Der Tate-Modul und die Weil-Paarung

Sommersemester 2015 bei Prof. Dr. K. Wingberg und O. Thomas

Dies ist die schriftliche Ausarbeitung des fünften Vortrages des Seminars über Elliptische Kurven, gehalten am 21.05.2015.

Wir werden zunächst in Abschnitt 1 die wichtigsten Definitionen und Eigenschaften projektiver Limites wiederholen und die l-adischen Zahlen einführen.

Daraufhin werden wir im zweiten Abschnitt den Tate-Modul einer elliptischen Kurve definieren und ihn benutzen, um Isogenien elliptischer Kurven besser zu verstehen. Außerdem werden wir einige Bemerkungen zu l-adischen Darstellungen der absoluten Galoisgruppe $\mathrm{Gal}(\overline{K}|K)$ assoziiert zu einer elliptischen Kurve machen.

Abschnitt 3 beschäftigt sich mit der Konstruktion und den Eigenschaften der Weil-Paarung auf einer elliptischen Kurve.

1 Projektive Limites

1.1 Definition. *Es seien $(G_n)_{n\in\mathbb{N}}$ eine Folge von Gruppen und $f_n\colon G_{n+1}\to G_n,\ n\in\mathbb{N}$, Gruppenhomomorphismen. Dann heißt*

$$G := \varprojlim_{n\in\mathbb{N}} G_n := \{(g_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} G_n \mid f_n(g_{n+1}) = g_n\ \forall n\in\mathbb{N}\}$$

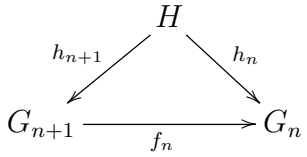
projektiver Limes von $(G_n, f_n)_{n\in\mathbb{N}}$. Die Abbildungen f_n heißen Übergangsabbildungen und die $\pi_m\colon G\to G_m, (g_n)_n\mapsto g_m$ Projektionen.

Der projektive Limes abelscher Gruppen ist wieder eine abelsche Gruppe. Analog definiert man den projektiven Limes von Ringen oder topologischen Räumen. Dabei versieht man im Falle topologischer Räume den projektiven Limes mit der kleinsten Topologie, sodass alle Projektionsabbildungen stetig sind. Diese stimmt mit der Teilraumtopologie der Produkttopologie überein.

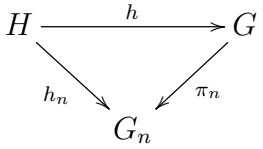
Der für uns wichtigste Speziallfall ist der von endlichen abelschen Gruppen oder Ringen, die wir mit der diskreten Topologie versehen. Es stellt sich dann heraus, dass der projektive Limes als abgeschlossener Teilraum des nun kompakten Produktraumes selbst kompakt und zusätzlich auch eine topologische abelsche Gruppe (bzw. ein topologischer Ring) ist, d. h., dass alle Gruppenoperationen stetig sind.

Auch kann als Indexmenge anstelle von $\mathbb{N}$ eine beliebige partiell geordnete Menge verwendet werden, wobei man dann eine Kompatibilitätsbedingung an die Übergangsabbildungen stellt.

1.2 Satz (Universelle Eigenschaft des projektiven Limes)**.** *Es seien (G_n, f_n) wie oben und H eine weitere Gruppe sowie $h_n\colon H\to G_n,\ n\in\mathbb{N}$, Gruppenhomomorphismen, sodass das Diagramm*



kommutativ ist für alle $n \in \mathbb{N}$. Dann gibt es genau einen Gruppenhomomorphismus $h\colon H \to G$, sodass für alle $n \in \mathbb{N}$ das Diagramm



kommutiert.

Falls die Gruppen G_n mehr Struktur besitzen, z. B. wenn es sich um Ringe oder topologische Gruppen handelt, so fordert man dementsprechend die gleiche Struktur von H und von den h_n und erhält, dass auch die Abbildung h jene Zusatzeigenschaften hat.

Kommen wir nun zum wichtigsten Beispiel, welches wir in Abschnitt 2 häufig verwenden werden.

1.3 Beispiel (l-adische Zahlen)**.** Es sei $l \in \mathbb{N}$ eine Primzahl. Wir betrachten die Ringe $\mathbb{Z}/l^n\mathbb{Z}$ zusammen mit den surjektiven Ringhomomorphismen

$$\mathbb{Z}/l^{n+1}\mathbb{Z} \to \mathbb{Z}/l^n\mathbb{Z}, \quad 1 \mapsto 1.$$

Dann heißt

$$\mathbb{Z}_l := \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$$

Ring der l-adischen ganzen Zahlen. $\mathbb{Z}_l$ ist ein kompakter, topologischer Ring, der zudem folgende Eigenschaften hat.

1. Ein Element $(a_0, a_1, a_2, \ldots) \in \mathbb{Z}_l$ mit $a_n \in \mathbb{Z}$, wobei diese Notation die Restklassenbildungen vernachlässigt, erfüllt $a_{n+1} \equiv a_n \bmod l^n$ für alle $n \in \mathbb{N}$. Sukzessive findet man also eindeutige Zahlen $b_0, b_1, \ldots \in \{0, \ldots, l-1\}$ mit

$$\begin{aligned} a_0 &\equiv b_0 && \bmod l \\ a_1 &\equiv b_0 + b_1 \cdot l && \bmod l^2 \\ a_2 &\equiv b_0 + b_1 \cdot l + b_2 \cdot l^2 && \bmod l^3 \\ &\vdots \end{aligned}$$

   Deswegen identifizieren wir das Element $(a_0, a_1, \ldots) \in \mathbb{Z}_l$ mit der Reihe $\sum_{k=0}^{\infty} b_k l^k$. Diese Reihe kann als konvergent aufgefasst werden, und die Abbildung

$$(a_0, a_1, \ldots) \mapsto \sum_{k=0}^{\infty} b_k l^k$$

   wird dann ein Ringisomorphismus, siehe Bemerkung 1.4. Damit lässt sich das Rechnen in $\mathbb{Z}_l$ als Addieren bzw. Multiplizieren „mit Übertrag“ interpretieren, also als die Fortsetzung des Rechnens in $\mathbb{Z}$ bzgl. der Basis l auf unendliche Reihen.

2. Wir erhalten die Abbildung $\mathbb{Z} \to \mathbb{Z}_l,\ z \mapsto (z, z, \ldots)$. Diese ist injektiv, der Ring $\mathbb{Z}_l$ hat damit Charakteristik 0. Die zu $(z, z, \ldots)$ gehörige Reihe ist gerade die Darstellung der ganzen Zahl z in Basis l, d. h. $z = \sum_{k=0}^{N} b_k l^k$.

3. $\mathbb{Z}_l$ ist nullteilerfrei: Sind nämlich $(a_n), (c_n) \in \mathbb{Z}_l$ ungleich 0, so gibt es $m, n \in \mathbb{N}_0$ mit $a_m \not\equiv 0 \mod l^{m+1}$ und $c_n \not\equiv 0 \mod l^{n+1}$. Dann gilt aber auch $a_{m+n} \cdot c_{m+n} \not\equiv 0 \mod l^{m+n+1}$, denn angenommen, dies wäre falsch, dann teilte l^{m+n+1} die Zahl $a_{m+n} \cdot c_{n+m}$, also teilte l^{m+1} die Zahl a_{m+n} oder l^{n+1} die Zahl c_{m+n} und damit folgte $a_m \equiv 0 \mod l^m$ oder $c_n \equiv 0 \mod l^n$.

4. $\mathbb{Z}_l$ ist ein lokaler Ring mit maximalem Ideal $l\mathbb{Z}_l$ und nach 3. auch nullteilerfrei, also ein diskreter Bewertungsring. Sein Quotientenkörper $\mathbb{Q}_l = \mathbb{Z}_l[\frac{1}{l}]$ heißt *Körper der l-adischen Zahlen*. Er hat Charakteristik 0. Analog zur Potenzreihendarstellung von Elementen von $\mathbb{Z}_l$ lassen sich Elemente von $\mathbb{Q}_l$ als Laurent-Reihen in Potenzen von l interpretieren, d. h. ein $x \in \mathbb{Q}_l$ entspricht einer Reihe der Form $\sum_{k=-N}^{\infty} b_k l^k$ mit $b_k \in \{0, \dots, l-1\}$.

1.4 Bemerkung (l-adische Zahlen als Vervollständigung)**.** Wir vergessen zunächst die gerade definierten Bezeichnungen und betrachten die Abbildung v_l auf $\mathbb{Q}$, die einer von Null verschiedenen rationalen Zahl den Exponenten von l in ihrer Primfaktorzerlegung zuordnet, d. h.

$$v_l\left(l^n \frac{a}{b}\right) = n, \quad n, a, b \in \mathbb{Z},\ a, b \neq 0 \text{ nicht durch } l \text{ teilbar}.$$

Zusätzlich definiert man $v_l(0) := \infty$. Es gilt

1. $v_l(xy) = v_l(x) + v_l(y)$ für alle $x, y \in \mathbb{Q}$,
2. $v_l(x+y) \geq \min\{v_l(x), v_l(y)\}$ für alle $x, y \in \mathbb{Q}$,
3. $v_l(x) = \infty \Leftrightarrow x = 0$.

Eine solche Abbildung nennt man *diskrete Bewertung*. Aus der Bewertung v_l lässt sich ein Betrag auf $\mathbb{Q}$ definieren, und zwar durch

$$|x|_l := l^{-v_l(x)}, \quad x \in \mathbb{Q}.$$

Obige Eigenschaften für v_l übertragen sich auf $|\cdot|_l$ wie folgt:

1. $|xy|_l = |x|_l |y|_l$ für alle $x, y \in \mathbb{Q}$,
2. $|x+y|_l \leq \max\{|x|_l, |y|_l\}$ für alle $x, y \in \mathbb{Q}$,
3. $|x|_l = 0 \Leftrightarrow x = 0$.

Die zweite Eigenschaft nennt man auch die *ultrametrische Dreiecksungleichung*. Sie ist stärker als die gewöhnliche Dreiecksungleichung. Aus diesem Betrag lässt sich via $(x, y) \mapsto |x-y|_l$ eine Metrik auf $\mathbb{Q}$ definieren und alle Körperoperationen sind stetig bzgl. dieser Metrik. Zwei rationale Zahlen x und y liegen in dieser Metrik nahe beieinander, wenn ihre Differenz durch eine hohe Potenz von l teilbar ist.

Nun kann man, analog zur Konstruktion der reellen Zahlen, den topologischen Körper $\mathbb{Q}$ vervollständigen und erhält einen vollständigen Körper, den wir ebenfalls $\mathbb{Q}_l$ nennen, zusammen mit einem Betrag $|\cdot|_l$ und einer isometrischen Einbettung $(\mathbb{Q}, |\cdot|_l) \hookrightarrow (\mathbb{Q}_l, |\cdot|_l)$. Vollständigkeit bedeutet, dass alle Cauchy-Folgen in $\mathbb{Q}_l$ auch in $\mathbb{Q}_l$ konvergent sind.

Es stellt sich heraus, dass der so konstruierte Körper mit dem Körper der l-adischen Zahlen aus Definition 1.3 übereinstimmt. Das werden wir kurz erläutern.

Zunächst definiert man $\mathbb{Z}_l$ als den Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_l$. Auf Grund der ultrametrischen Dreiecksungleichung lässt sich direkt zeigen, dass eine Reihe $\sum_{k=0}^{\infty} a_k$ genau dann in $\mathbb{Q}_l$ konvergiert, wenn a_k eine Nullfolge ist (jedwede Konvergenz bezieht sich ab jetzt immer auf die von $|\cdot|_l$ induzierte Metrik).

Insbesondere konvergieren alle Reihen der Form $\sum_{k=-N}^{\infty} b_k l^k$ mit $b_k \in \{0, \dots, l-1\}$ und $N \in \mathbb{N}_0$, denn es gilt $|b_k l^k|_l = l^{-k} \to 0,\ k \to \infty$. Nun lässt sich zeigen, dass sich jedes Element $x \in \mathbb{Q}_l$ eindeutig als eine solche Reihe schreiben lässt, und mehr noch, dass x genau dann in $\mathbb{Z}_l$ liegt, wenn $b_k = 0$ für alle $k < 0$ gilt. Wir erhalten also

$$\mathbb{Z}_l = \left\{ \sum_{k=0}^{\infty} b_k l^k \mid b_k \in \{0, \dots, l-1\} \right\}$$

sowie

$$\mathbb{Q}_l = \left\{ \sum_{k=-N}^{\infty} b_k l^k \mid b_k \in \{0, \dots, l-1\}, N \in \mathbb{N}_0 \right\}.$$

Außerdem ist der Betrag $|x|_l = l^{-v_l(x)}$ von $x = \sum_{k=-N}^{\infty} b_k l^k \in \mathbb{Q}_l$ explizit gegeben durch die diskrete Bewertung

$$v_l\left(\sum_{k=-N}^{\infty} b_k l^k \right) = \min\{k \mid b_k \neq 0\}.$$

Aus diesen Darstellungen lässt sich die Äquivalenz der Definition von $\mathbb{Z}_l$ als projektiver Limes zu der als Vervollständigung von $\mathbb{Z}$ zeigen. Abschließend sei noch erwähnt, dass

$$\mathbb{Z}_l = \{x \in \mathbb{Q}_l \mid |x|_l \leq 1\}$$

und

$$l\mathbb{Z}_l = \{x \in \mathbb{Q}_l \mid |x|_l < 1\}$$

gilt und dass $\mathbb{Z}_l$ gerade der Bewertungsring der diskreten Bewertung v_l auf $\mathbb{Q}_l$ ist.

2 Der Tate-Modul

Dieser Abschnitt folgt [Si, Chapter III.7]. Wir betrachten eine elliptische Kurve E definiert über einem Körper K. Ist $m \in \mathbb{N}_{\geq 2}$, gegebenenfalls teilerfremd zu $\mathrm{char}(K)$, falls diese positiv ist, so wissen wir aus dem letzten Vortrag, dass die Untergruppe der m-Torsionspunkte von E als abelsche Gruppe die folgende Struktur hat:

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

Allerdings besitzt $E[m]$ noch die Wirkung der absoluten Galoisgruppe $\mathrm{Gal}(\overline{K}|K)$ von K, denn weil E über K definiert ist, folgt aus $[m]P = 0$ auch $[m](P^\sigma) = ([m]P)^\sigma = 0$ für alle $P \in E$ und $\sigma \in \mathrm{Gal}(\overline{K}|K)$. Diese Wirkung geht unter dem reinen Gruppenisomorphismus verloren.

Die Idee des Tate-Moduls ist es, gewissermaßen unendliche viele dieser Torsionsuntergruppen simultan zu behandeln.

2.1 Definition. *Es sei E eine elliptische Kurve und l eine Primzahl. Der l-adische Tate-Modul von E ist*

$$T_l(E) := \varprojlim_n E[l^n],$$

wobei der projektive Limes bzgl. der Übergangsabbildungen

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

gebildet wird.

Da jedes $E[l^n]$ auf eindeutige Weise ein $\mathbb{Z}/l^n\mathbb{Z}$-Modul ist und damit auch

$$\begin{array}{ccc} \mathbb{Z}/l^{n+1}\mathbb{Z} \times E[l^{n+1}] & \longrightarrow & E[l^{n+1}] \\ \downarrow \quad \downarrow [l] & & \downarrow [l] \\ \mathbb{Z}/l^n\mathbb{Z} \times E[l^n] & \longrightarrow & E[l^n] \end{array}$$

kommutativ ist, erhalten wir durch Bildung des projektiven Limes, dass $T_l(E)$ ein $\mathbb{Z}_l$-Modul ist.

Die Struktur von $T_l(E)$ als $\mathbb{Z}_l$-Modul ist durch den folgenden Satz gegeben.

2.2 Satz ($T_l(E)$ als $\mathbb{Z}_l$-Modul)**.** *Es sei E eine elliptische Kurve über K und l eine Primzahl.*

1. *Falls $l \neq \mathrm{char}(K)$, so gilt $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ als $\mathbb{Z}_l$-Modul.*
2. *Falls $l = \mathrm{char}(K) > 0$, so gilt entweder $T_l(E) = 0$ oder $T_l(E) \cong \mathbb{Z}_l$ als $\mathbb{Z}_l$-Modul.*

Beweis. Nach [Si, III.6.4] ist $E[l^n]$ als abelsche Gruppe isomorph zu $\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$, falls $l \neq \mathrm{char}(K)$, und für $l = \mathrm{char}(K)$ gilt entweder $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z}$ für alle $n \in \mathbb{N}$ oder $E[l^n] = 0$ für alle $n \in \mathbb{N}$.

Zudem sind alle Übergangsabbildungen $[l]\colon E[l^{n+1}] \to E[l^n]$ surjektiv, weil $[l]$ auf E als nicht-konstante Isogenie (s. [Si, III.4.2]) surjektiv ist.

Weil außerdem projektive Limites mit Produkten vertauschen, erhält man die Behauptung durch Limes-Übergang. Hierbei muss man streng genommen schrittweise vorgehen und in jedem Schritt möglicherweise die vorher gewählten, leider nicht explizit gegebenen Isomorphismen $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ um einen Automorphismus von $\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ abändern, um mit dem nächsten kompatibel zu sein. □

Neben der $\mathbb{Z}_l$-Modulstruktur besitzt $T_l(E)$ auch eine Wirkung der absoluten Galoisgruppe $\mathrm{Gal}(\overline{K}|K)$ von K. Dies liegt daran, dass alle Übergangsabbildungen $[l]$, da sie über K definiert sind, mit der $\mathrm{Gal}(\overline{K}|K)$-Wirkung auf E vertauschen, d. h. es gilt $([l]P)^\sigma = [l](P^\sigma)$ für $P \in E$ und $\sigma \in \mathrm{Gal}(\overline{K}|K)$.

Durch Übergang zum projektiven Limes erhalten wir eine $\mathrm{Gal}(\overline{K}|K)$-Wirkung auf $T_l(E)$. Explizit:

$$(P_1, P_2, \ldots)^\sigma := (P_1^\sigma, P_2^\sigma, \ldots), \quad (P_1, P_2, \ldots) \in T_l(E), P_n \in E[l^n], \sigma \in \mathrm{Gal}(\overline{K}|K).$$

Diese Wirkung ist zudem stetig bzgl. der proendlichen Topologien auf $\mathrm{Gal}(\overline{K}|K)$ und auf $T_l(E)$, d. h. $\mathrm{Gal}(\overline{K}|K) \times T_l(E) \to T_l(E), (\sigma, P) \mapsto P^\sigma$ ist stetig. Außerdem wirkt jedes $\sigma \in \mathrm{Gal}(\overline{K}|K)$ durch einen $\mathbb{Z}_l$-Modul-Automorphismus auf $T_l(E)$.

2.3 Definition. *Die l-adische Darstellung von* $\mathrm{Gal}(\overline{K}|K)$ *assoziiert zu E ist der zu obiger Wirkung gehörende Homomorphismus*

$$\rho_l\colon \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)).$$

2.4 Bemerkung. Im Fall $l \neq \mathrm{char}(K)$ ist dies eine zweidimensionale Darstellung von $\mathrm{Gal}(\overline{K}|K)$, denn dann ist $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ und damit $\mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l)$, d. h. nach einer $\mathbb{Z}_l$-Basiswahl für $T_l(E)$ entspricht jedes ρ_l einer 2×2-Matrix mit Einträgen aus $\mathbb{Z}_l$. Das liefert

$$\rho_l\colon \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l) \subset \mathrm{GL}_2(\mathbb{Q}_l),$$

Dies ist nun eine Darstellung über einem Körper der Charakteristik 0, und mit solchen Darstellungen lässt sich gut umgehen.

2.5 Bemerkung (Tate-Modul von K)**.** Es sei $l \neq \mathrm{char}(K)$ eine Primzahl. Obige Konstruktion des Tate-Moduls von E ist sehr ähnlich zu der folgenden Konstruktion: Wir betrachten die Gruppe μ_{l^n} der l^n-ten Einheitswurzeln als Teilmenge von $\overline{K}^\times$. Wir haben die Übergangsabbildungen

$$\mu_{l^{n+1}} \to \mu_{l^n}, \quad \zeta \mapsto \zeta^l$$

und können damit den projektiven Limes

$$T_l(\mu) := \varprojlim_n \mu_{l^n}$$

bilden. Dieser heißt *l-adischer Tate-Modul von K* (bzw. von $\overline{K}^\times$).

Als abelsche Gruppen gilt $\mu_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$ und die Übergangsabbildungen sind surjektiv, sodass sich $T_l(\mu) \cong \mathbb{Z}_l$ als $\mathbb{Z}_l$-Modul ergibt.

Allerdings wirkt $\mathrm{Gal}(\overline{K}|K)$ auf jedem μ_{l^n} und diese Wirkung vertauscht mit den Übergangsabbildungen, sodass wir erneut eine stetige $\mathrm{Gal}(\overline{K}|K)$-Wirkung erhalten, diesmal auf $T_l(\mu)$, d. h. eine Darstellung

$$\chi\colon \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l(\mu)) \cong \mathbb{Z}_l^\times.$$

Dies ist nun (nach Einbetten in $\mathbb{Q}_l^\times$) eine eindimensionale Darstellung von $\mathrm{Gal}(\overline{K}|K)$.

Warum haben wir den Tate-Modul eingeführt? Weil er sich als sehr nützlich bei der Untersuchung von Isogenien herausstellt. Es sei nun

$$\Phi\colon E_1 \to E_2$$

eine Isogenie. Insbesondere induziert Φ Gruppenhomomorphismen $\Phi\colon E_1[l^n] \to E_2[l^n]$ und damit im Limes einen $\mathbb{Z}_l$-Modul-Homomorphismus

$$\Phi_l\colon T_l(E_1) \to T_l(E_2).$$

Wir erhalten also einen Gruppenhomomorphismus

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)), \quad \Phi \mapsto \Phi_l.$$

Der Homomorphismus Φ_l enthält genau die Information, wie die Isogenie Φ auf den l^n-Torsionspunkten von E_1 wirkt. Beachte: Im Falle $E_1 = E_2 = E$ ist $\Phi \mapsto \Phi_l$ sogar ein Ringhomomorphismus (mit der Komposition von Abbildungen als Multiplikation).

Zentral ist das folgende Theorem:

2.6 Theorem. *Es seien E_1, E_2 elliptische Kurven und $l \neq \mathrm{char}(K)$ eine Primzahl. Dann ist*

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)), \quad \Phi = \sum_i \Phi_i \otimes z_i \mapsto \Phi_l := \sum_i z_i \Phi_{i,l}$$

injektiv.

Für den Beweis benötigen wir folgendes Lemma:

2.7 Lemma. *Es sei $M \subset \mathrm{Hom}(E_1, E_2)$ eine endlich erzeugte Untergruppe und*

$$M^{\mathrm{div}} := \{\Phi \in \mathrm{Hom}(E_1, E_2) \mid \exists m \in \mathbb{N}\colon [m] \circ \Phi \in M\}.$$

Dann ist auch M^{div} endlich erzeugt.

Beweis. Wir haben die Gradabbildung

$$\deg\colon \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

und möchten diese nun fortsetzen auf $M \otimes_{\mathbb{Z}} \mathbb{R}$. Hierzu benötigen wir die Aussage [Si, III.6.3], die besagt, dass obige Abbildung deg eine positiv definite, quadratische Form ist, d. h. dass für alle $\Phi, \Psi \in \mathrm{Hom}(E_1, E_2)$ gilt

1. $\deg(\Phi) = \deg(-\Phi)$.
2. Die Paarung $\langle \Phi, \Psi \rangle := \deg(\Phi + \Psi) - \deg(\Phi) - \deg(\Psi)$ ist bilinear.
3. $\deg(\Phi) \geq 0$ und $\deg(\Phi) = 0$ genau dann, wenn $\Phi = 0$.

Mit diesen Eigenschaften lässt sich deg durch obige Bilinearform $\langle \cdot, \cdot \rangle$ darstellen. Man setze nämlich $\Psi = -\Phi$ und erhält dann

$$\deg \Phi = \frac{1}{2}\langle \Phi, \Phi \rangle.$$

Da M endlich erzeugt ist, ist $M \otimes_{\mathbb{Z}} \mathbb{R}$ ein endlich dimensionaler $\mathbb{R}$-Vektorraum. Darauf definieren wir nun

$$\deg\colon M \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}, \quad \deg\left(\sum_i \Phi_i \otimes x_i\right) := \frac{1}{2} \sum_{i,j} x_i x_j \langle \Phi_i, \Phi_j \rangle.$$

Alternativ kann man auch zuerst eine $\mathbb{Z}$-Basis $\{e_1, \ldots, e_t\}$ für M wählen (nach [Si, III.4.2] ist $\mathrm{Hom}(E_1, E_2)$ und damit M nämlich torsionsfrei und als endlich erzeugte abelsche Gruppe damit frei). Dann ist $\{e_1 \otimes 1, \ldots, e_t \otimes 1\}$ eine $\mathbb{R}$-Vektorraum-Basis für $M \otimes_{\mathbb{Z}} \mathbb{R}$ und $\deg(\sum_i x_i e_1 \otimes 1) = \frac{1}{2} \sum_{i,j} x_i x_j \langle e_i, e_j \rangle$, $x_i \in \mathbb{R}$.

An dieser Darstellung liest man sofort ab, dass deg stetig ist bzgl. der Standardtopologie auf dem endlich-dimensionalen $\mathbb{R}$-Vektorraum $M \otimes_{\mathbb{Z}} \mathbb{R}$. Damit ist

$$U := \{\Phi \in M \otimes_{\mathbb{Z}} \mathbb{R}\colon \deg(\Phi) < 1\}$$

eine offene Teilmenge von $M \otimes_{\mathbb{Z}} \mathbb{R}$.

Nun nutzen wir aus, dass torsionsfreie abelsche Gruppen flach sind. Zunächst ist deswegen $\mathbb{R}$ ein flacher $\mathbb{Z}$-Modul und damit liefert die Inklusion $M \subset M^{\mathrm{div}}$ eine injektive Abbildung

$$M \otimes_{\mathbb{Z}} \mathbb{Z} \hookrightarrow M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{R}, \quad \Phi \otimes x \mapsto \Phi \otimes x.$$

Diese Abbildung ist auch surjektiv und damit ein Isomorphismus, denn ist $\Phi \otimes x \in M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{R}$ einer der Erzeuger von $M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{R}$, so gibt es ein $m \in \mathbb{N}$ mit $m\Phi = [m] \circ \Phi \in M$. Dann wird $m\Phi \otimes \frac{x}{m} \in M \otimes_{\mathbb{Z}} \mathbb{R}$ abgebildet auf $m\Phi \otimes \frac{x}{m} = \Phi \otimes x \in M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{R}$.

Weiter ist auch M^{div} torsionsfrei, da $\mathrm{Hom}(E_1, E_2)$ torsionsfrei ist, und damit erhalten wir

$$M^{\mathrm{div}} \cong M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{Z} \hookrightarrow M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{R} \cong M \otimes_{\mathbb{Z}} \mathbb{R}.$$

Mit Hilfe dieser injektiven Abbildung lässt sich M^{div} als Untergruppe des endlich dimensionalen $\mathbb{R}$-Vektorraums $M \otimes_{\mathbb{Z}} \mathbb{R}$ auffassen. Weil diese Abbildung zudem den Grad deg respektiert und jedes $\Phi \in M^{\mathrm{div}} \setminus \{0\}$ Grad ≥ 1 hat, gilt $M^{\mathrm{div}} \cap U = \{0\}$. Mit anderen Worten: M^{div} ist eine diskrete Untergruppe eines endlich dimensionalen $\mathbb{R}$-Vektorraumes und damit endlich erzeugt. □

Beweis von Theorem 2.6. Sei $\Phi \in \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ mit $\Phi_l = 0$. Sei $M \subset \mathrm{Hom}(E_1, E_2)$ eine endlich erzeugte Untergruppe mit $\Phi \in M \otimes_{\mathbb{Z}} \mathbb{R}$. Nach Lemma 2.7 ist dann M^{div} ebenfalls endlich erzeugt, und wegen der Torsionsfreiheit von $\mathrm{Hom}(E_1, E_2)$ ist M^{div} eine freie abelsche Gruppe. Sei also

$$\psi_1, \ldots, \psi_t \in \mathrm{Hom}(E_1, E_2)$$

eine $\mathbb{Z}$-Basis von M^{div}.

Das ist auch eine $\mathbb{Z}_l$-Basis für $M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ und damit erhalten wir (beachte, dass $\mathbb{Z}_l$ torsionsfrei ist und damit $M \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow M^{\mathrm{div}} \otimes_{\mathbb{Z}} \mathbb{Z}_l$)

$$\Phi = \alpha_1\psi_1 + \ldots + \alpha_t\psi_t, \quad \alpha_1, \ldots, \alpha_t \in \mathbb{Z}_l.$$

Sei nun $n \in \mathbb{N}$ fest gewählt sowie $a_1, \ldots, a_n \in \mathbb{Z}$ mit

$$a_i \equiv \alpha_i \pmod{l^n}.$$

Definiere

$$\psi := [a_1] \circ \psi_1 + \ldots + [a_t] \circ \psi_t \in \mathrm{Hom}(E_1, E_2).$$

Da $\Phi_l = 0$ gilt, Φ also alle l^n-Torsionspunkte auf O abbildet, folgt $\psi(P) = O$ für alle $P \in E_1[l^n]$. Detaillierter: In dem kommutativen Diagramm

$$\begin{array}{ccc} T_l(E_1) & \xrightarrow{\Phi_l} & T_l(E_2) \\ {\scriptstyle \pi_n^1}\downarrow & & \downarrow{\scriptstyle \pi_n^2} \\ E_1[l^n] & \xrightarrow[\Phi^{(n)}]{} & E_2[l^n] \end{array}$$

bezeichne π_n^j die Projektion auf die n-te Komponente von $T_l(E_j)$ und $\Phi^{(n)}$ die Wirkung von Φ auf den l^n-Torsionpunkten, gegeben durch $P \mapsto \sum_{i=1}^{t} (\alpha_i \bmod l^n)\psi_i(P)$. Nun ist $\Phi_l = 0$, π_n^1 surjektiv und damit $O = \Phi^{(n)}(P) = \sum_{i=1}^{t} (\alpha_i \bmod l^n)\psi_i(P) = \psi(P)$.

Nun benutzen wir [Si, III.4.11], eine Art Homomorphisatz für Isogenien, mit der separablen Isogenie $[l^n]\colon E_1 \to E_1$ (genau an dieser Stelle benötigen wir $l \neq \mathrm{char}(K)$) und erhalten eine Isogenie $\lambda \in \mathrm{Hom}(E_1, E_2)$ mit

$$\psi = \lambda \circ [l^n] = [l^n] \circ \lambda,$$

wobei die zweite Gleichheit nur benutzt, dass die Isogenie λ ein Gruppenhomomorphismus ist.

Damit gilt $\lambda \in M^{\mathrm{div}}$ (genau an dieser Stelle benötigen wir M^{div} und obiges Lemma), es gibt also $b_1, \ldots, b_t \in \mathbb{Z}$ mit

$$\lambda = [b_1] \circ \psi_1 + \ldots + [b_t] \circ \psi_t.$$

Daraus folgt

$$[a_1] \circ \psi_1 + \ldots + [a_t] \circ \psi_t = \psi = [l^n] \circ \lambda = [l^n b_1] \circ \psi_1 + \ldots + [l^n b_t] \circ \psi_t.$$

Da die ψ_i eine $\mathbb{Z}$-Basis von M^{div} bilden, folgt daraus

$$a_i = l^n b_i,$$

also

$$\alpha_i \equiv 0 \pmod{l^n}.$$

Da n beliebig war, folgt $\alpha_i = 0$ für alle i und damit $\Phi = 0$. □

2.8 Korollar. *Es seien E_1, E_2 elliptische Kurven. Dann gilt*

$$\mathrm{Rang}_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2) \leq 4.$$

Beweis. Wir wählen eine Primzahl $l \neq \mathrm{char}(K)$. Dann gilt

$$\begin{aligned}
\mathrm{Rang}_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2) &= \dim_{\mathbb{Q}} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q} && \text{(nach Definition)} \\
&= \dim_{\mathbb{Q}_l} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}_l && \text{(wähle z. B. eine } \mathbb{Q}\text{-Basis)} \\
&= \dim_{\mathbb{Q}_l} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l && (\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}_l = \mathbb{Q}_l = \mathbb{Z}_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) \\
&= \mathrm{Rang}_{\mathbb{Z}_l} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l && \text{(nach Definition)} \\
&\leq \mathrm{Rang}_{\mathbb{Z}_l} \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) && \text{(wegen Theorem 2.6)} \\
&= 4 && \text{(wegen } T_l(E_i) \cong \mathbb{Z}_l \times \mathbb{Z}_l).
\end{aligned}$$

□

Wir beenden diesen Abschnitt mit einem kleinen Ausblick über weitere Resultate.

2.9 Bemerkung. Eine Isogenie heißt *über K definiert*, falls sie mit der $\mathrm{Gal}(\overline{K}|K)$-Wirkung vertauscht. Die Gruppe aller über K definierten Isogenien bezeichnen wir mit

$$\mathrm{Hom}_K(E_1, E_2).$$

Analog definiert man

$$\mathrm{Hom}_K(T_l(E_1,), T_l(E_2))$$

als die Menge derjenigen $\mathbb{Z}_l$-linearen Abbildungen von $T_l(E_1)$ nach $T_l(E_2)$, die mit der $\mathrm{Gal}(\overline{K}|K)$-Wirkung vertauschen.

Aus Theorem 2.6 folgt für eine Primzahl $l \neq \mathrm{char}(K)$ sofort die Injektivität von

$$\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2)).$$

Tatsächlich stellt sich im folgenden, sehr tiefliegenden Theorem heraus, dass diese Abbildung oft ein Isomorphismus ist.

2.10 Theorem (Isogenie-Theorem)**.** *Es sei $l \neq \mathrm{char}(K)$ eine Primzahl. Ist K ein endlicher Körper oder ein Zahlkörper, so ist*

$$\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2))$$

ein Isomorphismus.

Wir kehren noch einmal zu den in Definition 2.3 eingeführten l-adischen Darstellungen

$$\rho_l \colon \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E))$$

zurück. Für diese gilt der folgende Satz.

2.11 Theorem (Serre)**.** *Es sei K ein Zahlkörper und E über K eine elliptische Kurve ohne komplexe Multiplikation, d. h. mit $\mathrm{End}(E) \cong \mathbb{Z}$. Dann gilt*

1. *$\rho_l(\mathrm{Gal}(\overline{K}|K))$ hat endlichen Index in $\mathrm{Aut}_{\mathbb{Z}_l}(T_l(E))$ für alle Primzahlen l.*
2. *$\rho_l(\mathrm{Gal}(\overline{K}|K)) = \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E))$ für fast alle Primzahlen l.*

3 Die Weil-Paarung

In diesem Abschnitt, der [Si, Chapter III.8] folgt, sei E stets eine elliptische Kurve über einem Körper K und $m \in \mathbb{N}_{\geq 2}$ eine natürliche Zahl, welche im Fall $\mathrm{char}(K) = p > 0$ teilerfremd zu p sei.

Nach Wahl einer $\mathbb{Z}/m\mathbb{Z}$-Basis $\{T_1, T_2\}$ für $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (als abelsche Gruppe) erhalten wir duch die Determinante

$$\det \colon E[m] \times E[m] \to \frac{\mathbb{Z}}{m\mathbb{Z}}, \quad (aT_1 + bT_2, cT_1 + dT_2) \mapsto ad - bc$$

eine nicht-entartete, bilineare Paarung, die selbstverständlich nicht von der gewählten Basis abhängt. Dabei missachten wir allerdings, dass $E[m]$ eine Wirkung der absoluten Galoisgruppe $\mathrm{Gal}(\overline{K}|K)$ besitzt und die Paarung det im Allgemeinen nicht kompatibel mit dieser Wirkung ist.

Ziel dieses Abschnittes ist es deswegen, eine modifizierte, Galois-kompatible Paarung zu konstruieren.

Da wir im Folgenden häufig mit (Haupt-)Divisoren auf elliptischen Kurven umgehen werden, benötigen wir zunächst ein Lemma.

3.1 Lemma (Hauptdivisoren auf E)**.** *Es sei $D = \sum_P n_p(P) \in \mathrm{Div}(E)$. Dann gilt*

1. *D ist genau dann ein Hauptdivisor, wenn $\sum_P n_P = 0$ und $\sum_P [n_p]P = O$.*

2. *Falls $D = \operatorname{div}(f)$ ein Hauptdivisor ist, so ist $f \in \overline{K}(E)^\times$ bis auf Konstanten aus $\overline{K}^\times$ eindeutig bestimmt.*

Beweis. 1. Da Hauptdivisoren immer Grad 0 haben (s. [Si, II.3.1]), sei ohne Einschränkung $D \in \operatorname{Div}^0(E)$, d. h. $\sum_P n_P = 0$. Nach [Si, III.3.4] ist E als abelsche Gruppe isomorph zur Picard-Gruppe $\operatorname{Pic}^0(E)$. Dieser Isomorphismus ist gegeben durch

$$\sigma^{-1} \colon E \to \operatorname{Pic}^0(E), \quad P \mapsto \overline{(P) - (O)}.$$

Nun ist D genau dann ein Hauptdivisor, wenn sein Bild $\overline{D}$ in $\operatorname{Pic}^0(E)$ Null ist, d. h. genau dann, wenn

$$\begin{aligned} 0 = \sigma(\overline{D}) &= \sigma\Big(\sum n_P(P)\Big) = \sigma\Big(\sum n_P(P) - \sum n_P(O)\Big) = \sigma\Big(\sum n_P\big((P) - (O)\big)\Big) \\ &= \sum [n_P]\sigma\big((P) - (O)\big) = \sum [n_P]P, \end{aligned}$$

wobei wir hier ab der zweiten Gleichheit nicht mehr notationell zwischen einem Divisor und seiner Restklasse in $\operatorname{Pic}^0(E)$ unterscheiden und in der dritten Gleichheit verwenden, dass $\sum n_P = 0$ gilt.

2. Wir verwenden [Si, II.5.5], ein Korollar zum Satz von Riemann-Roch, welches besagt, dass für einen Divisor D von Grad $\deg(D) \geq 1$ gilt:

$$\dim_{\overline{K}} \mathcal{L}(D) = \deg(D),$$

wobei $\mathcal{L}(D) = \{g \in \overline{K} \mid \operatorname{div}(g) \geq -D\} \cup \{0\}$ (beachte, dass das Geschlecht einer elliptischen Kurve 1 ist).

Zu $D = \operatorname{div}(f)$ definiere $\tilde{D} := D + (\tilde{P})$, wobei $\tilde{P} \in E$ beliebig. Dann hat $\tilde{D}$ Grad 1, somit liefert obiger Satz $\dim_{\overline{K}} \mathcal{L}(\tilde{D}) = 1$. Weiter gilt $0 \neq \frac{1}{f} \in \mathcal{L}(D) \subset \mathcal{L}(\tilde{D})$, also ist auch $\mathcal{L}(D)$ eindimensional und $\frac{1}{f}$ eine $\overline{K}$-Basis davon.

Hat nun ein $g \in \overline{K}(E)^\times$ ebenfalls Divisor D, so gilt $\frac{1}{g} \in \mathcal{L}(D) = \overline{K} \cdot \frac{1}{f}$ und somit $g = c \cdot f$ für ein $c \in \overline{K}^\times$.

□

3.2 Konstruktion (Weil-Paarung)**.** Es sei $T \in E[m]$. Wähle ein $f \in \overline{K}(E)$ mit

$$\boxed{\operatorname{div}(f) = m(T) - m(O).}$$

Solch ein f existiert nach Lemma 3.1. Es sei weiter $T' \in E[m]$ mit $[m]T' = T$. Dann gibt es ein $g \in \overline{K}(E)$ mit

$$\boxed{\operatorname{div}(g) = [m]^*(T) - [m]^*(O)} = \sum_{R \in E[m]} \big((T' + R) - (R)\big).$$

Die Existenz von g folgt erneut aus Lemma 3.1, denn es gilt

- $[m]^*(Q) = \sum_{P \colon [m]P = Q} e_{[m]}(P)(P)$, und da $[m]$ separabel ist, ist $e_{[m]}(P) = 1$ ([Si, III.4.10, III.5.4]) für alle $P \in E$. Damit folgt erstens, dass $[m]^*(T) - [m]^*(O)$ Grad 0 hat, und zweitens, dass dieser Divisor gleich $\sum_R \big((T' + R) - (R)\big)$ ist.

- $\sum_R (T' + R - R) = [m^2]T' = [m]T = O$.

Weiter gilt

$$\operatorname{div}(f \circ [m]) = \sum_P \operatorname{ord}_P(f \circ [m])(P) = m[m]^*(T) - m[m]^*(O) = m \operatorname{div}(g) = \operatorname{div}(g^m),$$

da die Null- bzw. Polstellen von $f \circ [m]$ genau die Urbilder der Null- bzw. Polstelle von f unter $[m]$ sind und die jeweiligen Ordnungen dabei erhalten werden. Nach dem zweiten Teil von Lemma 3.1 können wir also durch Abändern von f um eine Konstante erreichen, dass gilt:

$$\boxed{f \circ [m] = g^m.}$$

Sei nun $S \in E[m]$ ($S = T$ ist erlaubt). Dann gilt für alle $X \in E$:

$$g(X+S)^m = f([m]X + [m]S) = f([m]X] = g(X)^m,$$

also nimmt der Morphismus $E \to \mathbb{P}^1,\ X \mapsto \frac{g(X+S)}{g(X)}$ nur m-te Einheitswurzeln als Bilder an, ist somit nicht surjektiv und deswegen nach [Si, II.2.3] konstant.

Definiere damit die *Weil-Paarung*

$$e_m \colon E[m] \times E[m] \to \mu_m, \quad e_m(S,T) := \frac{g(X+S)}{g(X)},$$

wobei $X \in E$ ein beliebiger Punkt sei, sodass $g(X)$ und $g(X+S)$ definiert und ungleich 0 sind. Solch ein X existiert immer, da g und damit auch die verschobene Funktion $g(\cdot + S)$ nur endlich viele Null- und Polstellen besitzt, E aber unendlich viele Punkte hat.

Beachte: In der Konstruktion von $e_m(S,T)$ benutzt man also zuerst T, um die Funktionen f und g zu erhalten. Am Ende setzt man den Punkt S „in g“ ein. Dabei ist es nicht schlimm, dass g nur bis auf eine Konstante eindeutig bestimmt ist, denn diese kürzt sich in obigem Bruch wieder heraus.

Schließlich sei noch erwähnt, dass die Funktion f nur eine Hilfsgröße ist, die in den folgenden Rechnungen dem besseren Überblick dient. In die Definition von $e_m(S,T)$ geht nur die Funktion g ein.

3.3 Satz. *Die Weil-Paarung e_m ist*

1. *bilinear, d. h. für alle $S, S_1, S_2, T, T_1, T_2 \in E[m]$ gilt*

$$e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T),$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2).$$

2. *alternierend, d. h. für alle $T \in E[m]$ gilt*

$$e_m(T,T) = 1$$

und damit insbesondere für alle $S, T \in E[m]$ auch

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

3. *nicht ausgeartet, d. h. falls $e_m(S,T) = 1$ für alle $S \in E[m]$, dann folgt $T = 0$.*

4. *Galois-äquivariant, d. h. für alle* $S, T \in E[m]$ *und* $\sigma \in \mathrm{Gal}(\overline{K}|K)$ *gilt*

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma).$$

5. *kompatibel, d. h. für alle* $m' \in \mathbb{N}_{\geq 2}$, $p \nmid m'$, $S \in E[mm']$ *und* $T \in E[m]$ *gilt*

$$e_{mm'}(S,T) = e_m([m']S, T).$$

Beweis. Ein ausführlicher Beweis ist zu finden in [Si, III.8.1]. Wir zeigen beispielhaft die erste Aussage. Es seien dazu f und g wie in 3.2. Linearität im ersten Argument folgt aus

$$e_m(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X)}\frac{g(X+S_1)}{g(X+S_1)} = e_m(S_2,T)e_m(S_1,T),$$

wobei $X \in E$ so gewählt sei, dass alle Ausdrücke hier existieren.

Zum Beweis der Linearität im zweiten Argument seien $f_1, f_2, f_3, g_1, g_2, g_3$ die Funktionen aus Konstruktion 3.2, die zu den Punkten T_1,T_2 und $T_3 := T_1 + T_2$ gehören. Wir benötigen einen Zusammenhang zwischen diesen Funktionen. Sei dazu $h \in \overline{K}(E)$ mit

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

Die Existenz von h folgt erneut mit Lemma 3.1. Damit gilt

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = m\,\mathrm{div}(h).$$

Nach der zweiten Aussage von Lemma 3.1 gibt es ein $c \in \overline{K}^\times$ mit

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

Potenzieren liefert

$$g_3^m = f_3 \circ [m] = c f_1 f_2 h^m \circ [m] = c g_1^m g_2^m (h \circ [m])^m$$

und anschließendes Ziehen der m-ten Wurzel ergibt

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

für ein $c' \in \overline{K}$. Es ergibt sich somit

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

wobei wir im letzten Schritt $[m]S = O$ ausnutzen. □

3.4 Korollar. *Es gibt* $S, T \in E[m]$, *sodass* $e_m(S,T)$ *eine primitive* m*-te Einheitswurzel ist. Insbesondere ist* e_m *surjektiv, und falls* $E[m] \subset E(K)$, *so folgt* $\mu_m \subset K^\times$.

Beweis. Wir wählen unter dem Isomorphismus $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ Urbilder S und T von $(1,0)$ und $(0,1)$. Es wird sich herausstellen, dass $e_m(S,T)$ eine primitive m-te Einheitswurzel ist.

Nehmen wir an, dass $e_m(S,T)^d = 1$ gilt. Dann gilt für alle $a, b \in \mathbb{Z}$, da die Paarung bilinear und alternierend ist:

$$e_m([a]S + [b]T, [d]T) = e_m(S,T)^{ad} e_m(T,T)^{bd} = 1.$$

Wegen der Nicht-Ausgeartetheit und der Wahl von S und T folgt damit $[d]T = O$ und somit $m|d$, also hat $e_m(S,T)$ Ordnung m und ist eine primitive m-te Einheitswurzel.

Für die zweite Aussage nutzen wir die Galois-Äquivarianz aus: Ist $E[m] \subset E(K)$, so folgt für alle $\sigma \in \mathrm{Gal}(\overline{K}|K)$ und $S, T \in E[m]$:

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T).$$

Nach Galoistheorie folgt daraus $e_m(S,T) \in K$. Da e_m nach der ersten Aussage surjektiv ist, folgt also $\mu_m \subset K^\times$. □

Zu obigen Eigenschaften der Weil-Paarung kommt noch hinzu, dass die duale Isogenie $\hat{\Phi}$ einer Isogenie Φ adjungiert zu Φ bzgl. der Weil-Paarung ist. Zur Erinnerung: Ist $\Phi\colon E_1 \to E_2$ eine Isogenie, so gibt es die duale Isogenie $\hat{\Phi}\colon E_2 \to E_1$ mit $\hat{\Phi} \circ \Phi = [\deg \Phi]$, siehe [Si, Chapter III.6] für die Definition und die Eigenschaften der dualen Isogenie.

3.5 Satz. *Es seien E_1, E_2 elliptische Kurven über K und $\Phi\colon E_1 \to E_2$ eine Isogenie. Dann gilt für alle $S \in E_1[m]$ und $T \in E_2[m]$*

$$e_m\big(S, \hat{\Phi}(T)\big) = e_m\big(\Phi(S), T\big).$$

Beweisskizze. Man muss die Funktionen $f, g \in \overline{K}(E_2)$, die zum Punkt T gehören, in Bezug bringen zu den entsprechenden Funktionen zu $\hat{\Phi}(T)$. Dies funktioniert ähnlich zum Beweis des ersten Teils von Satz 3.3.

Man benutzt die Darstellung [Si, III.6.1], die $\hat{\Phi}$ als Gruppenhomomorphismus beschreibt, sowie Lemma 3.1, um eine Funktion $h \in \overline{K}(E_1)$ zu finden mit

$$\mathrm{div}(h) = \Phi^*\big((T)\big) - \Phi^*\big((O)\big) - \big(\hat{\Phi}T\big) + \big(O\big).$$

Durch Berechnung der Divisoren jener Funktionen stellt sich heraus, dass $\frac{f\circ\Phi}{h^m}$ die Rolle von f und $\frac{g\circ\Phi}{h\circ[m]}$ die von g für den Punkt $\hat{\Phi}(T)$ erfüllen. Damit ergibt sich schließlich

$$e_m(S, \hat{\Phi}T) = \frac{\frac{g\circ\Phi}{h\circ[m]}(X+S)}{\frac{g\circ\Phi}{h\circ[m]}(X)} = \frac{g(\Phi X + \Phi S)}{g(\Phi X)} \frac{h([m]X + [m]S)}{h([m]X)} = e_m(\Phi S, T),$$

wobei wir im letzten Schritt die Definition von $e_m(\Phi S, T)$ (mit ΦX anstelle von X) sowie $[m]S = O$ verwendet haben. □

Zum Abschluss dieser Arbeit verbinden wir die Abschnitte 2 und 3, d. h. wir benutzen die gerade hergeleiteten Eigenschaften der Weil-Paarung e_m, um eine Paarung auf dem Tate-Modul der elliptischen Kurve zu konstruieren.

Sei dazu $l \neq \mathrm{char}(K)$ eine Primzahl. Wir haben die Weil-Paarungen

$$e_{l^n}\colon E[l^n] \times E[l^n] \to \mu_{l^n}$$

für alle $n \in \mathbb{N}$ und werden diese nun kombinieren, um die *l-adische Weil-Paarung*

$$e\colon T_l(E) \times T_l(E) \to T_l(\mu)$$

auf dem Tate-Modul von E zu erhalten. Dazu müssen wir überprüfen, ob die Paarungen e_{l^n} mit den Übergangsabbildungen

$$[l]\colon E[l^{n+1}] \to E[l^n]$$

und

$$(\cdot)^l\colon \mu_{l^{n+1}} \to \mu_{l^n}, \quad \zeta \mapsto \zeta^l$$

verträglich sind. Mit anderen Worten: Die Kommutativität des Diagramms

$$\begin{array}{ccc} E[l^{n+1}] \times E[l^{n+1}] & \xrightarrow{e_{l^{n+1}}} & \mu_{l^{n+1}} \\ \downarrow{\scriptstyle [l]} \quad \downarrow{\scriptstyle [l]} & & \downarrow{\scriptstyle (\cdot)^l} \\ E[l^n] \times E[l^n] & \xrightarrow[e_{l^n}]{} & \mu_{l^n} \end{array}$$

ist zu zeigen. Sei dazu $S, T \in E[l^{n+1}]$. Dann ist

$$e_{l^n}([l]S, [l]T) = e_{l^{n+1}}(S, T)^l$$

zu zeigen. Dies folgt aus Satz 3.3 (e) und (a):

$$e_{l^n}([l]S, [l]T) = e_{l^{n+1}}(S, [l]T) = e_{l^{n+1}}(S, T)^l.$$

Alle Eigenschaften der Weil-Paarung übertragen sich und wir erhalten den folgenden Satz.

3.6 Satz. *Es sei $l \neq \mathrm{char}(K)$ eine Primzahl. Dann gibt es eine $\mathbb{Z}_l$-bilineare, alternierende, nicht-entartete, Galois-äquivariante Paarung*

$$e\colon T_l(E) \times T_l(E) \to T_l(\mu).$$

Ist außerdem $\Phi\colon E_1 \to E_2$ eine Isogenie und bezeichne $\Phi_l\colon T_l(E_1) \to T_l(E_2)$ die dazu assoziierte Abbildung der Tate-Moduln (vgl. Bemerkung vor Theorem 2.6), so gilt

$$e(\Phi_l S, T) = e(S, \hat{\Phi}_l T)$$

für alle $S \in T_l(E_1)$ und $T \in T_l(E_2)$.

Literatur

[Si] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106. Springer, Dordrecht, Heidelberg, London, New York, 2009.