[x]$, so dass gilt

$$f(x, y) = v(x) + yw(x). \tag{2.4}$$

Diese Darstellung existiert, denn wir können jede gerade Potenz von y durch ein Polynom in x ersetzen, sowie ungerade Potenzen von y durch y mal ein Polynom in x.

Wir wollen den Grad eines Polynoms auf E definieren. Man setzt:

$$\deg(x) := 2 \quad \text{und} \quad \deg(y) := 3.$$

Mit $\deg_x(f)$ wollen wir den Grad eines Polymons f in x bezeichnen.

Definition 2.2.2. Sei $f(x, y) = v(x) + yw(x)$ ein Polynom auf E. Wir definieren den Grad von f durch

$$\deg(f) = \max\{2\deg_x(v), 3 + 2\deg_x(w)\} \tag{2.5}$$

Weiter ist $\overline{f}$ definiert durch $\overline{f}(x, y) := v(x) - yw(x)$. Damit definieren wir nun die Norm von f durch

$$N(f) := f \cdot \overline{f}.$$

Die Norm ist nur noch ein Polynom in x und mit der Definition des Grades kann man leicht nachrechnen, dass $\deg(f) = \deg_x(N(f))$ gilt. Mit Hilfe der Norm können wir zeigen, dass die Darstellung (2.4) eindeutig ist. Gilt

$$f(x, y) = v_1(x) + yw_1(x) = v_2(x) + yw_2(x),$$

so folgt

$$g(x, y) := (v_1(x) - v_2(x)) + y(w_1(x) - w_2(x)) = 0$$

und weiter, dass ebenso

$$N(g)(x) = \underbrace{(v_1(x) - v_2(x))^2}_{=:h_1(x)} - (x^3 + Ax + B)\underbrace{(w_1(x) - w_2(x))^2}_{=:h_2(x)}$$

die Nullfunktion ist. Da aber $\deg_x(h_1(x))$ und $\deg_x(h_2(x))$ gerade sind, folgt

$$h_1(x) = 0 = h_2(x)$$

und somit $v_1(x) = v_2(x)$ und $w_1(x) = w_2(x)$. Da (2.4) eindeutig ist, folgt die wohldefiniertheit von (2.5).

Wir wollen nun prüfen, dass die uns bekannte Rechenregel bei der Gradrechnung weiterhin gültig ist.

Proposition 2.2.3. *Es seien $f, g \in K[x, y]$. Dann gilt*

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

Beweis. Es gilt

$$\begin{aligned}\deg(f \cdot g) &= \deg_x(N(f \cdot g)) = \deg_x(N(f) \cdot N(g)) \\ &= \deg_x(N(f)) + \deg_x(N(g)) = \deg(f) + \deg(g).\end{aligned}$$

□

Bei einer rationalen Funktion $f \in K(x, y)$ ist besondere Vorsicht geboten. Da es sich um Äquivalenzklassen handelt, ist es nicht möglich, zu zeigen, dass der Nenner oder der Zähler von einem bestimmen Grad ist. Gilt aber $f = g/h = u/v$, so gilt $gv = uh$ und nach unser eben bewiesenen Proposition $\deg(g) - \deg(h) = \deg(u) - \deg(v)$. Diese Differenz ist also unabhängig vom Repräsentanten der Funktion f. Mit diesem Wissen können wir nun den Wert einer rationalen Funktion in O bestimmen.

Definition 2.2.4. Sei $f = g/h \in K(x, y)$. Im Fall $\deg(g) - \deg(h) < 0$ setzen wir $f(O) = 0$. Ist $\deg(g) - \deg(h) > 0$, so hat f in O einen Pol. Gilt $\deg(g) - \deg(h) = 0$, so müssen wir eine Fallunterscheidung machen. Sind g und h in der Darstellung (2.4) gegeben, so unterscheiden wir danach, ob $N := \deg(g) = \deg(h)$ gerade oder ungerade ist. Ist N gerade, so hat g den Leitterm $a_N x^N$ und ebenso h den Term $b_N x^N$ mit $a_N, b_N \in K$. Wir setzen dann $f(O) := a_N/b_N$. Ist N ungerade, so hat g den Leitterm $a_N y x^N$ und entsprechend h den Term $b_N y x^N$ mit $a_N, b_N \in K$ und wieder setzen wir $f(O) := a_N/b_N$.

Proposition 2.2.5. *Sei $f \in K[x, y]$. Dann ist die Summe der Vielfachheiten der Nullstellen gleich dem Grad von f.*

Beweis. Sei $\deg(f) = n$ und f gegeben durch $f(x, y) = v(x) + yw(x)$. Dann gilt

$$N(f)(x) = v^2(x) - (x^3 + Ax + B)w^2(x)$$

und es folgt $\deg_x(N(f)) = \deg(f) = n$. Da K algebraisch abgeschlossen ist, existieren $c, a_1, \ldots, a_n \in K$ mit

$$N(f)(x) = c(x - a_1) \cdot \ldots \cdot (x - a_n).$$

Gilt $a_i \neq e_j,\ j = 1, 2, 3$, so hat $(x - a_i)$ zwei Nullstellen auf E. Ist hingegen $a_i = e_j$ für ein j, so hat $(x - a_i)$ nur eine Nullstelle auf E. Diese hat aber die Vielfachheit 2. Damit besitzt $N(f)$ insgesamt $2n$ Nullstellen. Da aber f und $\overline{f}$ dieselbe Anzahl von Nullstellen haben, ist also die Summe der Vielfachheiten der Nullstellen von f gleich n und damit gleich $\deg(f)$. □

Damit erhalten wir:

Corollar 2.2.6. *Eine rationale Funktion auf E hat nur endlich viele Null- und Polstellen.*

Wir wollen jetzt Divisoren auf der elliptischen Kurve E betrachten.

Definition 2.2.7. Sei $D \in \mathrm{Div}(E)$ ein Divisor mit $D = \sum_j a_j\,[P_j]$. Dann definieren wir die Summe von D durch

$$\mathrm{sum}(\sum_j a_j\,[P_j]) := \sum_j a_j P_j \in E(K).$$

Wir wollen nun die Summen-Funktion

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

etwas genauer betrachten. Da die Addition auf einer elliptischen Kurve assoziativ ist, folgt, dass sum ein Homomorphismus ist. Weiter gilt

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

Damit ergibt sich die Surjektivität der Abbildung. Es stellt sich jetzt die Frage, wie die Elemente aus dem Kern aussehen. Es wird sich zeigen, dass der Kern aus Divisoren von Funktionen, also Hauptdivisoren, besteht.

Wir erinnern kurz daran, wie der Divisor einer Funktion aussieht. Nach (2.1), ist für eine Funktion f auf E $\mathrm{div}(f)$ gegeben durch

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)[P].$$

Für elliptische Kurven ergibt sich die Endlichkeit dieser Summe aus Corollar 2.2.6. Um $\mathrm{ord}_P(f)$ berechnen zu können, benötigen wir eine Ortsuniformisierende u_P von f in P. Nach Proposition 2.1.1 existieren diese Ortsuniformisierenden a priori und die folgenden Beispiele zeigen, dass man sie konkret berechnen kann:

Beispiel 2.2.8. Es sei $f \in K(x, y)$ mit $f(x, y) = v(x) + yw(x),\ v, w \in K(x)$ und (x_0, y_0) eine Nullstelle von f mit $(x_0, y_0) \neq O$ und $y_0 \neq 0$. Es ist also

$$f(x_0, y_0) = v(x_0) + y_0 w(x_0) = 0. \tag{2.6}$$

Gilt $\overline{f}(x_0, y_0) = 0$, so ist $v(x_0) + y_0 w(x_0) = 0$ und daher folgt mit (2.6)

$$v(x_0) = 0 \quad \text{und} \quad w(x_0) = 0.$$

Dann existiert ein maximals $k \in \mathbb{N}$ mit

$$f(x, y) = (x - x_0)^k (v_1(x) + y w_1(x)).$$

Jetzt prüfen wir, ob $v_1(x) + y w_1(x)$ eine Nullstelle in (x_0, y_0) hat. Ist dies der Fall, so muss, nach der Maximalitätsbedinugung an k, $v_1(x_0) - y_0 w_1(x_0) \neq 0$ gelten. Mit

$$(v_1(x) + y w_1(x))(v_1(x) - y w_1(x)) = v_1^2(x) - y^2 w_1^2(x)$$

erhalten wir eine rationale Funktion in x, die in x_0 eine Nullstelle besitzt. Damit existiert wieder ein maximales $k_1 \in \mathbb{N}$, so dass $(x - x_0)^{k_1}$ diese rationale Funktion teilt.

Im Fall $\overline{f}(x_0, y_0) \neq 0$ berechnen wir

$$N(f) = f(x, y) \cdot \overline{f}(x, y) = v^2(x) - y^2 w^2(x)$$

und können erneut eine entsprechende Potenz von $(x - x_0)$ aus $N(f)$ und somit auch aus f ausklammern. Insgesamt sehen wir, dass im Punkt $(x_0, y_0) \neq O$ und $y_0 \neq 0$, die Funktion $(x - x_0)$ eine Ortsuniformisierende ist.

Beispiel 2.2.9. Es sei $f \in K(x, y)$ und P ein Punkt der Ordnung 2 mit $f(P) = 0$. Wir können ohne Einschränkung annehmen, dass $P = (e_1, 0)$ gilt. Weiter ist f gegeben durch $f = g/h$ mit $g(P) = 0$ und $g(x, y) = v(x) + y w(x),\ v, w \in K[x]$. Aus $g(e_1, 0) = 0$ folgt, dass $v(e_1) = 0$ gilt. Daher existiert ein Polynom v_1 mit $v(x) = (x - e_1) v_1(x)$. Da $e_i \neq e_j,\ i \neq j$ gilt, haben $(x - e_2)$ und $(x - e_3)$ keine Nullstelle in P. Damit erhalten wir

$$\begin{aligned} g(x, y) &= (x - e_1) v_1(x) + y w(x) \\ &= \frac{(x - e_2)(x - e_3)(x - e_1) v_1(x) + y \overbrace{(x - e_2)(x - e_3) w(x)}^{=: w_1(x)}}{(x - e_2)(x - e_3)} \\ &= \frac{y^2 v_1(x) + y w_1(x)}{(x - e_2)(x - e_3)} \\ &= y \frac{\overbrace{y v_1(x) + w_1(x)}^{=: g_1(x, y)}}{(x - e_2)(x - e_3)}. \end{aligned}$$

Ist $g_1(e_1, 0) = 0$, so folgt $w(e_1) = 0$ und wir können erneut eine Potenz von y ausklammern. Da wir nur Polynome betrachten, bricht dieses Verfahren nach endlich vielen Schritten ab und damit ist $u(x, y) = y$ eine Ortsuniformisierende in $P = (e_1, 0)$.

Beispiel 2.2.10. Sei wieder $f \in K(x, y)$ mit $f = g/h,\ g, h \in K[x, y]$. Wir wollen jetzt eine Ortsuniformisierende in O konstruieren. Dazu wollen wir annehmen, dass f eine

Nullstelle in O hat. Dann gilt $\deg(g) - \deg(h) = d < 0$. Da $\deg(y) - \deg(x) = 1$ ist, folgt $\deg(x^d g) = \deg(y^d h)$ und somit gilt

$$\frac{x^d g}{y^d h}(O) \neq \infty \quad \text{und} \quad \frac{x^d g}{y^d h}(O) \neq 0.$$

Damit erhalten wir

$$f = \frac{x^{-d}}{y^{-d}} \left(\frac{x^d g}{y^d h} \right) = \left(\frac{x}{y} \right)^{-d} \left(\frac{x^d g}{y^d h} \right).$$

Also ist x/y eine Ortsuniformisierende in O und es gilt $\mathrm{ord}_O(f) = -d$.

Bemerkung 2.2.11. Seien $P_1, P_2 \in E$. Dann existiert eine Funktion $g \in K(x, y)$, so dass

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \mathrm{div}(g)$$

gilt.

Dies kann man leicht einsehen. Seien $P_i = (x_i, y_i) \in E$, $i = 1, 2, 3$, Punkte auf der Geraden $ax + by + c = 0$, so hat die Funktion $f(x, y) = ax + by + c$ Nullstellen in P_1, P_2, P_3. Ist $b \neq 0$, so folgt

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

Betrachten wir die Gerade durch P_3 und $-P_3$, welche durch $x - x_3 = 0$ gegeben ist. Ihr Divisor lautet

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

Wir erhalten

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

Da $P_1 + P_2 = -P_3$ auf E gilt, ergibt sich insgesamt

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

Proposition 2.2.12. *Sei $f \in K(x, y)$. Dann gilt*

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

Beweis. Es reicht aus, die Behauptung für Polynome zu zeigen. Sei also $f \in K[x, y]$. Dann gilt nach Proposition 2.2.5

$$\sum_{P \in E - \{O\}} \mathrm{ord}_P(f) = \deg(f).$$

Nach Beispiel 2.2.10 ist $\mathrm{ord}_O(f) = -\deg f$ und wir erhalten insgesamt

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

□

Wir werden nun ein paar Hilfssätze formulieren, anhand derer es möglich ist, das Hauptergebnis dieses Abschnittes zu beweisen.

Lemma 2.2.13. *Sei t eine Unbestimmte und $P_1, P_2 \in K[t]$ ohne gemeinsame Nullstellen. Falls es vier Paare $(a_i, b_i),\ a_i, b_i \in K,\ 1 \leq i \leq 4$, gibt, die folgende Eigenschaften haben:*

i. für jedes i gilt $a_i \neq 0$ oder $b_i \neq 0$,

ii. für $i \neq j$ existiert kein $c \in K^*$ mit $(a_i, b_i) = (ca_j, cb_j)$,

iii. für $1 \leq i \leq 4$ ist $a_iP_1 + b_iP_2$ ein quadratisches Polynom,

so folgt, dass P_1 und P_2 konstant sind.

Beweis. Aus den Voraussetzungen folgt, dass die (a_i, b_i) paarweise linear unabhängig über K sind, und damit K^2 aufspannen. Wir wollen nun annehmen, dass mindestens eines der beiden Polynome P_1 und P_2 nicht konstant ist. Seien P_1 und P_2 so gewählt, dass

$$\max(\deg(P_1), \deg(P_2)) > 0$$

so klein wie möglich ist. Da P_1 und P_2 keine gemeinsamen Nullstellen haben, existiert kein $c \in K$, so dass $cP_1 = P_2$ gilt. Damit sind P_1 und P_2 linear unabhängig über K. Nach Voraussetzung *iii.* existiert $R_i \in K[t],\ 1 \leq i \leq 4$, mit

$$a_iP_1 + b_iP_2 = R_i^2,\ 1 \leq i \leq 4. \tag{2.7}$$

Für $i \neq j$ existiert kein $s \in K$ mit $R_i^2 = sR_j^2$, denn ansonsten würde folgen, dass

$$a_iP_1 + b_iP_2 - s(a_jP_1 + b_jP_2) = 0$$

gilt. Mit der linearen Unabhängigkeit von P_1 und P_2 würden wir $a_i = sa_j$ und $b_i = sb_j$ erhalten, was ein Widerspruch zu Voraussetzung *ii.* wäre. Da (a_1, b_1) und (a_2, b_2) den K^2 aufspannen, existieren für $i = 1, 2$ Konstanten $c_i, d_i \in K$ ungleich null mit

$$(a_3, b_3) = c_1(a_1, b_1) - d_1(a_2, b_2) \quad \text{und} \quad (a_4, b_4) = c_2(a_1, b_1) - d_2(a_2, b_2).$$

Damit erhalten wir

$$R_3^2 = c_1R_1^2 - d_1R_2^2,\ R_4^2 = c_2R_1^2 - d_2R_2^2.$$

Dabei gilt, dass (c_1, d_1) kein Vielfaches von (c_2, d_2) ist, denn andernfalls wäre R_3^2 ein Vielfaches von R_4^2. Weiter erhalten wir durch die lineare Unabhängigkeit von (a_1, b_1) und

(a_2, b_2), dass die Gleichung (2.7) nach P_1 und P_2 aufgelöst werden kann und damit P_1 und P_2 Linear-Kombinationen von R_1^2 und R_2^2 sind. Eine gemeinsame Nullstelle von R_1 und R_2 ist damit auch eine gemeinsame Nullstelle von P_1 und P_2. Daher besitzen R_1 und R_2 keine gemeinsamen Nullstellen. Dann besitzen auch

$$\sqrt{c_1}R_1 + \sqrt{d_1}R_2 \text{ und } \sqrt{c_1}R_1 - \sqrt{d_1}R_2$$

keine gemeinsamen Nullstellen, denn eine gemeinsame Nullstelle ist eine Nullstelle von

$$(\sqrt{c_1}R_1 + \sqrt{d_1}R_2) - (\sqrt{c_1}R_1 - \sqrt{d_1}R_2) = 2\sqrt{d_1}R_2$$

und

$$(\sqrt{c_1}R_1 + \sqrt{d_1}R_2) + (\sqrt{c_1}R_1 - \sqrt{d_1}R_2) = 2\sqrt{c_1}R_2$$

und damit also eine gemeinsame Nullstelle von R_1 und R_2. Mit

$$(\sqrt{c_1}R_1 + \sqrt{d_1}R_2)(\sqrt{c_1}R_1 - \sqrt{d_1}R_2) = c_1R_1^2 - d_1R_2^2 = R_3^2$$

folgt insgesamt, dass jeder Faktor ein Quadrat sein muss. Analog folgt, dass

$$\sqrt{c_2}R_1 + \sqrt{d_2}R_2 \text{ und } \sqrt{c_1}R_1 - \sqrt{d_1}R_2$$

quadratische Polynome sind. Wir haben jetzt Polynome R_1 und R_2, die mit den Paaren

$$(\sqrt{c_1}, \sqrt{d_1}),\ (\sqrt{c_1}, -\sqrt{d_1}),\ (\sqrt{c_2}, \sqrt{d_2}),\ (\sqrt{c_2}, -\sqrt{d_2})$$

die Bedingungen *i.* und *iii.* des Lemmas erfüllen. Wir müssen jetzt noch die Bedingung *ii.* prüfen. Da (c_1, d_1) kein Vielfaches von (c_2, d_2) ist, ist keines der ersten beiden Paare ein Vielfaches der letzten beiden. Wenn $(\sqrt{c_1}, -\sqrt{d_1})$ ein Vielfaches von $(\sqrt{c_1}, \sqrt{d_1})$ wäre, dann würde folgen, dass $c_1 = 0$ oder $d_1 = 0$ gilt. Damit würden wir aber erhalten, dass R_3^2 ein Vielfaches von R_1^2 oder R_2^2 wäre, was wie oben ausgeführt, ein Widerspruch ist. Analog folgt die lineare Unabhängigkeit von $(\sqrt{c_2}, \sqrt{d_2})$ und $(\sqrt{c_2}, -\sqrt{d_2})$. Damit sind alle Voraussetzungen des Lemmas erfüllt und wir erhalten aus der Gleichung (2.7)

$$\max(\deg(P_1), \deg(P_2)) \geq 2\max(\deg(R_1), \deg(R_2)).$$

Da R_1 und R_2 nicht konstant sind, erhalten wir einen Widerspruch zur Minimalität von $\max(\deg(P_1), \deg(P_2))$. □

Lemma 2.2.14. *Sei wieder t eine Unbestimmte. Dann existieren keine nicht konstanten, rationalen Funktionen $X(t), Y(t) \in K(t)$, so dass*

$$Y(t)^2 = X(t)^3 + AX(t) + B$$

gilt.

Beweis. Es gilt

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3),$$

mit $e_1, e_2, e_2 \in K$, wobei e_1, e_2 und e_3 paarweise verschieden sind. Damit ergibt sich

$$B = -e_1e_2e_3, \quad A = e_1e_2 + e_1e_3 + e_2e_3 \text{ und } e_1 + e_2 + e_3 = 0.$$

Wir nehmen nun an, dass $X(t), Y(t) \in K(t)$ existieren mit

$$X(t) = \frac{P_1(t)}{P_2(t)}, \quad Y(t) = \frac{Q_1(t)}{Q_2(t)}.$$

Dabei ist $P_i, Q_i \in K[t],\ i = 1, 2$. Wir interessieren uns natürlich dabei nur für den Fall, dass $X(t)$ und $Y(t)$ nicht konstant sind. Weiter dürfen wir annehmen, dass P_1 und P_2 sowie Q_1 und Q_2 keine gemeinsamen Nullstellen haben. Durch Einsetzen von $X(t)$ und $Y(t)$ in die Gleichung für E erhalten wir

$$Q_1^2(t)P_2^3(t) = Q_2^2(t)\left(P_1^3(t) + AP_1(t)P_2^2(t) + BP_2^3(t)\right).$$

Die rechte Seite ist ein Vielfaches von Q_2^2, also gilt dies auch für die linke Seite. Da aber Q_1 und Q_2 keine gemeinsamen Nullstellen besitzen, ist P_2^3 ein Vielfaches von Q_2^2. Jede gemeinsame Nullstelle von P_2 und $P_1^3 + AP_1P_2^2 + BP_2^3$ ist auch eine Nullstelle von P_1. Da aber P_1 und P_2 keine gemeinsamen Nullstellen besitzen, kann eine solche Nullstelle nicht existieren. Daraus folgt, dass Q_2^2 ein Vielfaches von P_2^3 ist. Insgesamt existiert eine Konstante $c \in K$ mit $cP_2^3 = Q_2^2$ und damit können wir nach einigen Anpassungen annehmen, dass

$$P_2^3 = Q_2^2$$

gilt. Nun können wir also kürzen und erhalten

$$\begin{aligned} Q_1^2 &= P_1^3 + AP_1P_2^2 + BP_2^3 = P_1^3 + (e_1e_2 + e_1e_3 + e_2e_3)P_1P_2^2 - e_1e_2e_3P_2^3 \\ &= (P_1 - e_1P_2)(P_1 - e_2P_2)(P_1 - e_3P_2). \end{aligned}$$

Wenn wir nun annehmen, dass für $P_1 - e_iP_2$ und $P_1 - e_jP_2$ für $i \neq j$ eine gemeinsame Nullstelle t_0 existiert, dann ist t_0 auch Nullstelle von

$$e_j(P_1 - e_iP_2) - e_i(P_1 - e_jP_2) = (e_j - e_i)P_1$$

und

$$(P_1 - e_iP_2) - (P_1 - e_jP_2) = (e_j - e_i)P_2.$$

Da $e_j - e_i \neq 0$ ergibt sich, dass t_0 eine gemeinsame Nullstelle von P_1 und P_2 ist, was ein Widerspruch zur Voraussetzung ist. Also haben $P_1 - e_iP_2$ und $P_1 - e_jP_2$ für $i \neq j$ keine gemeinsamen Nullstellen. Das Produkt

$$(P_1 - e_1P_2)(P_1 - e_2P_2)(P_1 - e_3P_2)$$

ist ein Quadrat eines Polynoms. Weil wir eben festgestellt haben, dass die einzelnen Faktoren keine gemeinsamen Nullstellen haben, ergibt sich damit, dass jeder Faktor das

Produkt von einem Quadrat eines Polynoms mit einer Konstanten ist. In K ist jede Konstante ein Quadrat und daher folgt insgesamt, dass alle Faktoren das Quadrat eines Polynoms sind. Wegen $P_2^3 = Q_2^2$ ist auch P_2 das Quadrat eines Polynoms. Wir haben jetzt also Polynome P_1 und P_2 und vier Paare

$$(1, -e_1),\ (1, -e_2),\ (1, -e_3),\ (0, 1),$$

die die Bedingungen von Lemma 2.2.13 erfüllen. Es folgt, dass P_1 und P_2 konstant sind. Also ist auch $X(t) = \frac{P_1(t)}{P_2(t)}$ konstant, was ein Widerspruch zur unserer Annahme ist. □

Lemma 2.2.15. *Seien $P, Q \in E$ und existiere eine Funktion h auf E mit*

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

so folgt, dass $P = Q$ gilt.

Beweis. Wir nehmen an, dass $P \neq Q$ gilt. Dann hat die Funktion $h - c$ für alle $c \in K$ eine einfache Polstelle in Q. Nach Proposition 2.2.12, besitzt $h - c$ dann genau eine einfache Nullstelle. Sei $f \in K(x, y)$ beliebig. Hat f keine Null- oder Polstelle in Q, so definieren wir

$$g(x, y) := \prod_{R \in E} \left(h(x, y) - h(R)\right)^{\mathrm{ord}_R(f)}.$$

Jeder Faktor dieses Produktes hat eine Null- oder Polstelle in Q der Ordnung $\mathrm{ord}_R(f)$. Da nach Proposition 2.2.12 $\sum_R \mathrm{ord}_R(f) = 0$ gilt, haben g und f denselben Divisor. Nach Proposition 2.1.3 folgt, dass f/g konstant ist und damit ist f eine rationale Funktion in h. Hat f eine Pol- oder Nullstelle in Q, so hat $f \cdot h^{\mathrm{ord}_Q(f)}$ keine Pol- oder Nullstellen mehr in Q und wir können erneut folgern, dass $f \cdot h^{\mathrm{ord}_Q(f)}$ eine rationale Funktion in h ist und damit gilt dies auch für f. Damit sind alle Funktionen rationale Funktionen in h. Insbesondere gilt dies auch für x und y, was ein Widerspruch zu Lemma 2.2.14 ist. □

Theorem 2.2.16. *Sei E eine elliptische Kurve und D ein Divisor auf E mit* $\deg(D) = 0$. *Genau dann existiert eine Funktion f auf E mit*

$$\mathrm{div}(f) = D,$$

wenn

$$\mathrm{sum}(D) = O$$

gilt.

Beweis. Sei $D = \sum_j a_j[P_j] \in Div(E)$ mit $\deg(D) = 0$ beliebig. Nach Bemerkung 2.2.11 existiert eine Funktion $g \in K(x, y)$, so dass für $P_1, P_2 \in E$

$$[P_1] + [P_1] = [P_1 + P_2] + [O] + \mathrm{div}(g)$$

gilt. Weiter folgt

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

Wir setzen $D^+ := \sum_{a_j>0} a_j[P_j]$ und $P := \sum_{a_j>0} a_j P_j$. Dann existiert $k \in \mathbb{N}$ und eine Funktion $g_1 \in K(x,y)$ mit

$$D^+ = [P] + k[O] + \operatorname{div}(g_1)$$

Analog erhalten wir ein ähnliches Ergebnis für $D^- := \sum_{a_j<0} a_j[P_j]$. Insgesamt existieren also $P, Q \in E, n \in \mathbb{N}$ und $g_2 \in K(x,y)$ mit

$$D = [P] - [Q] + n[O] + \operatorname{div}(g_2).$$

Da g_2 der Quotient von Produkten von Funktionen h mit $\operatorname{sum}(\operatorname{div}(h)) = O$ ist, folgt auch $\operatorname{sum}(\operatorname{div}(g_2)) = O$. Nach Proposition 2.2.12 gilt $\deg(\operatorname{div}(g_2)) = 0$ und damit erhalten wir

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

und somit

$$D = [P] - [Q] + \operatorname{div}(g_2).$$

Daraus können wir

$$\operatorname{sum}(D) = P - Q + \operatorname{sum}(\operatorname{div}(g_2)) = P - Q$$

folgern.

Nehmen wir an, dass $\operatorname{sum}(D) = O$ gilt. Damit folgt $P - Q = O$, woraus sich $P = Q$ ergibt und somit $D = \operatorname{div}(g_2)$ ist.

Gilt nun, dass eine Funktion $f \in K(x,y)$ existiert mit $D = \operatorname{div}(f)$, so erhalten wir

$$[P] - [Q] = \operatorname{div}(f/g_2).$$

Nach Lemma 2.2.15 folgt $P = Q$. Also gilt $\operatorname{sum}(D) = O$. □

3. Die Weil-Paarung

3.1. Konstruktion der Weil-Paarung

Sei K ein beliebiger Körper mit $\operatorname{char} K \neq 2, 3$. Sei E eine elliptische Kurve in vereinfachter Weierstrass-Normalform $Y^2 = X^3 + AX + B$ mit $A, B \in K$ über dem Körper K.

Ein Endomorphismus auf E ist ein Homomorphismus $\alpha : E(\overline{K}) \to E(\overline{K})$, der durch rationale Funktionen gegeben ist. Da α ein Endomorphismus ist gilt:

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y).$$

Daraus folgt, es existieren rationale Funktionen r_1, r_2, so dass der Endomorphismus α gegeben ist durch:

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

Ein Endomorphismus heißt separabel, wenn $r_1 \not\equiv 0$ gilt.

Definition 3.1.1. Sei $n \in \mathbb{N}$. Die n-Teilungsspunkte der elliptischen Kurve E, die wir mit $E[n]$ bezeichnen, sind definiert durch

$$E[n] := \left\{ P \in E(\overline{K}) : nP = O \right\}.$$

Wird n nicht von der Charakteristik von K geteilt, so gilt, siehe [30],

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

Es gibt dann n^2 Punkte der Ordnung n. Für den Fall, dass n von $\operatorname{char} K = p$ geteilt wird, schreiben wir $n = p^r n'$ mit $p \nmid n'$. In diesem Fall gilt

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

Wir wollen die natürliche Zahl $n > 1$ im weiteren Verlauf so wählen, dass n nicht von der Charakteristik des Körpers K geteilt wird. Weiter soll für die elliptische Kurve E

$$E[n] \subseteq E(K) \tag{3.1}$$

gelten. Wir wollen eine Abbildung e_n konstruieren, die auf den n-Teilungspunkten der Kurve operiert und in die n-ten Einheitswurzeln abbildet. Gesucht ist demnach

$$e_n : E[n] \times E[n] \to \mu_n.$$

Dabei bezeichne μ_n die n-ten Einheitswurzeln in $\overline{K}$. Wir werden feststellen, dass mit Hilfe von e_n und der Eigenschaft (3.1) gezeigt werden kann, dass sogar

$$\mu_n \subseteq K$$

gilt.

Wir wollen uns zuerst mit der Konstruktion der Paarung e_n beschäftigen. Dazu sei $T \in E[n]$. Wir definieren einen Divisor D durch $D := n\,[T] - n\,[O]$. Es gilt $\deg D = 0$ und $\operatorname{sum} D = O$. Damit existiert nach Theorem 2.2.16 eine Funktion f auf E mit

$$\operatorname{div}(f) = n\,[T] - n\,[O]\,. \tag{3.2}$$

Wir wählen zusätzlich einen Punkt $T' \in E\big[n^2\big]$ mit $nT' = T$. Der Punkt T' existiert, da das Multiplizieren mit n ein surjektiver Endomorphismus auf der elliptischen Kurve ist. Weiter definieren wir jetzt einen zweiten Divisor D' durch

$$D' = \sum_{R \in E[n]} \big(\big[T' + R\big] - [R]\big)\,.$$

Gesucht ist wiederum eine Funktion g auf der elliptischen Kurve mit $\operatorname{div}(g) = D'$. Da wir erneut Theorem 2.2.16 anwenden wollen, müssen wir zeigen, dass $\operatorname{sum} D' = O$ und $\deg(D') = 0$ gilt. In $E[n]$ gibt es n^2 Punkte. Damit erhalten wir:

$$\operatorname{sum} D' = \sum_{R \in E[n]} T' + R - R = \sum_{R \in E[n]} T' = n^2 T' = O.$$

Offensichtlich gilt $\deg(D') = 0$, also existiert eine Funktion g mit

$$\operatorname{div}(g) = \sum_{R \in E[n]} \big(\big[T' + R\big] - [R]\big)\,.$$

Es stellt sich die Frage, inwiefern die Funktion g von der Wahl des Punktes T' abhängt. Sei also $T'' \in E\big[n^2\big]$ mit $nT'' = T = nT'$. Dann existiert $S \in E[n]$ mit $T'' = T' + S$, das heißt, die Funktion g hat Nullstellen in allen Punkten T'', für die $nT'' = T$ gilt. Damit hängt g nicht von der Wahl des Punktes T' ab.

Wir bezeichnen im weiteren Verlauf mit $f \circ n$ diejenige Funktion, die erst einen Punkt mit n multipliziert und dann f darauf anwendet. Für $R \in E[n]$ sind die Punkte der Form $P = T' + R$ diejenigen Punkte mit $nP = T$. Damit können wir nun $\operatorname{div}(f \circ n)$ bestimmen. Aus (3.2) erhalten wir

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

Nach Proposition 2.1.3 folgt, dass $f \circ n$ ein konstantes Vielfaches von g^n ist. Wenn wir f mit einer geeigneten Konstanten mulitplizieren, können wir davon ausgehen, dass

$$f \circ n = g^n$$

gilt. Sei $S \in E[n]$ und $P \in E(\overline{K})$, dann gilt:

$$g^n(P+S) = (f \circ n)(P+S) = f(n(P+S)) = f(n(P)) = g^n(P). \tag{3.3}$$

Daraus folgt, dass $g(P+S)/g(P)$ eine n-te Einheitswurzel ist. Wir können nun mit der Funktion g die Funktion e_n definieren.

Definition 3.1.2. Sei $S, T \in E[n]$ und g die oben konstruierte Funktion auf der elliptischen Kurve. Dann ist die Weil-Paarung e_n definiert durch

$$e_n(S,T) := \frac{g(P+S)}{g(P)}, \tag{3.4}$$

wobei $P \in E(\overline{K})$ beliebig wählbar ist.

Proposition 3.1.3. *Die Weil-Paarung ist wohldefiniert.*

Beweis. Wir müssen zeigen, dass $g(P+S)/g(P)$ für alle $P \in E(\overline{K})$ konstant ist. Mit τ_S bezeichnen wir die Translation mit S. Aus (3.3) folgt $\operatorname{div}((g \circ \tau_S)^n) = \operatorname{div}(g^n)$ und daraus erhalten wir $\operatorname{div}(g \circ \tau_S) = \operatorname{div}(g)$. Damit können wir aus Proposition 2.1.3 folgern, dass $(g \circ \tau_S)/g$ konstant ist. □

3.2. Die Eigenschaften der Weil-Paarung

Bevor wir uns mit den Beweisen der Eigenschaften der Weil-Paarung beschäftigen können, benötigen wir ein weiteres Lemma.

Lemma 3.2.1. *Sei $f(x,y)$ eine Funktion von E nach $\overline{K} \cup \{\infty\}$ und $n \in \mathbb{N}$, so dass n nicht von der Charakteristik des Körpers K geteilt wird. Gilt für alle $P \in E(\overline{K})$ und $T \in E[n]$*

$$f(P+T) = f(P),$$

so existiert eine Funktion h auf E mit

$$f(P) = h(nP),\ P \in E(\overline{K}).$$

Beweis. Im Fall $n = 1$ setzen wir $h := f$. Sei also im weiteren Verlauf $n > 1$. Sei $T \in E[n]$. Für $(x,y) \in E(\overline{K})$ existieren dann rationale Funktionen $R_T(x,y)$ und $S_T(x,y)$ mit

$$(x,y) + T = (R_T(x,y), S_T(x,y)).$$

Da $(R_T, S_T) \in E(\overline{K})$ gilt, ist die Abbildung

$$\begin{aligned} \sigma_T :\ \overline{K}(x,y) &\to \overline{K}(x,y), \\ f(x,y) &\mapsto f(R_T, S_T) \end{aligned}$$

ein Endomorphismus auf $\overline{K}(x,y)$. σ_T ist sogar ein Automorphismus, denn die Umkehrabbildung ist durch σ_{-T} gegeben. Falls $T \neq T',\ T' \in E[n]$, gilt, ist

$$(x,y) + T \neq (x,y) + T'$$

und damit $\sigma_T \neq \sigma_{T'}$. Da $E[n]$ n^2 Elemente besitzt, bekommen wir also n^2 verschiedene Automorphismen σ_T auf $\overline{K}(x,y)$. Aus der Galoistheorie wissen wir, ist G eine Gruppe von Automorphismen eines Körpers L, so gilt $[L:F] = |G|$ für den Fixkörper F von G. In unserem Fall besteht der Fixkörper F unserer Automorphismen σ_T gerade aus den Funktionen mit der Eigenschaft

$$f(P+T) = f(P),\ P \in E(\overline{K}),\ T \in E[n]$$

und es gilt

$$[\overline{K}(x,y) : F] = n^2. \tag{3.5}$$

Die Multiplikation mit n sei gegeben durch $n(x,y) = (g_n(x), yh_n(x))$ mit rationalen Funktionen g_n und h_n. Diese Einschränkung können wir machen, indem wir feststellen, dass wir gerade Potenzen von y durch eine Potenz von $x^3 + Ax + B$ ersetzen können und dass $n(x,-y) = n(-(x,y)) = -n(x,y)$ gilt. Da $n(x,y)$ ein Endomorphismus und $T \in E[n]$ ist, gilt

$$\overline{K}(g_n(x), yh_n(x)) \subseteq F,$$

das heißt

$$[F : \overline{K}(g_n(x), yh_n(x))] \geq 1. \tag{3.6}$$

Weiter ist

$$[\overline{K}(g_n(x), yh_n(x)) : \overline{K}(g_n(x))] \geq 2, \tag{3.7}$$

denn $yh_n \notin \overline{K}(g_n(x))$. Wir erhalten jetzt mit (3.5), (3.6), (3.7) und dem Gradsatz

$$[\overline{K}(x,y) : \overline{K}(g_n(x))] \geq 2n^2.$$

Aus Theorem B.3 und Lemma B.2 wissen wir, dass

$$g_n(x) = \frac{\phi_n(x)}{\psi_n^2(x)}$$

und

$$\phi_n(X) = X^{n^2} + \ldots,\ \psi_n^2(X) = n^2 X^{n^2-1} + \ldots$$

gilt. Also ist $X = x$ eine Nullstelle des Polynoms

$$P(X) = \phi_n(X) - g_n(x)\psi_n^2(X) \in \overline{K}(g_n(x))[X]$$

und damit ist x höchstens vom Grad n^2 über $\overline{K}(g_n(x))$, das heißt

$$[\overline{K}(x) : \overline{K}(g_n(x))] \leq n^2.$$

Da

$$[\overline{K}(x,y) : \overline{K}(x)] = 2$$

gilt, erhalten wir mit dem Gradsatz

$$[\overline{K}(x,y) : \overline{K}(g_n(x))] \leq 2n^2$$

und damit insgesamt

$$F = \overline{K}(g_n(x), yh_n(y)).$$

Auf der linken Seite stehen nun die Funktionen, die invariant unter der Translation mit Elementen aus $E[n]$ sind und auf der rechten Seite diejenigen von der Form $h(n(x,y))$, womit unsere Behauptung bewiesen ist. □

Theorem 3.2.2. *Sei E eine elliptische Kurve über einem Körper K und $n \in \mathbb{N}$, so dass n nicht von der Charakteristik des Körpers K geteilt wird. Dann besitzt die Weil-Paarung*

$$e_n : E[n] \times E[n] \to \mu_n$$

folgende Eigenschaften:

i. e_n *ist linear in beiden Variablen. Es gilt also für* $S, T, S_i, T_i \in E[n]\,, i = 1, 2$

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

und

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$

ii. e_n *ist nicht entartet in beiden Variablen, das heißt gilt für* $S \in E[n]$ *beliebig* $e_n(S,T) = 1$ *für alle* $T \in E[n]\,$, *so folgt* $S = O$. *Ebenso gilt, ist* $T \in E[n]$ *beliebig und* $e_n(S,T) = 1$ *für alle* $S \in E[n]$ *dann folgt* $T = O$.

iii. $e_n(T,T) = 1,\ T \in E[n]$.

iv. $e_n(S,T) = e_n(T,S)^{-1},\ S,T \in E[n]$.

v. Ist σ ein Automorphismus auf $\overline{K}$ und außerdem die Identität auf den Koeffizienten von E, so gilt

$$e_n(\sigma S, \sigma T) = \sigma(e_n(S,T)).$$

vi. Ist α ein separabler Endomorphismus auf E, so gilt

$$e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{\deg \alpha}.$$

Liegen die Koeffizienten von E in einem endlichen Körper, so gilt diese Eigenschaft auch für den Frobenius Endomorphismus.

Beweis. i. Seien $S_1, S_2, T \in E[n]$ und $P \in E(\overline{K})$ beliebig. Nach Proposition 3.1.3 ist e_n unabhängig von der Wahl des Punktes P. Wir benutzen also (3.4) mit P und $P + S_1$. Damit erhalten wir

$$\begin{aligned} e_n(S_1, T)e_n(S_2, T) &= \frac{g(P + S_1)}{g(P)} \frac{g(P + S_1 + S_2)}{g(P + S_1)} \\ &= \frac{g(P + S_1 + S_2)}{g(P)} \\ &= e_n(S_1 + S_2, T). \end{aligned}$$

Um die Linearität in der zweiten Variablen zu beweisen, sei nun $S \in E[n]$ beliebig und $T_1, T_2, T_3 \in E[n]$ mit $T_1 + T_2 = T_3$. Für $i = 1, 2, 3$ bezeichnen f_i und g_i diejenigen Funktionen, die gebraucht werden, um $e_n(S, T_i)$ zu definieren. Es gilt

$$\operatorname{div}(f_i) = n\,[T_i] - n\,[O]\,,\ i = 1, 2, 3.$$

Weiter ist $\operatorname{sum}([T_3] - [T_1] - [T_2] + [O]) = T_3 - (T_1 + T_2) = O$ und daher existiert nach Theorem 2.2.16 eine Funktion h mit

$$\operatorname{div}(h) = [T_3] - [T_1] - [T_2] + [O]\,.$$

Damit erhalten wir nun

$$\begin{aligned} \operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) &= n\,[T_3] - n\,[O] - (n\,[T_1] + n\,[T_2] - 2n\,[O]) \\ &= n\,([T_3] - [T_1] - [T_2] + [O]) \\ &= n\,\operatorname{div}(h) = \operatorname{div}(h^n). \end{aligned}$$

Es existiert also eine Konstante $c \in \overline{K}, c \neq 0$, mit

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

Einsetzen liefert

$$\begin{aligned} g_3^n &= f_3 \circ n = (c f_1 f_2 h^n) \circ n \\ &= c\,((f_1 \circ n)\,(f_2 \circ n)\,(h^n \circ n)) \\ &= c\,(g_1^n g_2^n\,(h^n \circ n))\,. \end{aligned}$$

Also gilt

$$g_3 = c^{1/n} g_1 g_2\,(h \circ n)\,.$$

Wir setzen nun diese Gestalt von g_3 in die Definition von e_n ein und bekommen, da $S \in E[n]$,

$$\begin{aligned} e_n(S, T_1 + T_2) = \frac{g_3(P + S)}{g_3(P)} &= \frac{c^{1/n} g_1(P + S) g_2(P + S) h(n(P + S))}{c^{1/n} g_1(P) g_2(P) h(n(P))} \\ &= \frac{g_1(P + S)}{g_1(P)} \frac{g_2(P + S)}{g_2(P)} \\ &= e_n(S, T_1)e_n(S, T_2). \end{aligned}$$

Damit haben wir die Linearität in beiden Variablen gezeigt.

ii. Sei $T \in E[n]$, so dass gilt

$$e_n(S,T) = 1,\ S \in E[n]\,.$$

Es folgt mit der Definition der Weil-Paarung, dass

$$g(P+S) = g(P),\ P \in E(\overline{K}), S \in E[n]$$

gilt. Nun können wir Lemma 3.2.1 anwenden und erhalten eine Funktion h mit $g = h \circ n$. Dann ist

$$(h \circ n)^n = g^n = f \circ n.$$

Da die Multiplikation mit n ein surjektiver Endomorphismus auf E ist, gilt $h^n = f$. Daraus folgt dann

$$\operatorname{div}(h^n) = n \operatorname{div}(h) = \operatorname{div}(f) = n\,[T] - n\,[O]\,.$$

Also ist $\operatorname{div}(h) = [T] - [O]$. Mit Theorem 2.2.16 folgt nun, dass $T = O$ gilt. Womit wir gezeigt haben, dass e_n nicht entartet in der zweiten Variable ist. Mit Hilfe der Eigenschaft *iv.* und der eben bewiesenen Eigenschaft folgt, dass e_n nicht entartet ist in der ersten Variable. Existiert nämlich ein $S \in E[n]$ mit $e_n(S,T) = 1,\ T \in E[n]$, so gilt

$$1 = e_n(S,T)^{-1} = e_n(T,S),$$

woraus $S = O$ folgt.

iii. Sei $T \in E[n]$ beliebig. Wir definieren für $j \in \mathbb{N}_0$ die Abbildung

$$\tau_{jT} : E(\overline{K}) \to E(\overline{K}),\ P \mapsto P + jT.$$

Damit ist die Abbildung $f \circ \tau_{jT}$ gegeben durch $P \mapsto f(P + jT)$ und der Divisor von $f \circ \tau_{jT}$ ergibt sich zu $n\,[T - jT] - n\,[-jT]$. Weiter ist

$$\begin{aligned}
\operatorname{div}(\prod_{j=0}^{n-1} (f \circ \tau_{jT})) &= \sum_{j=0}^{n-1} (n\,[T - jT] - n\,[-jT]) \\
&= \sum_{j=0}^{n-1} ([(1-j)T] - n\,[-jT]) \\
&= n\,[T] - n\,[-nT + T] \\
&= n\,[T] - n\,[T] \\
&= 0.
\end{aligned}$$

Nach Proposition 2.1.3 ist $\prod_{j=0}^{n-1}(f \circ \tau_{jT})$ konstant. Wir wählen nun einen weiteren Punkt $T' \in E\left[n^2\right]$ mit $nT' = T$. Es gilt

$$\begin{aligned}\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n &= \prod_{j=0}^{n-1}(g^n \circ \tau_{jT'}) \\ &= \prod_{j=0}^{n-1}(f \circ n \circ \tau_{jT'}) \\ &= \prod_{j=0}^{n-1}(f \circ \tau_{jT}).\end{aligned}$$

Also ist $\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n$ konstant und es gilt

$$0 = \operatorname{div}\left(\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n\right) = n \operatorname{div}\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right).$$

Daraus folgt $\operatorname{div}\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right) = 0$ und somit ist $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ konstant. Also nimmt sie an den Punkten P und $P + T'$ denselben Wert an, das heißt es gilt

$$\prod_{j=0}^{n-1} g(P + T' + jT') = \prod_{j=0}^{n-1} g(P + jT').$$

Dabei wählen wir den Punkt $P \in E(\overline{K})$ so, dass alle Faktoren endlich und von 0 verschieden sind. Wie oben können wir nun die meisten Terme kürzen und übrig bleibt

$$g(P + nT') = g(P).$$

Mit $nT' = T$ können wir schließen, dass

$$e_n(T, T) = \frac{g(P + T)}{g(P)} = 1$$

gilt.

iv. Seien $S, T \in E[n]$, dann folgt mit *i*. und *iii*.

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

Damit ist $e_n(T, S) = e_n(S, T)^{-1}$.

v. Sei σ ein Automorphismus auf $\overline{K}$, der die Koeffizienten von E fest lässt. Mit f^σ und g^σ bezeichnen wir diejenigen Funktionen, die aus f und g durch Anwenden von σ auf

ihre Koeffizienten hervorgehen. Da σ die Identität auf den Koeffizienten von E ist, folgt aus $T \in E(\overline{K})$ auch $\sigma T \in E(\overline{K})$. Ebenso ist für $T \in E[n]$ auch $\sigma T \in E[n]$. Dann gilt

$$\operatorname{div}(f^\sigma) = n[\sigma T] - n[O]$$

und

$$\sigma(g(P)) = g^\sigma(\sigma P),\ P \in E(\overline{K}).$$

Damit erhalten wir

$$\sigma(e_n(S,T)) = \sigma\left(\frac{g(P+S)}{g(P)}\right) = \frac{g^\sigma(\sigma P + \sigma S)}{g^\sigma(\sigma P)} = e_n(\sigma S, \sigma T),\ S,T \in E(\overline{K}).$$

vi. Sei $S,T \in E[n]$ und α ein separabler Endomorphismus auf E, dessen Kern gegeben sei durch $\ker(\alpha) = \{Q_1, \ldots, Q_k\}$, $Q_i \in E(\overline{K})$, $i = 1, \ldots, k$. Da α separabel ist, gilt nach Proposition A.1 $\deg \alpha = k$. Mit f_t und $f_{\alpha(T)}$ wollen wir diejenigen Funktionen bezeichnen, die gegeben sind durch

$$\operatorname{div}(f_T) = n\,[T] - n\,[O]\,,\quad \operatorname{div}(f_{\alpha(T)}) = n\,[\alpha(T)] - n\,[O]\,.$$

Damit erhalten wir zwei Funktionen g_T und $g_{\alpha(T)}$, für die gilt

$$g_T^n = f_T \circ n,\quad g_{\alpha(T)}^n = f_{\alpha(T)}^n \circ n.$$

Wie in *iii.* wollen wir mit τ_Q die Translation mit Q bezeichnen. Es folgt

$$\operatorname{div}\left(f_T \circ \tau_{-Q_i}\right) = n\,[T + Q_i] - n\,[Q_i]\,.$$

Wir erhalten dann

$$\begin{aligned}
\operatorname{div}\left(f_{\alpha(T)} \circ \alpha\right) &= n \cdot \sum_{\alpha(T'')=\alpha(T)} \left[T''\right] - n \cdot \sum_{\alpha(Q)=O} [Q] \\
&= n \sum_{i=1}^{k} \left([T+Q_i] - [Q_i]\right) \\
&= \operatorname{div}\left(\prod_{i=1}^{k} (f_T \circ \tau_{-Q_i})\right).
\end{aligned}$$

Für jedes i wählen wir jetzt ein $Q_i' \in E(\overline{K})$ mit $nQ_i' = Q_i$. Dann ist

$$g_T(P - Q_i')^n = (f_T \circ n)(P - Q_i') = f_T(nP - Q_i).$$

Damit ist

$$\begin{aligned}
\operatorname{div}\left(\prod_{i=1}^{k} (g_T \circ \tau_{-Q_i'})^n\right) &= \operatorname{div}\left(\prod_{i=1}^{k} f_T \circ \tau_{-Q_i} \circ n\right) \\
&= \operatorname{div}(f_{\alpha(T)} \circ \alpha \circ n) \\
&= \operatorname{div}(f_{\alpha(T)} \circ n \circ \alpha) \\
&= \operatorname{div}(g_{\alpha(T)}^n \circ \alpha) \\
&= \operatorname{div}(g_{\alpha(T)} \circ \alpha)^n.
\end{aligned}$$

Also haben auch $\prod_{i=1}^{k}(g_T \circ \tau_{-Q_i'})$ und $g_{\alpha(T)} \circ \alpha$ denselben Divisor und daraus folgt, dass ein $c \in \overline{K}^*$ existiert mit $c\left(\prod_{i=1}^{k} g_T \circ \tau_{-Q_i'}\right) = (g_{\alpha(T)} \circ \alpha)$. Durch Einsetzen in die Definition der Weil-Paarung erhalten wir

$$\begin{aligned} e_n(\alpha(S), \alpha(T)) &= \frac{g_{\alpha(T)}(\alpha(P) + \alpha(S))}{g_{\alpha(T)}(\alpha(P))} = \frac{g_{\alpha(T)}(\alpha(P+S))}{g_{\alpha(T)}(\alpha(P))} \\ &= \frac{c\left(\prod_{i=1}^{k} g_T(P + S - Q_i')\right)}{c\left(\prod_{i=1}^{k} g_T(P - Q_i')\right)} \\ &= \prod_{i=1}^{k} \frac{g_T(P - Q_i' + S)}{g_T(P - Q_i')} = \prod_{i=1}^{k} e_n(T, S) \\ &= e_n(T, S)^k \\ &= e_n(T, S)^{\deg \alpha}. \end{aligned}$$

Sei jetzt E eine elliptische Kurve über dem Körper $\mathbb{F}_q$. Dann erfüllt der Frobenius-Endomorphismus ϕ_q die Voraussetzungen von $v.$ und damit ist

$$e_n(\phi_q(S), \phi_q(T)) = \phi_q(e_n(S, T)) = e_n(S, T)^q.$$

Da $\deg \phi_q = q$ gitl, haben wir insgesamt die Behauptung bewiesen. □

Bemerkung.

- Ist E in der vereinfachten Weierstrass'schen Normalform gegeben, so bedeutet die Bedingung an den Automorphismus σ in $v.$, dass $\sigma A = A$ und $\sigma B = B$ gilt.
- Die Eigenschaft $vi.$ gilt auch für nicht separable Endomorphismen, siehe [9].

Mit Hilfe der Weil-Paarung ist es uns jetzt möglich, die am Anfang des Kapitels aufgestellte Behauptung, nämlich dass aus der Voraussetzung (3.1) folgt, dass $\mu_n \subseteq K$ gilt, zu beweisen. Vorher benötigen wir jedoch das folgende Corollar.

Corollar 3.2.3. *Ist $\{T_1, T_2\}$ eine Basis von $E[n]$, so folgt, dass $e_n(T_1, T_2)$ eine primitive n-te Einheitswurzel ist.*

Beweis. Sei $\{T_1, T_2\}$ eine Basis von $E[n]$ und $e_n(T_1, T_2) := \zeta$ mit $\zeta^d = 1$. Mit Hilfe der Eigenschaften der Weil-Paarung folgt

$$1 = e_n(T_1, T_2)^d = e_n(T_1, dT_2)$$

und

$$1 = e_n(T_2, T_2)^d = e_n(T_2, dT_2).$$

Weiter sei $S \in E[n]$ beliebig. Dann existieren $a, b \in \mathbb{Z}$ mit $S = aT_1 + bT_2$. Wir erhalten damit

$$\begin{aligned} e_n(S, dT_2) &= e_n(aT_1 + bT_2, dT_2) = e_n(aT_1, dT_2)e_n(bT_2, dT_2) \\ &= e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1. \end{aligned}$$

Da S beliebig war, folgt mit der Eigenschaft *ii.* der Weil-Paarung $dT_2 = O$. Es folgt nun, dass ζ eine primitive n-te Einheitswurzel ist, denn da T_2 ein Basiselement von $E[n]$ ist, gilt genau dann $dT_2 = O$, wenn d von n geteilt wird. □

Corollar 3.2.4. *Gilt $E[n] \subseteq E(K)$, so folgt $\mu_n \subseteq K$.*

Beweis. Sei σ ein beliebiger Automorphismus auf $\overline{K}$ mit der Eigenschaft, dass σ die Identität auf K ist und $\{T_1, T_2\}$ eine Basis von $E[n]$ mit $e_n(T_1, T_2) = \zeta$. Nach Voraussetzung gilt $T_1, T_2 \in E(K)$ und daher folgt $\sigma T_1 = T_1$ und $\sigma T_2 = T_2$. Mit der Eigenschaft *v.* der Weil-Paarung erhalten wir

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

ζ liegt also im Fixkörper und damit in einer rein inseparablen Körpererweiterung von K. Da die Charakteristik von K aber nicht n teilt, ist ζ separabel. Daraus folgt, dass ζ schon im Körper K liegen muss. Da nach Corollar 3.2.3 ζ eine primitive n-te Einheitswurzel ist, folgt nun die Behauptung. □

3.3. Berechnung der Weil-Paarung

Die Weil-Paarung ist in der Darstellung (3.4) nicht effizient zu berechnen. Daher wollen wir noch eine andere Darstellung der Weil-Paarung, sowie einen Algorithmus zur Berechnung dieser, vorstellen.

Definition 3.3.1. Sei $D \in \operatorname{div}(E)$ gegeben durch $D = \sum n_P[P]$. Dann definieren wir den Träger von D durch

$$\operatorname{supp}(D) := \left\{ P \in E(\overline{K}) : n_p \neq 0 \right\}.$$

Definition 3.3.2. Sei $f \in K(x, y)$ und $D \in \operatorname{div}(E)$ gegeben durch $D = \sum n_P[P]$ mit

$$\operatorname{supp}(\operatorname{div}(f)) \cap \operatorname{supp}(D) = \emptyset.$$

Dann definieren wir

$$f(D) := \prod f(P)^{n_P}.$$

Theorem 3.3.3. *Sei $S, T \in E[n], D_S, D_T \in \operatorname{div}^0(E)$ und $f_S, f_T \in K(x, y)$ mit folgenden Eigenschaften*

i. $\mathrm{sum}(D_S) = S$ *und* $\mathrm{sum}(D_T) = T$,

ii. $\mathrm{supp}(D_S) \cap \mathrm{supp}(D_T) = \emptyset$,

iii. $\mathrm{div}(f_S) = nD_S$ *und* $\mathrm{div}(f_T) = nD_T$.

Dann gilt

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

Beweis. Siehe [18] Kapitel VI. Theorem 12. □

Für die Divisoren D_S und D_T können wir

$$D_S = [S + R_1] - [R_1] \quad \text{und} \quad D_T = [T + R_2] - [R_2]$$

mit $R \in E(\overline{K})$ beliebig wählen. Dann gilt

$$e_n(S,T) = \frac{f_S(D_T)}{f_T(D_S)} = \frac{f_S(T + R_2) f_T(R_1)}{f_S(R_2) f_T(S + R_1)}. \tag{3.8}$$

Was jetzt noch fehlt, ist ein Algorithmus um (3.8) berechnen zu können. Bei dem folgenden Algorithmus nach [4] werden wir in der Lage sein, $f_S(D_T)$ zu berechnen ohne die Funktion f_S explizit aufzustellen.

Für $b \in \mathbb{N}$ definieren wir

$$D_b := b[S + R_1] - b[R_1] - [bS] + [O]. \tag{3.9}$$

Damit gilt $\deg(D_b) = 0$ und $\mathrm{sum}(D_b) = O$, also existiert nach Theorem 2.2.16 eine Funktion f_b mit $\mathrm{div}(f) = D_b$ und weiter gilt

$$D_n = n[S + R_1] - n[R_1] - [nS] + [O] = n[S + R_1] - n[R_1] = nD_S.$$

Daraus können wir also $\mathrm{div}(f_n) = \mathrm{div}(f_S)$ folgern, was es uns erlaubt $f_n = f_S$ anzunehmen. Somit gilt $f_n(D_T) = f_S(D_T)$.

Lemma 3.3.4. *Seien $b, c \in \mathbb{N}$. Dann existieren Funktionen g_1, g_2, so dass gilt*

$$f_{b+c}(D_T) = f_b(D_T) \cdot f_c(D_T) \cdot \frac{g_1(D_T)}{g_2(D_T)}.$$

Beweis. Sei $a_1 x + b_1 + c_1 = 0$ die Gerade durch die Punkte bS und cS. Gilt $b = c$, so ist $a_1 x + b_1 + c_1 = 0$ die Tangente von E in bS. Weiter sei $x + c_2 = 0$ die Senkrechte durch den Punkt $(b + c)S$. Wir definieren

$$g_1(x,y) := a_1 x + b_1 + c_1 \quad \text{und} \quad g_2(x,y) := x + c_2. \tag{3.10}$$

Dann erhalten wir

$$\operatorname{div}(g_1) = [bS] + [cS] + [-(b+c)S] - 3[O]$$

und

$$\operatorname{div}(g_2) = [(b+c)S] + [-(b+c)S] - 2[O].$$

Nach (3.9) gilt

$$\begin{aligned} D_b &= b[S+R_1] - b[R_1] - [bS] + [O] \\ D_c &= c[P+R_1] - c[R_1] - [cS] + [O] \\ D_{b+c} &= (b+c)[P+R_1] - (b+c)[R_1] - [(b+c)S] + [O]. \end{aligned}$$

Es folgt

$$D_{b+c} = D_b + D_c + \operatorname{div}(g_1) - \operatorname{div}(g_2)$$

und daraus

$$f_{b+c}(D_T) = f_b(D_T) \cdot f_c(D_T) \cdot \frac{g_1(D_T)}{g_2(D_T)}.$$

□

Sind also $f_b(D_T), f_c(D_T)$ sowie $bP, cP, (b+c)P$ gegeben, so können wir durch Auswerten von $g_1(D_T)$ und $g_2(D_T)$ auch $f_{b+c}(D_T)$ bestimmen. Damit erhalten wir einen Algorithmus A der durch Eingabe von $f_b(D_T), f_c(D_T), bP, cP, (b+c)P$ den Wert $f_{b+c}(D_T)$ berechnet. Bevor wir nun einen Algorithmus zur Berechnung von $f_n(D_T)$ angeben können, müssen wir noch f_0 und f_1 berechnen. Für f_0 setzen wir $f_0(D_T) = 1$ und für f_1 gilt

$$\operatorname{div}(f_1) = [S+R_1] - [R_1] - [S] + [O].$$

Seien g_1 und g_2 definiert wie in (3.10), dann ist $\operatorname{div}(f_1) = \operatorname{div}(g_2) - \operatorname{div}(g_1)$. Daraus können wir nun

$$f_1(x,y) = \frac{g_2(x,y)}{g_1(x,y)}$$

schließen.

Sei $b_m b_{m-1} \dots b_1 b_0$ die Binärdarstellung von n, das heißt es gilt $n = \sum_{i=1}^{m} b_i 2^i$.

Algorithmus 3.3.5. *Am Anfang setzen wir* $Z := O, V := f_1(D_T)$ *und* $k = 0$.
für $i = m, m-1 \dots, 0$ *tue:*

- *Ist* $b_i = 1$, *setze* $V := A(V, f_1(D_T), Z, P, Z+S)$, $Z := Z+S$ *und* $k := k+1$.
- *Ist* $i > 0$, *so setze* $V := A(V, V, Z, Z, 2Z)$, $Z := 2Z$ *und* $k := 2k$.

Ist am Ende $i = 0$, so ist $Z = nS, V = f_n(D_T)$ und $k = n$.

4. Die Weil-Paarung in der Kryptographie

Im letzten Kapitel haben wir die Weil-Paarung auf elliptischen Kurven kennen gelernt. Wir wollen jetzt diese Abbildung in der Kryptographie nutzen. Bevor wir dieses allerdings tun können, benötigen wir noch etwas Theorie zu elliptischen Kurven über endlichen Körpern. Im weiteren Verlauf sei $q = p^m$ eine Primzahlpotenz mit $p \neq 2, 3$.

4.1. Elliptische Kurven über endlichen Körpern und supersinguläre Kurven

Sei $N := q + 1 - a$. Es existiert nach [30] genau dann eine elliptische Kurve über $\mathbb{F}_q$, mit $\#E(\mathbb{F}_q) = N$, wenn $|a| \leq 2\sqrt{q}$ und eine der folgenden Bedingungen gilt:

i. $\gcd(a, p) = 1$,

ii. m ist gerade und eine der folgende Bedingungen gilt

a. $a^2 = 4q$,
b. $a^2 = q$ und $p \not\equiv 1 \mod 3$,
c. $a = 0$ und $p \not\equiv 1 \mod 4$,

iii. m ist ungerade und eine der folgenden Bedingungen gilt

a. $a^2 = 2q$ und $p = 2$,
b. $a^2 = 3q$ und $p = 3$,
c. $a = 0$.

Theorem 4.1.1. *Sei E eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$. Dann gilt*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad \textit{oder} \quad E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2},$$

mit $n, n_1, n_2 \in \mathbb{N}$ und n_1 teilt n_2.

Beweis. Aus der Gruppentheorie wissen wir, dass jede endliche abelsche Gruppe isomorph zu der direkten Summe von zyklischen Gruppen

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r},$$

mit $n_i | n_{i+1},\ i \geq 1$, ist. Für alle i hat $\mathbb{Z}_{n_i}$ n_1 Elemente, deren Ordnung n_1 teilt. Es folgt insgesamt, dass $E(\mathbb{F}_q)$ n_1^r Elemente besitzt, deren Ordnung n_1 teilt. Da $E[n_1]$ maximal aus n_1^2 Elementen besteht, folgt also $r \leq 2$. □

Theorem 4.1.2. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ mit $\#E(\mathbb{F}_q) = q + 1 - a$. Weiter sei $\alpha, \beta \in \mathbb{C}$ gegeben durch $X^2 - aX + q = (X - \alpha)(X - \beta)$. Dann gilt*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),\ n \geq 1.$$

Beweis. Siehe Theorem 4.12 in [30]. □

Definition 4.1.3. Eine elliptische Kurve E über einem Körper der Charakteristik p heißt supersingulär, wenn $E[p] = \{O\}$ gilt.

Proposition 4.1.4. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q+1-\#E(\mathbb{F}_q)$. Dann ist E supersingulär genau dann, wenn $a \equiv 0 \mod p$ gilt.*

Beweis. Sei $X^2 - aX + q = (X - \alpha)(X - \beta)$ mit $\alpha, \beta \in \mathbb{C}$. Nach Theorem 4.1.2 gilt

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),\ n \geq 1.$$

Wir setzen nun $s_n := \alpha^n + \beta^n,\ n \in \mathbb{N}$. Dann ist $s_0 = 2$ und $s_1 = a$. Es gilt $\alpha^2 - a\alpha + q = 0$. Wenn wir die Gleichung mit α^{n-1} multiplizieren, erhalten wir $\alpha^{n+1} = \alpha^n a - \alpha^{n-1} q$ und analog $\beta^{n+1} = \beta^n a - \beta^{n-1} q$ und damit insgesamt

$$s_{n+1} = \left(\alpha^{n+1} + \beta^{n+1}\right) = \left(\alpha^n a - \alpha^{n-1} q + \beta^n a - \beta^{n-1} q\right) = s_n a - s_{n-1} q.$$

Sei jetzt $a \equiv 0 \mod p$. Es folgt $s_1 = a \equiv 0 \mod p$ und somit $s_{n+1} \equiv 0 \mod p$ für alle $n \in \mathbb{N}$. Also ergibt sich

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) = q^n + 1 - s_n \equiv 1 \mod p,\ n \in \mathbb{N}.$$

Folglich existieren keine Punkte der Ordnung p in $E(\mathbb{F}_{q^n}),\ n \in \mathbb{N}$. Da $\overline{\mathbb{F}_q} = \cup_{n \geq 1} \mathbb{F}_{q^n}$ gilt, gibt es keine Punkte der Ordnung p in $E(\overline{\mathbb{F}_q})$ und damit ist E supersingulär.

Sei nun $a \not\equiv 0 \mod p$. Wir erhalten dann $s_{n+1} \equiv a s_n \mod p,\ n \in \mathbb{N}$. Da $s_1 = a$ ist, gilt also $s_n \equiv a^n,\ n \in \mathbb{N}$, und damit ist

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a^n \mod p,\ n \in \mathbb{N}.$$

Nach dem kleinen Satz von Fermat gilt $a^{p-1} \equiv 1 \mod p$, womit die Ordnung von $E\left(\mathbb{F}_{q^{p-1}}\right)$ durch p teilbar ist. Es folgt, dass ein Punkt der Ordnung p existiert. Somit ist E nicht supersingulär. □

Corollar 4.1.5. *Sei $p \geq 5$ eine Primzahl. Dann ist E genau dann supersingulär, wenn $a = 0$, das heißt $\#E(\mathbb{F}_p) = p + 1$, gilt.*

Beweis. Ist $a = 0$, dann ist E nach Proposition 4.1.4 supersingulär.

Sei Umgekehrt E supersingulär und $a \neq 0$. Aus $a \equiv 0 \mod p$ folgt dann $|a| \geq p$. Nach dem Theorem von Hasse erhalten wir aber auch $|a| \leq 2\sqrt{p}$, also insgesamt $p \leq 2\sqrt{p}$. □

Die supersingulären Kurven wollen wir in sechs verschiedene Klassen einteilen. Ist $E(\mathbb{F}_q)$ eine supersinguläre Kurve mit $\#E(\mathbb{F}_q) = q + 1 - a$, so gehört $E(\mathbb{F}_q)$ genau in eine der folgenden Klassen:

(I) $a = 0$ dann gilt $E(\mathbb{F}_q) \equiv \mathbb{Z}_q$,

(II) $a = 0$ und $q \equiv 3 \mod 4$,

(III) m ist gerade und $a^2 = q$,

(IV) m ist gerade und $a^2 = 4q$,

(V) m ist ungerade, $p = 2$ und $a^2 = 2q$,

(VI) m ist ungerade, $p = 3$ und $a^2 = 3q$.

4.2. Elliptische Kurven in der Kryptographie

Wir wollen jetzt ein asymmetrisches Kryptosystem mit elliptischen Kurven vorstellen, das ElGamal-Kryptosystem. Die beiden Kommunikationspartner A und B bezeichnen wir mit Alice und Bob. Weiter gibt es noch die Angreiferin Eve. Sie kann Nachrichten zwischen Alice und Bob abfangen. Ihr Ziel ist es die abgefangenen Nachrichten zu entschlüsseln.

Sei $E(\mathbb{F}_q)$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Weiter sei $P \in E(\mathbb{F}_q)$ ein Punkt der Ordnung n. Der Punkt P wird dabei so gewählt, dass n eine große Primzahl ist, siehe zum Beispiel [16]. Besteht die Primfaktorzerlegung der Ordnung der elliptischen Kurve nur aus kleinen Primzahlen, so ist es möglich, zum Beispiel mit dem Pohlig-Silver-Hellman-Algorithmus den diskreten Logartihmus zu berechnen. Das ElGamal-Kryptosystem wird nun folgendermaßen erstellt:

- Bob wählt eine Geheimzahl $s \in \mathbb{Z}/p\mathbb{Z}$.
- Er berechnet $B = sP$.
- Bob veröffentlicht seinen öffentlichen Schlüssel $(E(\mathbb{F}_q), \mathbb{F}_q, P, B)$.

Die Zahl s ist der geheime Schlüssel von Bob. Möchte Alice Bob eine verschlüsselte Nachricht senden, so führt sie die folgenden Schritte aus:

- Sie lädt den öffentlichen Schlüssel von Bob runter.
- Sie drückt ihre Nachricht als einen Punkt $M \in E(\mathbb{F}_q)$ aus.

- Sie wählt eine Geheimzahl $k \in \mathbb{Z}/p\mathbb{Z}$ und berechnet $M_1 = kP$.
- Dann berechnet sie $M_2 = M + kB$
- Sie schickt Bob (M_1, M_2).

Bemerkung. Für eine Methode, wie Alice eine Nachricht m als Punkt einer elliptischen Kurve ausdrücken kann, siehe [16].

Möchte Bob die Nachricht von Alice entschlüsseln, so berechnet er

$$M_2 - sM_1.$$

Er erhält damit

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - s(kP) = M.$$

Die Sicherheit der ElGamal-Verschlüssung beruht auf dem diskreten Logarithmus-Problem für elliptische Kurven.

Diskretes Logarithmus-Problem (DLP):
Gegeben sind $Q, P \in E(\mathbb{F}_q)$. Bestimme $k \in \mathbb{Z}$, so dass $Q = kP$ gilt.

Gelangt Eve in den Besitz von M_1 und M_2, so kann sie M nur durch die Berechnung eines diskreten Logarithmus bestimmen. Kennt Eve s, so kann sie M auf demselben Weg wie Bob berechnen. Allerdings liefert Eve auch die Kenntnis von k den Klartext M, indem sie einfach $M = M_2 - kB$ berechnet.

Ein Angriffspunkt ist die Wahl von k. Alice muss bei jeder Verschlüsselung ein anderes k benutzen. Wird zweimal dasselbe k benutzt, so besteht die Möglichkeit, dass Eve den Klartext M berechnen kann. Nehmen wir an, dass Alice zwei Nachrichten M und M' mit demselben k verschlüsselt hat. Der Angreiferin Eve fällt dies auf, da $M_1 = M_1'$ gilt. Ist M eine Nachricht die irgendwann öffentlich gemacht wird, so kann Eve durch

$$M' = M_2' - kB = M - M_2 + M_2'$$

den neuen Klartext M' berechnen.

Der Vorteil eines asymmetrischen Kryptosystems ist, dass kein Schlüsselaustausch nötig ist. Allerdings sind diese Kryptosysteme langsam. Symmetrische Kryptosysteme sind dagegen schnell, aber es muss ein Schlüssel ausgetauscht werden. In der Praxis werden daher zumeist hybride Verfahren eingesetzt. Der Klartext wird mit Hilfe eines symmetrischen Verfahrens verschlüsselt. Dann wird der zugehörige Schlüssel mit einem öffentlichen Schlüssel eines asymmetrischen Verfahrens chiffriert. Der Empfänger kann den symmetrischen Schlüssel mit seinem geheimen asymmetrischen Schlüssel dechiffrieren und damit den Klartext mit dem symmetrischen Verfahren berechnen.

Ein Vorteil von Kryptosystemen mit elliptischen Kurven ist, dass viele Verfahren zum lösen des diskrete Logarithmus-Problems, zum Beispiel der Index-Calculus-Algorithmus, nicht anwendbar sind. Der Index-Calculus-Algorithmus benötigt eine Faktorbasis, diese existiert aber auf E nicht. Im Allgemeinen wird vermutet, dass es keinen subexponentiellen Algorithmus gibt, der das diskrete Logarithmus-Problem auf elliptischen Kurven löst. Die einzigen verbleibenden Algorithmen sind generische Methoden, also Methoden, die einen allgemeinen Ansatz verfolgen. Sei G eine zyklische Gruppe der Ordnung ℓ und $g \in G$ ein Erzeuger, dann lautet das DLP:

Gegeben sei $y \in G$, bestimme $x \in \mathbb{Z}$, so dass $y = g^x$ gilt.

Die Pollard-Rho-Methode kann nun ohne weitere Information über die Gruppe G das DLP in einer Laufzeit von $O(\ell^{1/2})$ lösen. Nach [26] ist dies auch die bestmögliche Laufzeit eines generischen Algorithmus. Im Fall der Kryptographie mit elliptischen Kurven ist die zyklische Gruppe, die von dem Punkt P erzeugte Untergruppe. Diese hat die Ordnung n, dabei ist n eine große Primzahl. Die Laufzeit ist also enstprechend lang und dementsprechend ist es möglich, bei gleicher Sicherheit, Schlüssel geringer Länge zu nehmen. Es stellt sich die Frage, ob es Sonderfälle gibt, in denen die Laufzeit verbessert werden kann. Einer dieser Sonderfälle wird im nächsten Abschnitt behandelt.

4.3. Der MOV-Angriff

Sei $E(\mathbb{F}_q)$ eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$. Weiter sei $P \in E(\mathbb{F}_q)$ ein Punkt der Ordnung n und $R \in E(\mathbb{F}_q)$. Wir wollen eine eindeutige natürliche Zahl l, $l \leq n-1$, finden, so dass $R = lP$ gilt.

Zuerst wollen wir untersuchen, unter welchen Bedingungen eine Lösung existiert.

Lemma 4.3.1. *Sei E eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Sei P ein Punkt mit* $\operatorname{ord}(P) = N$, $\gcd(N, q) = 1$ *und $Q \in E(\mathbb{F}_q)$ ein beliebiger Punkt. Es existiert genau dann ein $k \in \mathbb{Z}$ mit $Q = kP$, wenn $NQ = O$ und $e_N(P, Q) = 1$ gilt.*

Beweis. Sei $k \in \mathbb{Z}$ mit $Q = kP$. Dann ist $NQ = kNP = O$ und es gilt

$$e_N(P, Q) = e_N(P, kP) = e_N(P, P)^k = 1^k = 1.$$

Sei umgekehrt $NQ = O$, woraus $Q \in E[n]$ folgt, und $e_N(P, Q) = 1$. Da $\gcd(N, q) = 1$ ist, gilt $E[n] \simeq \mathbb{Z}_N \oplus \mathbb{Z}_N$. Wir wählen einen Punkt $R \in E[n]$, so dass $\{P, R\}$ eine Basis von $E[n]$ ist. Dann existieren $a, b \in \mathbb{Z}$ mit

$$Q = aP + bR.$$

Nach Corollar 3.2.3 ist $e_N(P, R) = \zeta$ eine primitive N-te Einheitswurzel. Damit gilt

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b.$$

Da ζ eine primitive N-te Einheitswurzel ist, folgt $b \equiv 0 \mod N$. Damit ist $bR = O$ und insgesamt somit $Q = aP$. □

Bezeichnung. Mit $<P>$ wollen wir im weiteren Verlauf die von P erzeugte Untergruppe von $E(\mathbb{F}_q)$ bezeichnen.

Als erstes wollen wir uns mit einem Algorithmus beschäftigen, der es erlaubt Teilinformationen über l zu erhalten, indem wir einen diskreten Logarithmus in $\mathbb{F}_q$ berechnen.

Algorithmus 4.3.2. *Gegeben sei ein Punkt $P \in E(\mathbb{F}_q)$ der maximalen Ordnung n_2 und ein Punkt $R \in E(\mathbb{F}_q)$ mit $R = lP,\ l \in \mathbb{Z}$.*

Schritt 1: *Wähle einen zufälligen Punkt $T \in E(\mathbb{F}_q)$.*

Schritt 2: *Berechne $\alpha := e_{n_2}(P,T)$ und $\beta := e_{n_2}(R,T)$.*

Schritt 3: *Berechne l', den diskreten Logarithmus von β zur Basis α in $\mathbb{F}_q$.*

Proposition 4.3.3. *Der Algorithmus 4.3.2 ergibt $l' \equiv l \mod \operatorname{ord}(\alpha)$, wobei $\operatorname{ord}(\alpha)$ ein Teiler von n_1 ist.*

Beweis. Sei n' die Ordnung von α und $G \in E(\mathbb{F}_q)$ ein Punkt der Ordnung n_1 mit der Eigenschaft, dass $E(\mathbb{F}_q)$ von $\{P, G\}$ erzeugt wird. Dann existieren $c_1, c_2 \in \mathbb{Z}$, so dass für den zufällig gewählten Punkt $T \in E(\mathbb{F}_q)$

$$T = c_1 P + c_2 G$$

gilt. Damit erhalten wir

$$\begin{aligned} \alpha^{n_1} &= e_{n_2}(P,T)^{n_1} = e_{n_2}(P, c_1P + c_2G)^{n_1} \\ &= e_{n_2}(P,P)^{n_1 c_1} e_{n_2}(P, c_2 n_1 G) \\ &= e_{n_2}(P,O) \\ &= 1. \end{aligned}$$

Da n' die Ordnung von α war, ist also n' ein Teiler von n_1. Mit

$$\begin{aligned} \beta &= e_{n_2}(R,T) = e_{n_2}(lP,T) \\ &= e_{n_2}(P,T)^l = \alpha^l \\ &= \alpha^{l'} \end{aligned}$$

folgt die Behauptung. □

Lemma 4.3.4. *Sei E eine elliptische Kurve mit $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ und $P \in E(\mathbb{F}_q)$ ein Punkt maximaler Ordnung n_2. Dann gilt für alle $P_1, P_2 \in E(\mathbb{F}_q)$, dass P_1 und P_2 genau dann in derselben Nebenklasse von $<P>$ liegen, wenn $e_{n_2}(P,P_1) = e_{n_2}(P,P_2)$ gilt.*

Beweis. Seien $P_1, P_2 \in E(\mathbb{F}_q)$ beliebig. Liegen P_1 und P_2 in derselben Nebenklasse von $< P >$, so existiert ein $k \in \mathbb{Z}$ mit $P_1 - P_2 = kP$. Es folgt

$$e_{n_2}(P, P_1) = e_{n_2}(P, P_2 + kP) = e_{n_2}(P, P_2)e_{n_2}(P, P)^k = e_{n_2}(P, P_2).$$

Nehmen wir nun also an, dass P_1 und P_2 in verschiedenen Nebenklassen von $< P >$ liegen. Wir wählen $Q' \in E[n_2]$ so, dass $\{P, Q'\}$ eine Basis von $E[n_2]$ ist. Der Punkt $Q := (n_2/n_1)Q'$ hat dann die Ordnung n_1 und somit wird $E(\mathbb{F}_q)$ von $\{P, Q\}$ erzeugt. Es existieren dann also $a, b \in \mathbb{Z}$ mit

$$P_1 - P_2 = aP + bQ \quad \text{und} \quad bQ \neq O.$$

Wir erhalten

$$e_{n_2}(P, P_1) = e_{n_2}(P, P_2 + aP + bQ) = e_{n_2}(P, P_2)e_{n_2}(P, bQ).$$

Um $e_{n_2}(P, bQ) \neq 1$ zu prüfen, nehmen wir einen beliebigen Punkt $T \in E[n_1]$. Dann existieren $r, s \in \mathbb{Z}$ mit $T = rP + sQ'$. Wir setzen T in die Weil-Paarung ein:

$$\begin{aligned} e_{n_2}(T, bQ) &= e_{n_2}(rP, bQ)e_{n_2}(sQ', bQ) \\ &= e_{n_2}(P, bQ)^r e_{n_2}(Q', Q')^{(bsn_2)/n_1} \\ &= e_{n_2}(P, bQ)^r. \end{aligned}$$

Wäre nun $e_{n_2}(P, bQ) = 1$, würde, da T beliebig war und die Weil-Paarung nicht entartet ist, $bQ = O$ folgen, was ein Widerspruch ist. □

Da es n_1 verschiedene Nebenklassen von $< P >$ in $E(\mathbb{F}_q)$ gibt, folgt mit Hilfe des Lemmas 4.3.4, dass die Wahrscheinlichkeit, das $n' = n_1$ ist, $\phi(n_1)/n_1$ beträgt. Dabei bezeichne ϕ die Eulersche Phi-Funktion. Ist n_1 allerdings klein, so ist der Informationsgewinn über l sehr gering, daher wollen wir nun einen Algorithmus behandeln, mit dem wir $l \mod n$ erhalten.

Sei k die kleinste natürliche Zahl, so dass $E[n] \subseteq E\left(F_{q^k}\right)$ gilt. Nach Corollar 3.2.4 ist dann $\mu_n \subseteq F_{q^k}$. Damit ergibt sich sofort:

Proposition 4.3.5. *Sei $Q \in E[n]$, so dass $e_n(P, Q)$ eine primitive n-te Einheitswurzel ist, und $f :< P > \rightarrow \mu_n$ definiert durch $f : R \mapsto e_n(R, Q)$. Dann ist f ein Gruppenisomorphismus.*

Wir sind jetzt in der Lage den Algorithmus zu formulieren.

Algorithmus 4.3.6. *Gegeben sei ein Punkt $P \in E(\mathbb{F}_q)$ der Ordnung n und ein Punkt $R \in E(\mathbb{F}_q)$ mit $R = lP$, $l \in \mathbb{Z}$.*

Schritt 1: *Bestimme die kleinste natürliche Zahl k, so dass $E[n] \subseteq E\left(\mathbb{F}_{q^k}\right)$.*

Schritt 2: *Suche $Q \in E[n]$, so dass $\alpha := e_n(P,Q)$ Ordnung n hat.*

Schritt 3: *Berechne $\beta := e_n(R,Q)$.*

Schritt 4: *Berechne l, den diskreten Logarithmus von β zur Basis α in F_{q^k}.*

Wir erhalten das korrekte Ergebnis, denn es gilt

$$\begin{aligned}\beta &= e_n(lP,Q)\\ &= e_n(P,Q)^l\\ &= \alpha^l.\end{aligned}$$

Leider hat auch dieser Algorithmus Schwächen, denn es ist problematisch k zu bestimmen und den Punkt $Q \in E(\mathbb{F}_q)$ zu finden, so dass α die Ordnung n hat. Für supersinguläre Kurven sind wir aber in der glücklichen Situation, dass das k für alle Klassen bekannt ist. Für Kurven der Klassen **(I)** und **(II)** gilt:

Proposition 4.3.7. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ mit $a = q + 1 - \#E(\mathbb{F}_q) = 0$ und $N \in \mathbb{N}$. Existiert ein Punkt $P \in E(\mathbb{F}_q)$ der Ordnung N, so ist*

$$E[n] \subseteq E\left(\mathbb{F}_{q^2}\right).$$

Beweis. Der Frobenius-Endomorphismus ϕ_q erfüllt $\phi_q^2 - a\phi_q + q = 0$. Mit $a = 0$ ergibt sich $\phi_q^2 = -q$. Sei nun $S \in E[n]$ beliebig. Da $\#E(\mathbb{F}_q) = q + 1$ gilt und ein Punkt der Ordnung N existiert, wird $q+1$ von N geteilt. Somit ist $-q \equiv 1 \mod N$. Insgesamt gilt also

$$\phi_q^2(S) = -qS = 1S.$$

Nach Proposition A.3 folgt $S \in E\left(\mathbb{F}_{q^2}\right)$. □

Haben wir eine supersinguläre Kurve, für die $a \neq 0$ gilt, so reicht es nicht aus $k = 2$ zu wählen.

Beispiel 4.3.8. E ist gegeben durch $y^2 + y = x^3 + x$ über $\mathbb{F}_2$. Es gilt

$$E(\mathbb{F}_2) = \{(0,0),(0,1),(1,0),(1,1),O\},$$

also ist $\#E(\mathbb{F}_2) = q+1-a = 5$. Es ergibt sich $a = -2$, das heißt $a \equiv 0 \mod 2$ und somit ist E supersingulär. Weiter gilt für den Frobenius-Endormorphismus $\phi_2^2 + 2\phi_2 + 2 = 0$ und $X^2 + 2X + 2 = (X - (-1 - i))(X - (-1 + i))$. Damit erhalten wir

$$\phi_2^4 = (-2\phi_2 - 2)^2 = 4\phi_2^2 + 8\phi_2 + 4 = -4.$$

Dann folgt $E[5] \subseteq E(\mathbb{F}_{16})$, denn für $T \in E[5]$ gilt

$$\phi_2^4(T) = -4T = T$$

und damit ist $T \in E(\mathbb{F}_{16})$. Es gilt nach Theorem 4.1.2

$$\#E(\mathbb{F}_{2^2}) = 2^2 + 1 - ((-1+i)^2 + (-1-i)^2) = 5$$

und

$$\#E(\mathbb{F}_{2^4}) = 2^4 + 1 - ((-1+i)^4 + (-1-i)^4) = 25.$$

Da $\#E[n] = 25$ erhalten wir insgesamt, dass $E[5] \not\subseteq E(\mathbb{F}_{2^2})$ und $m = 4$ die kleinste natürliche Zahl ist, so dass $E[5] \subseteq E(\mathbb{F}_{2^m})$ gilt.

Für die anderen Klassen von supersingulären elliptischen Kurven können wir das k aus der in [22] aufgestellten Tabelle 4.1 ablesen:

Klasse der Kurve	a	Gruppenstruktur	k
(I)	0	zyklisch	2
(II)	0	$\mathbb{Z}_{(q+1/2)} \oplus \mathbb{Z}_2$	2
(III)	$\pm\sqrt{q}$	zyklisch	3
(IV)	$\pm\sqrt{2q}$	zyklisch	4
(V)	$\pm\sqrt{3q}$	zyklisch	6
(VI)	$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1} \oplus \mathbb{Z}_{\sqrt{q}\mp 1}$	1

Tabelle 4.1.: Informationen über supersinguläre Kurven

Damit können wir für supersinguläre Kurven das erste Problem lösen. Die zweite Schwäche des Algorithmus 4.3.6 umgehen wir, indem wir uns einen zufälligen Punkt $T \in E(\mathbb{F}_{q^k})$ wählen. Dann setzen wir $d := \gcd(N, \mathrm{ord}(T))$ und erhalten nach Durchführung des Algorithmus 4.3.6 k modulo d. Wir wiederholen nun diese Schritte und setzen am Ende das k mit dem chinesischen Restsatz zusammen. Dadurch ergibt sich der folgende Algorithmus.

Algorithmus 4.3.9. *Gegeben sei ein Punkt $P \in E(\mathbb{F}_q)$ der Ordnung n und ein Punkt $R \in E(\mathbb{F}_q)$ mit $R = lP$, $l \in \mathbb{Z}$.*

Schritt 1: *Wähle aus Tabelle 4.1 das entsprechende k.*

Schritt 2: *Wähle einen zufälligen Punkt $T \in E(\mathbb{F}_{q^k})$.*

Schritt 3: *Berechne $m_T := \mathrm{ord}(T)$.*

Schritt 4: *Setze $d_1 := \gcd(m_T, n)$ und $T_1 := (m_T/d_1)T$.*

Schritt 5: *Berechne $\zeta_1 := e_n(P, T_1)$ und $\zeta_2 := e_n(R, T_1)$.*

Schritt 6: *Löse das diskrete Logarithmus-Problem $\zeta_2 = \zeta_1^l$ in $\mathbb{F}_{q^k}^*$.*

Schritt 7: *Wiederhole die Schritte 2-6 solange, bis das kleinste gemeinsame Vielfache der d_i n ergibt.*

Schritt 8: *Berechne* $l \mod n$.

Bemerkung 4.3.10.

- T_1 hat die Ordnung d_1 und es gilt $T_1 \in E[n]$.
- ζ_1 und ζ_2 sind aus $\mu_d \subseteq \mathbb{F}_{q^k}^*$.
- In **Schritt 6** erhalten wir $l \mod d_1$.

Menezes, Vanstone und Okamoto zeigen in [22], dass dieser Algorithmus eine subexponentielle Laufzeit hat.

4.4. Schlüsselerzeugung mit der Weil-Paarung

Wir wollen den Schlüsselaustausch nach Diffie-Hellman für elliptische Kurven vorstellen. Dann werden wir die Weil-Paarung benutzen, um eine Drei-Parteien Version des Diffie-Hellman-Protokolles zu erzeugen. Die Schlüsselerzeugung für zwei Parteien nach dem Diffie-Hellman-Protokoll lautet:

- Alice und Bob einigen sich auf eine elliptische Kurve E über einem endlichen Körper $\mathbb{F}_q$, so dass das diskrete Logarithmus Problem in $E(\mathbb{F}_q)$ schwer ist. Weiter einigen sie sich über einen Punkt $P \in E(\mathbb{F}_q)$, so dass die von P erzeugte Untergruppe einen großen Primteiler hat.
- Dann wählen Alice und Bob jeweils eine geheime Zahl a und b.
- Sie berechnen $P_A := aP$ und $P_B := bP$.
- Austausch von P_A und P_B.
- Berechnung von aP_B und bP_A.

Alice und Bob erhalten jetzt den gemeinsamen Punkt abP. Jetzt könnten sie zum Beispiel die letzten 256Bit der x-Koordinate von abP als Schlüssel nehmen. Die Sicherheit des Diffie-Hellman-Protokolls beruht auf der Schwierigkeit diskrete Logarithmen zu berechnen. Wir wollen jetzt einen Algorithmus von Joux [14], für den Diffie-Hellman-Schlüsselaustausch mit 3 Teilnehmern, vorstellen. Bei Verfahren, die keine Paarungen benutzen, müssen dabei alle Teilnehmer zweimal interagieren, während bei dem folgenden Verfahren nur eine Interaktion notwendig ist.

Alice, Bob und Cedric wollen einen gemeinsamen Schlüssel $K_{A,B,C}$ erzeugen.

- Alice, Bob und Cedric einigen sich, wie oben, auf eine elliptische Kurve E und einen Punkt $P \in E$.
- Sie wählen jeweils eine geheime Zahl a, b, c.

- Berechnung von $P_A := aP, P_B := bP$ und $P_C := cP$.
- Austausch von P_A, P_B und P_C.
- Berechnung von $f(a, P_B, P_C), f(b, P_A, P_C)$ und $f(c, F_A, F_B)$.

Dabei müssen wir jetzt die Funktion f so wählen, dass

$$K_{A,B,C} = f(a, P_B, P_C) = f(b, P_A, P_C) = f(c, F_A, F_B)$$

gilt und dass aus der Kenntnis von $K_{A,B,C}$ nicht P_A, P_B und P_C berechnet werden kann. Wir wählen für f die Weil-Paarung, das heißt:

$$f(x, R, S) := e_{\mathrm{ord}(P)}(R, S)^x.$$

Damit erhalten wir

$$K_{A,B,C} = f(a, P_B, P_C) = f(b, P_A, P_C) = f(c, P_A, P_B) = e_{\mathrm{ord}(P)}(P, P)^{abc}.$$

Wir sehen, dass diese Wahl von f unglücklich ist, denn nach den Eigenschaften der Weil-Paarung folgt nun $K_{A,B,C} = 1$. Wir werden jetzt die Idee etwas modifizieren. Wir wählen dazu einen zu P linear unabhängigen Punkt $Q \in E$. Damit erhalten wir den folgenden Algorithmus.

Algorithmus 4.4.1. *Alice, Bob und Cedric wollen einen gemeinsamen Schlüssel erzeugen.*

Schritt 1: *Alice, Bob und Cedric einigen sich, unter den oben genannten Sicherheitsaspekten, auf eine elliptische Kurve E, einen Punkt $P \in E$ und einen von P linear unabhängigen Punkt $Q \in E$. Sei $N := kgV(\mathrm{ord}(P), \mathrm{ord}(Q))$.*

Schritt 2: *Sie wählen jeweils eine geheime Zahl a, b, c.*

Schritt 3: *Berechnung von $P_A := aP,\ Q_A := aQ,\ P_B := bP,\ Q_B := bQ$ und $P_C := cP,\ Q_C := cQ$.*

Schritt 4: *Austausch von $(P_A, Q_A), (P_B, Q_B)$ und (P_C, Q_C).*

Schritt 5: *Berechnung von $e_N(P_B, Q_C)^a, e_N(P_A, Q_C)^b$ und $e_N(P_A, Q_B)^c$.*

Durch die Eigenschaften der Weil-Paarung gilt

$$e_N(P_B, Q_C)^a = e_N(P_C, Q_B)^a = e_N(Q_C, P_B)^a = e_N(Q_B, P_C)^a$$

und

$$K_{A,B,C} = e_N(P, Q)^{abc}.$$

Da P und Q linear unabhängig sind, ist nun $K_{A,B,C}$ nicht konstant. Damit die Weil-Paarung schnell berechnet werden kann, muss die elliptische Kurve so gewählt sein, dass

ein möglichst kleines $k \in \mathbb{N}$ existiert, so dass $E[N] \subseteq E(\mathbb{F}_{q^k})$ gilt. Wir können hier also zum Beispiel eine supersinguläre Kurve mit $a = 0$ wählen, denn für diese Kurven ist $k = 2$. Wenn wir eine solche Kurve wählen, müssen wir darauf achten, dass q so groß ist, dass das diskrete Logarithmus-Problem in $\mathbb{F}_{q^2}$ nicht lösbar ist. Es gibt noch eine kleine Verfeinerung bei der man keine zwei linear unabhängigen Punkte benötigt, sondern nur einen. Dabei wird die Paarung etwas modifiziert, ein Beispiel hierfür sehen wir unten bei dem Diffie-Hellman-Entscheidungsproblem. Für weitere Details verweisen wir auf [29].

Aus der Schlüsselerzeugung mit Diffie-Hellman ergibt sich ein weiteres Problem, das sogenannte Diffie-Hellman-Entscheidungsproblem.

Diffie-Hellman-Entscheidungsproblem:
Gegeben sind $P, aP, bP \in E(\mathbb{F}_q)$ und ein weiterer Punkt $Q \in E(\mathbb{F}_q)$. Gilt $Q = abP$?

Das Diffie-Hellman-Entscheidungsproblem ist höchstens so schwer zu lösen wie das diskrete Logarithmus-Problem. Können wir das diskrete Logarithmus-Problem lösen, so ist es uns möglich das Diffie-Hellman-Entscheidungsproblem durch Einsetzen der Punkte zu lösen. Die Frage ist, ob das Diffie-Hellman-Entscheidungsproblem, ohne diskrete Logarithmen zu berechnen, lösbar ist. Im Fall der elliptischen Kurven können wir das Problem mit der Weil-Paarung lösen. Dazu wollen wir ein Beispiel betrachten. Sei E die supersingluäre Kurve $Y^2 = X^3 + 1$ über $\mathbb{F}_q$ mit $q \equiv 2 \mod 3$ und $\omega \in \mathbb{F}_{q^2}$ eine primitive dritte Einheitswurzel. Da die Ordnung von F_q^* gleich $q-1$ ist und $q - 1 \equiv 1 \mod 3$ gilt, folgt, dass die Ordnung von ω nicht $q-1$ teilt und somit $\omega \notin \mathbb{F}_q$ gilt. Mit ω definieren wir eine Abbildung

$$\beta : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q}), \;\; (x, y) \mapsto (\omega x, y) \;\text{ und }\; \beta(O) = O.$$

Da ω eine primitive dritte Einheitswurzel ist, ist β wohldefiniert. Durch Einsetzen in die Additionsformeln sehen wir, dass β ein Homomorphismus ist. Da β bijektiv ist, folgt insgesamt, dass β ein Isomorphismus ist. Sei nun $P \in E(\overline{\mathbb{F}_q})$ ein Punkt der Ordnung n, dann ist $\beta(P)$ auch ein Punkt der Ordnung n. Wir definieren damit eine Abbildung

$$\tilde{e}_n(P_1, P_2) := e_n(P_1, \beta(P_2)), \;\; P_1, P_2 \in E[n]\,.$$

Lemma 4.4.2. *Ist $P \in E(\mathbb{F}_q)$ ein Punkt der Ordnung n und es gilt $3 \nmid n$. Dann ist $\tilde{e}_n(P, P)$ eine primitive n-te Einheitswurzel.*

Beweis. Angenommen es existieren $u, v \in \mathbb{Z}$ mit $uP = v\beta(P)$. Dann gilt

$$\beta(vP) = v\beta(P) = uP \in E(\mathbb{F}_q)\,.$$

Ist $vP = O$, so folgt $uP = O$ und damit ist $u \equiv 0 \mod n$. Sei also $vP \neq O$ mit $vP = (a, b),\; a, b \in \mathbb{F}_q$. Dann gilt

$$(\omega a, b) = \beta(vP) \in E(\mathbb{F}_q)\,.$$

Da aber $\omega \notin E(\mathbb{F}_q)$ ist, folgt $a = 0$ und damit $vP = (0, \pm 1)$. Wir können nun nachrechnen, dass $2vP = (0, \mp 1)$ gilt. Daraus schließen wir, dass die Ordnung von vP gleich drei ist. Da wir aber $3 \nmid n$ angenommen hatten, ist dies nun ein Widerspruch. Damit folgt aus $uP = v\beta(P)$, dass $u, v \equiv 0 \mod n$ und somit bilden P und $\beta(P)$ eine Basis von $E[n]$. Nach Corollar 3.2.3 ist dann $\tilde{e}_n(P, P) = e_n(P, \beta(P))$ eine primitive n-te Einheitswurzel. □

Nehmen wir nun an, dass wir P, aP, bP und Q kennen. Jetzt müssen wir entscheiden ob $Q = abP$ gilt. Als erstes prüfen wir, ob überhaupt ein $k \in \mathbb{Z}$ existiert, so dass $Q = kP$ gilt. Nach Lemma 4.3.1 prüfen wir also, ob $e_n(Q, P) = 1$ gilt. Ist dies der Fall, so haben wir

$$\tilde{e}_n(aP, bP) = \tilde{e}_n(P, P)^{ab} = \tilde{e}_n(P, abP) \quad \text{und} \quad \tilde{e}_n(Q, P) = \tilde{e}_n(P, P)^k.$$

Gilt $3 \nmid n$, so ist nach Lemma 4.4.2 $\tilde{e}_n(P, P)$ eine primitive n-te Einheitswurzel und es gilt

$$Q = abP \iff k \equiv ab \mod n \iff \tilde{e}_n(aP, bP) = \tilde{e}_n(Q, P).$$

Um das Diffie-Hellman-Entscheidungsproblem in diesem Fall zu lösen, brauchen wir keine diskreten Logarithmen, sondern lediglich zweimal die Weil-Paarung zu berechnen.

4.5. Ein Kryptosystem mit der Weil-Paarung

Als letzte Anwendung der Weil-Paarung wollen wir die Idee für ein identitätsbasierendes Kryptosystem vorstellen. Die Idee hierfür stammt von Boneh und Franklin [4]. Der Vorteil eines identitätsbasierenden Kryptosystems ist, dass kein Austausch von Schlüsseln stattfindet und man nicht den öffentlichen Schlüssel eines Benutzers kennen muss, um eine Nachricht zu schicken. Denn der öffentliche Schlüssel wird aus der Identität des Benutzers abgeleitet, zum Beispiel der E-Mail-Adresse. Es gibt eine zentrale Instanz, die das Kryptosystem erzeugt. Diese zentrale Instanz verfügt über den sogenannten Master Key, welcher es ihr ermöglicht die geheimen Schlüssel zu erzeugen. An dieser Instanz melden sich die Benutzer mit ihrer Identität an. Dabei wird an dieser Stelle geprüft, ob der Benutzer auch derjenige ist, der er vorgibt zu sein. Danach erstellt die zentrale Instanz zu dem öffentlichen Schlüssel des Benutzers einen geheimen Schlüssel und sendet ihm diesen zu. Nun kann völlig unabhängig von der zentralen Instanz ein verschlüsselter Nachrichtenaustausch zwischen den Benutzern geschehen. Ein Nachteil solcher Systeme ist allerdings, falls der geheime Schlüssel eines Benutzers in die Hände von Eve gelangt, der Benutzer sich mit einer neuen Identität bei der zentralen Instanz anmelden muss. Denn Nachrichten, die mit der alten Identität verschlüsselt wurden, sind nun für Eve lesbar. Diesen Nachteil kann man etwas schmälern, indem die öffentlichen Schlüssel nur eine zeitlich begrenzte Gültigkeit haben. Dadurch ergibt sich allerdings wiederum die Notwendigkeit des Erstellens neuer geheimer Schlüssel. Für weitere Ergänzungen und Stärkungen gegen Angriffe siehe [4].

Für solche Kryptosysteme bietet es sich nicht an, die RSA-Verschlüsselung zu benutzen.

Denn wird für alle Benutzer dasselbe RSA-Modul N benutzt, so kann jeder Benutzer aus der Kenntnis seines öffentlichen und geheimen Schlüssels das RSA-Modul N faktorisieren und zu jedem anderen öffentlichen Schlüssel den geheimen Schlüssel berechnen. Damit ist es möglich jede verschlüsselte Nachricht zu lesen. Wird hingegen für jeden Benutzer ein anderes RSA-Modul N benutzt, so entfällt diese Schwachstelle. Allerdings muss nun für jede Übertragung einer verschlüsselten Nachricht geprüft werden, ob das richtige Modul N verwendet wird. Bei diesem Ansatz wird also zusätzliche Kommunikation benötigt.

Kommen wir nun zu der Idee des Kryptosystems. Wie in Abschnitt 4.4 wollen wir das Vorgehen beispielhaft anhand der supersingulären Kurve E darstellen, die durch $Y^2 = X^3 + 1$ über $\mathbb{F}_p$ mit $p \equiv 2 \mod 3$ gegeben ist. Wir wollen eine weitere Bedingung an die Primzahl p stellen. Es soll eine Primzahl l mit der Eigenschaft, dass $p = 6l - 1$ gilt existieren . Damit ist für alle Punkte $P \in E(\mathbb{F}_p)$, der Punkt $6P$ entweder von der Ordnung 1 oder l. Weiter sei wiederum $\omega \in \mathbb{F}_{p^2}$ eine primitive dritte Einheitswurzel. Ebenso definieren wir erneut

$$\beta : E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^2}), \;\; (x, y) \mapsto (\omega x, y) \;\; \text{und} \;\; \beta(O) = O,$$

und für Punkte $P \in E(\mathbb{F}_p)$ der Ordnung n

$$\tilde{e}_n(P, P) = e_n(P, \beta(P)).$$

Die zentrale Instanz erzeugt nun das Kryptosystem, indem sie die folgenden Schritte durchführt:

- Sie wählt eine große Primzahl der Form $p = 6l - 1$.
- Dann wählt sie einen Punkt P der Ordnung l in $E(\mathbb{F}_p)$.
- Nun wählt die zentrale Instanz zwei Hash-Funktionen H_1 und H_2. H_1 nimmt einen Bitstring beliebiger Länge und erzeugt daraus einen Punkt der Ordnung l auf $E(\mathbb{F}_p)$. H_2 nimmt ein Element der Ordnung l aus $E(\mathbb{F}_{p^2})$ und erstellt daraus einen binären String der Länge n. Dabei ist jetzt n die Länge der Nachrichten, die ausgetauscht werden.
- Nun wählt sie eine geheime Zahl $s \in \mathbb{F}_l^*$ und berechnet $P_{pub} := sP$.
- Veröffentlichung von $p, H_1, H_2, n, P, P_{pub}$.

Wenn sich nun ein Benutzer mit der Identität ID anmelden will, führt die zentrale Instanz folgendes durch:

- Berechnung von $Q_{ID} := H_1(ID) \in E(\mathbb{F}_p)$.
- Berechnung von $D_{ID} := sQ_{ID}$.
- Sie überzeugt sich, dass ID zu dem Benutzer gehört, mit dem sie gerade kommuniziert.

- Ist Schritt 3 erfolgreich, so wird dem Benutzer sein geheimer Schlüssel D_{ID} gesendet.

Nun möchte Alice Bob eine verschlüsselte Nachricht M schicken. Dazu tut sie folgendes:

- Sie schlägt Bobs Identität nach, zum Beispiel $ID = bob@secure.com$, und berechnet $Q_{ID} = H_1(ID)$.
- Sie wählt eine zufällige Zahl $r \in \mathbb{F}_l^*$.
- Dann berechnet sie $g_{ID} = \tilde{e}_l(Q_{ID}, P_{pub})$.
- Dann schickt sie Bob den Chiffretext

$$c = (rP, M \oplus H_2(g_{ID}^r)).$$

  Dabei bezeichnet $\oplus$ die Funktion XOR.

Bob hat einen Chiffretext (u, v) erhalten und entschlüsselt ihn nun wie folgt:

- Er berechnet $h_{ID} := \tilde{e}_l(D_{ID}, u)$.
- Dann berechnet er den Klartext durch $m = v \oplus H_2(h_{ID})$.

Wir müssen jetzt natürlich prüfen, ob Bob die ursprüngliche Nachricht erhält. Es gilt

$$\tilde{e}_l(D_{ID}, u) = \tilde{e}_l(sQ_{ID}, rP) = \tilde{e}_l(Q_{ID}, P)^{sr} = \tilde{e}_l(Q_{ID}, P_{pub})^r = g_{ID}^r.$$

Daraus folgt

$$m = v \oplus H_2(\tilde{e}_l(D_{ID}, u)) = (M \oplus H_2(g_{ID}^r)) \oplus H_2(g_{ID}^r) = M.$$

Wir wollen uns zum Schluß mit einer möglichen Hash-Funktion für H_1 beschäftigen. Sei H eine beliebige Hash-Funktion, die einen Bitstring in eine ganze Zahl modulo p umwandelt. Sei B ein beliebiger Bitstring. Wir setzen $b := H(B)$. Da in unserem Fall $p \equiv 2 \mod 3$ gilt, ist 3 kein Teiler der Ordnung von $\mathbb{F}_p^*$. Daraus folgt, dass $a \in \mathbb{F}_p^*$ mit $a^3 = b^2 - 1$ existiert. Wir setzen weiter $H_1(B) := 6(a, b)$. Gefordert war, dass $H_1(B)$ ein Punkt der Ordnung l ist. Nach Voraussetzung kann $6(a, b)$ nur die Ordnung 1 oder l haben. Da p kein Teiler von 6 ist, gibt es aber nur 36 Punkte der Ordnung 6 und da p eine große Primzahl ist, ist die Wahrscheinlichkeit sehr gering, dass $6(a, b)$ die Ordnung 1 hat.

Fazit / Ausblick

In dieser Arbeit ist gezeigt worden, dass für supersinguläre elliptische Kurven das diskrete Logarithmus-Problem auf dieser Kurve in subexponentieller Laufzeit gelöst werden kann. Die Sicherheit des Kryptosystems mit elliptischen Kurven hängt also entscheidend von der Wahl der elliptischen Kurve ab. In [2] wird gezeigt, dass bei einer zufälligen Wahl der elliptischen Kurve die Wahrscheinlichkeit, dass diese supersingulär ist, sehr gering ist.

Ein weiterer Ansatz mit einer Paarung liefert die Frey-Rück Reduktion. In ihr wird die Tate-Paarung benutzt, um das diskrete Logartihmus-Problem auf der elliptischen Kurve in ein diskretes Logarithmus-Problem in einem endlichen Körper zurückzuführen. Ein Vorteil der Frey-Rück Reduktion ist, dass sie auch in Fällen, in denen die MOV-Reduktion nicht anwendbar ist, eingesetzt werden kann. Für die Tate-Paarung ist es nicht nötig, dass (3.1) gilt, sondern es reicht schon die Existenz eines Punktes der Ordnung n. Zusätzlich muss die Spur des Frobenius-Endomorphismus der elliptischen Kurve kongruent 2 modulo n sein.

Weiter gibt es mehrere Ansätze, um für bestimme elliptische Kurven das diskrete Logarithmus-Problem zu lösen. Bisher ist es allerdings nicht gelungen diese zu verallgemeinern. Ein weiterer Ansatz ist der Xedni Calculus von Silverman [28]. In [13] wird allerdings gezeigt, dass die Erfolgswahrscheinlichkeit des Algorithmus, selbst über kleinen endlichen Körpern, sehr gering ist. Es bleibt also eine offene Frage, ob es Algorithmen gibt, die allgemein das diskrete Logarithmus-Problem über elliptischen Kurven in subexponentieller Zeit lösen können.

A. Sätze über Endomorphismen

Proposition A.1. *Sei $\alpha \neq 0$ ein separabler Endomorphismus auf einer elliptischen Kurve E über einem Körper K. Dann gilt*

$$\deg \alpha = \# \ker(\alpha).$$

Dabei ist $\ker(\alpha)$ *der Kern des Homomorphismuses $\alpha : E(\overline{K}) \to E(\overline{K})$. Ist $\alpha \neq 0$ ein nicht separabler Endomorphismus, so gilt*

$$\deg \alpha > \# \ker(\alpha).$$

Beweis. Siehe Proposition 2.20 in [30]. □

Theorem A.2. *Sei E eine elliptische Kurve über einem Körper K und $\alpha \neq 0$ ein Endomorphismus auf E. dann ist $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektiv.*

Beweis. Siehe Theorem 2.21 in [30]. □

Proposition A.3. *Sei $q = p^r$ eine Primzahlpotenz, E eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$ und ϕ_q der Frobenius-Endomorphismus. Ist $(x, y) \in E(\overline{\mathbb{F}}_q)$, so gilt*

i. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$,

ii. $(x, y) \in E(\mathbb{F}_q)$ *gilt genau dann, wenn $\phi_q(x, y) = (x, y)$ ist.*

Beweis. Siehe Lemma 4.5 in [30]. □

B. Divisionspolynome

Sei E eine elliptische Kurve über einem Körper der Charakteristik ungleich 2 und 3, gegeben durch $Y^2 = X^3 + AX + B$ mit $A, B \in K$. Dann definieren wir die Divisionspolynome $\psi_m \in \mathbb{Z}[x, y, A, B],\ m \in \mathbb{N}$ durch

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2,\\
&\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),\ m \geq 3.
\end{aligned}$$

Damit definieren wir für $m \in \mathbb{N}$,

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Lemma B.1. *Ist n ungerade, so gilt $\psi_n \in \mathbb{Z}[x, y^2, A, B]$. Ist hingegen n gerade, so gilt $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$.*

Beweis. Siehe Lemma 3.4 in [30]. □

Lemma B.2. *Sei $n \in \mathbb{N}$. Dann gilt*

$$\begin{aligned}
\phi_n(x) &= x^{n^2} + \textit{Terme niedriger Ordnung},\\
\psi_n^2(x) &= n^2x^{n^2-1} + \textit{Terme niedriger Ordnung}.
\end{aligned}$$

Beweis. Siehe Lemma 3.5 in [30]. □

Mit Hilfe der Divisionspolynome können wir jetzt das Multiplizieren mit einer natürlichen Zahl explizit aufschreiben.

Theorem B.3. *Sei $P = (x, y)$ ein Punkt auf E und $n \in \mathbb{N}$. Dann gilt*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right).$$

Beweis. Siehe Theorem 9.31 in [30]. □

Literaturverzeichnis

[1] Michael F. Atiyah and Ian G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] R. Balasubramanian and Neal Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), no. 2, 141–145.

[3] Stanisław Balcerzyk and Tadeusz Józefiak, *Commutative Noetherian and Krull rings*, Ellis Horwood Series: Mathematics and its Applications, Ellis Horwood Ltd., Chichester, 1989, Translated from the Polish by Maciej Juniewicz and Sergiusz Kowalski.

[4] Dan Boneh and Matthew Franklin, *Identity-based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), no. 3, 586–615 (electronic).

[5] Siegfried Bosch, *Algebra*, Springer-Verlag, Berlin, 2003, 5., überarbeite Auflage.

[6] Leonard S. Charlap and David P. Robbins, *An elementary introduction to elliptic curves*, CRD Expository Report No. 31, December 1988.

[7] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[8] National Security Agency Information Assurance Directorate, *The Case for Elliptic Curve Cryptography*, `http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm`.

[9] Andreas Enge, *Elliptic curves and their applications to cryptograhpy: An introduction*, Kluwer Academic Publishers, Dordrecht, 1999.

[10] Gerhard Frey, Michael Müller, and Hans-Georg Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1717–1719.

[11] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[12] Florian Heß, *Kryptographie mit elliptischen kurven*, Computeralgebra Rundbrief, Ausgabe 39 (2006), 14–18.

[13] Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, and Edlyn Teske, *Analysis of the xedni calculus attack*, Des. Codes Cryptogr. **20** (2000), no. 1, 41–64.

[14] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, J. Cryptology **17** (2004), no. 4, 263–276.

[15] Jr. Kaliski, Burton S., *Elliptic curves and cryptography :a pseudorandom bit generator and other tools*, Ph.D. thesis, Massachusetts Institute of Technology, February 1988.

[16] Neal Koblitz, *A course in number theory and cryptography*, second ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1994.

[17] Ernst Kunz, *Einführung in die algebraische Geometrie*, Vieweg Studium: Aufbaukurs Mathematik, vol. 87, Friedrich Vieweg & Sohn, Braunschweig, 1997.

[18] Serge Lang, *Abelian varieties*, Interscience Tracts in Pure and Applied Mathematics. No. 7, Interscience Publishers, Inc., New York, 1959.

[19] ———, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[20] Arjen K. Lenstra and Eric R. Verheul, *Selecting cryptographic key sizes*, J. Cryptology **14** (2001), no. 4, 255–293.

[21] Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[22] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto, *Reducing elliptic curve logarithms to logarithms in a finite field*, STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing (New York, NY, USA), ACM Press, 1991, pp. 80–89.

[23] Certicom Press Release, *Certicom Announces Elliptic Curve Cryptosystem (ECC) Challenge Winner*, `http://www.certicom.com/index.php?action=company,press_archive&view=121`.

[24] Sun Microsystems Press Release, *SUN Microsystems Laboratories Contribute Next Generation Security Technologies To Open Source Project*, `http://www.sun.com/smi/Press/sunflash/2002-09/sunflash.20020918.17.xml`.

[25] Wolfgang M. Ruppert, *Algebraische Geometrie*, Vorlesung Wintersemester 1996/97, Universität Erlangen-Nürnberg, `http://www.mi.uni-erlangen.de/~ruppert/skripten/ag.ps.gz`.

[26] Victor Shoup, *Lower bounds for discrete logarithms and related problems*, Advances in cryptology—EUROCRYPT '97 (Konstanz), Lecture Notes in Comput. Sci., vol. 1233, Springer-Verlag, Berlin, 1997, pp. 256–266.

[27] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[28] ———, *The xedni calculus and the elliptic curve discrete logarithm problem*, Des. Codes Cryptogr. **20** (2000), no. 1, 5–40.

[29] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296.

[30] Lawrence C. Washington, *Elliptic curves*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2003, Number theory and cryptography.

[31] Oscar Zariski and Pierre Samuel, *Commutative algebra, Volume I*, The University Series in Higher Mathematics, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, With the cooperation of I. S. Cohen.

[32] ———, *Commutative algebra. Vol. II*, The University Series in Higher Mathematics, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1960.