Der Tate-Modul und die Weil-Paarung

Seminar Elliptische Kurven - Wintersemester 2012/2013
bei Prof. Dr. K. Wingberg und K. Hübner

1. Der Tate-Modul

Sei E/K eine elliptische Kurve und $m \geq 2$ eine ganze Zahl, die teilerfremd zu $\mathrm{char}(K)$ ist, falls $\mathrm{char}(K) > 0$. Wie wir im vorherigen Vortrag gesehen haben, gilt dann

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),$$

wobei es sich hier um einen Isomorphismus abstrakter Gruppen handelt. Die Gruppe $E[m]$ besitzt noch mehr Struktur. Die Galoisgruppe $G_{\bar{K}/K}$ operiert auf $E[m]$, denn falls $[m]P = O$, so gilt $[m](P^\sigma) = ([m]P)^\sigma = O$. Wir erhalten also eine Darstellung

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

wobei der letzte Isomorphismus duch Basiswahl gegeben ist. Diese Darstellungen sind aber für jedes m einzeln betrachtet nicht zufriedenstellend, da es generell am einfachsten ist, Darstellungen zu betrachten, deren Matrizen Koeffizienten in einem Ring der Charakteristik 0 besitzen. Wir werden im Folgenden variierende m zusammenfügen, sodass wir eine solche Darstellung erhalten. Dabei gleicht die Konstruktion der Konstruktion der ℓ-adischen Zahlen $\mathbb{Z}_\ell$ als projektiver Limes der endlichen Gruppen $\mathbb{Z}/\ell^n\mathbb{Z}$.

1.1. Definition. *Sei E eine elliptische Kurve und $\ell \in \mathbb{Z}$ prim. Der **(ℓ-adische) Tate-Modul** von E ist die Gruppe*

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

wobei der projektive Limes bezüglich der natürlichen Abbildungen

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

gebildet wird. Da jedes $E[\ell^n]$ ein $\mathbb{Z}/\ell^n\mathbb{Z}$-Modul ist, erhält der Tate-Modul eine natürliche Struktur als $\mathbb{Z}_\ell$-Modul.

1.2. Bemerkung. Da die Multipliakationsabbildungen $[\ell]$ surjektiv sind, entspricht die Topologie, die der Tate Modul als projektiver Limes trägt, der ℓ-adischen Topologie, die er als $\mathbb{Z}_\ell$-Modul erhält.

1.3. Proposition. *Als $\mathbb{Z}_\ell$-Modul besitzt der Tate-Modul die folgende Struktur.*

(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_l$, *falls* $\ell \neq char(K)$.

(b) $T_\ell(E) \cong 0$ *oder* $\mathbb{Z}_\ell$, *falls* $p = char(K) > 0$.

Beweis. Dies folgt direkt aus den im vorherigen Vortrag bewiesenen Strukturaussagen über $E[m]$. □

Die Operation von $G_{\bar{K}/K}$ kommutiert offenbar mit den Multiplikationsabbildungen, die wir zur Konstruktion des projektiven Limes betrachtet haben. Daher operiert $G_{\bar{K}/K}$ auch auf $T_\ell(E)$. Weiterhin operiert die proendliche Gruppe $G_{\bar{K}/K}$ stetig auf jeder endlichen Gruppe $E[\ell^n]$, sodass die Operation auf $T_\ell(E)$ ebenfalls stetig ist.

1.4. Definition. *Die* ***ℓ-adische Darstellung*** *von $G_{\bar{K}/K}$ auf E, die mit ρ_ℓ bezeichnet wird, ist gegeben durch die Abbildung*

$$\rho_\ell : G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(E)),$$

die man durch die oben beschriebene Operation erhält.

Im Folgenden sei ℓ eine Primzahl, die von $\mathrm{char}(K)$ verschieden ist.

1.5. Bemerkung. Durch Wahl einer $\mathbb{Z}_\ell$-Basis von $T_\ell(E)$ erhalten wir eine Darstellung

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

und mit der natürlichen Inklusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ erhalten wir

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Wir haben also eine zweidimensionale Darstellung von $G_{\bar{K}/K}$ über einem Körper der Charakteristik 0.

1.6. Bemerkung. Die obige Konstruktion des Tate-Moduls verläuft analog zur folgenden Konstruktion. Sei

$$\mu_{\ell^n} \subset \bar{K}^\times$$

die Gruppe der ℓ^n-ten Einheitswurzeln. Dann erhalten wir durch das Potenzieren mit ℓ Abbildungen

$$\mu_{\ell^{n+1}} \xrightarrow{\ell} \mu_{\ell^n}.$$

Wir können wie oben den projektiven Limes betrachten und erhalten den *Tate-Modul* von K

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}.$$

Als abstrakte Gruppe haben wir $T_\ell(\mu) \cong \mathbb{Z}_\ell$. Weiterhin operiert $G_{\bar{K}/K}$ auf jedem μ_{ℓ^n}, sodass wir eine eindimensionale Darstellung

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(\mu)) \cong \mathbb{Z}_\ell^\times$$

erhalten. Für $K = \mathbb{Q}$ ist diese zyklotomische Darstellung surjektiv, was äquivalent dazu ist, dass die zyklotomischen Polynome vom Grad ℓ über $\mathbb{Q}$ irreduzibel sind.

Der Tate-Modul ist ein nützliches Hilfsmittel, um Isogenien zu studieren. Sei

$$\phi : E_1 \longrightarrow E_2$$

eine Isogenie von elliptischen Kurven. Dann definiert ϕ Abbildungen

$$\phi : E_1[\ell^n] \longrightarrow E_2[\ell^n]$$

und induziert somit eine ($\mathbb{Z}_\ell$-lineare) Abbildung

$$\phi_\ell : T_\ell(E_1) \longrightarrow T_\ell(E_2).$$

Wir erhalten also einen Homomorphismus

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

Im Fall $E_1 = E_2 = E$ ist die Abbildung

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(T_\ell(E))$$

sogar ein Ringhomomorphismus. Es ist nicht schwer zu zeigen, dass der obige Homomorphismus injektiv ist. Um $\mathrm{Hom}(E_1, E_2)$ genauer zu verstehen, brauchen wir allerdings die folgende, stärkere Aussage.

1.7. Satz. *Seien E_1 und E_2 elliptische Kurven. Dann ist die natürliche Abbildung*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)),$$
$$\phi \mapsto \phi_\ell$$

injektiv.

Bevor wir diesen Satz beweisen können, benötigen wir zunächst das folgende Hilfsresultat.

1.8. Lemma. *Sei $M \subset \mathrm{Hom}(E_1, E_2)$ eine endlich erzeugte Untergruppe. Dann ist*

$$M^{\mathrm{div}} = \{\phi \in \mathrm{Hom}(E_1, E_2) : [m] \circ \phi \in M \text{ für eine ganze Zahl } m \geq 1\}$$

ebenfalls endlich erzeugt.

Beweis. Wir erweitern zunächst die Gradabbildung auf den endlichdimensionalen $\mathbb{R}$-Vektorraum $M \otimes \mathbb{R}$. Weiterhin statten wir $M \otimes \mathbb{R}$ mit der natürlichen Topologie von $\mathbb{R}$ aus. Die Gradabbildung wird damit offenbar stetig und die Menge

$$U = \{\phi \in M \otimes \mathbb{R} : \deg(\phi) < 1\}$$

ist somit eine offene Umgebung der 0. Weiterhin wissen wir, dass $\mathrm{Hom}(E_1, E_2)$ ein torsionsfreier $\mathbb{Z}$-Modul ist. Wir haben also nach Definition von M^{div} eine natürliche Inklusion

$$M^{\mathrm{div}} \subset M \otimes \mathbb{R}.$$

Da jede von Null verschiedene Isogenie mindestens Grad 1 hat, gilt

$$M^{\mathrm{div}} \cap U = \{0\}.$$

Somit ist also M^{div} eine diskrete Untergruppe des endlichdimensionalen $\mathbb{R}$-Vektorraums $M \otimes \mathbb{R}$ und ist damit endlich erzeugt. □

Wir können nun Satz 1.7 beweisen.

Beweis von Satz 1.7. Sei $\phi \in \mathrm{Hom}(E_1, E_2) \times \mathbb{Z}_\ell$ mit $\phi_\ell = 0$. Sei nun

$$M \subset \mathrm{Hom}(E_1, E_2)$$

eine endlich erzeugte Unterguppe, sodass $\phi \in M \otimes \mathbb{Z}_\ell$. Damit ist M^{div} endlich erzeugt und torsionsfrei, also frei, da $\mathbb{Z}_\ell$ Hauptidealring ist. Sei

$$\phi_1, \ldots, \phi_t \in \mathrm{Hom}(E_1, E_2)$$

eine Basis von M^{div}. Wir haben also

$$\phi = \alpha_1\phi_1 + \cdots + \alpha_t\phi_t, \quad \text{mit } \alpha_i \in \mathbb{Z}_\ell.$$

Wir wählen nun $a_1, \ldots a_t \in \mathbb{Z}$, sodass

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

Da $\phi_\ell = 0$ gilt, muss die Isogenie

$$\psi = [a_1] \circ \phi_1 + \cdots + [a_t] \circ \phi_t \in \mathrm{Hom}(E_1, E_2)$$

die Punkte aus $E_1[\ell^n]$ auf 0 abbilden. Damit haben wir $\mathrm{Kern}([\ell^n]) \subset \mathrm{Kern}([\psi])$. Nach dem vorherigen Vortrag folgt, dass ψ durch $[\ell^n]$ faktorisiert. Wir finden also eine Isogenie $\lambda \in \mathrm{Hom}(E_1, E_2)$, sodass

$$\psi = [\ell^n] \circ \lambda.$$

Damit liegt λ also in M^{div}. Wir finden also $b_i \in \mathbb{Z}$, sodass

$$\lambda = [b_1] \circ \phi_1 + \cdots + [b_t] \circ \phi_t.$$

Da die Elemente ϕ_i eine $\mathbb{Z}$-Basis bilden, folgt

$$a_i = \ell^n b_i$$

und es gilt somit

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

Da dies für alle n gilt, haben wir $\alpha_i = 0$ und somit $\phi = 0$. □

1.9. Korollar. *Seien E_1, E_2 elliptische Kurven. Dann ist $\mathrm{Hom}(E_1, E_2)$ ein freier $\mathbb{Z}$-Modul von Rang kleiner oder gleich 4.*

Beweis. Da $\mathrm{Hom}(E_1, E_2)$ torsionsfrei ist, haben wir

$$\mathrm{Rang}_{\mathbb{Z}}(\mathrm{Hom}(E_1, E_2)) = \mathrm{Rang}_{\mathbb{Z}_\ell}(\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell).$$

Aus Satz 1.7 erhalten wir die Abschätzung

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

Durch Wahl von $\mathbb{Z}_\ell$-Basen für $T_\ell(E_1)$ und $T_\ell(E_2)$ erhalten wir mit Propostion 1.3, dass

$$\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \cong M_2(\mathbb{Z}_\ell).$$

Da $M_2(\mathbb{Z}_\ell)$ als $\mathbb{Z}_\ell$-Modul Rang 4 hat, folgt die Behauptung. □

1.10. Bemerkung. Nach Definition ist eine Isogenie über K definiert, falls sie mit der Operation von $G_{\bar{K}/K}$ kommutiert. Analog definieren wir

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

als die Gruppe der $\mathbb{Z}_\ell$-linearen Abbildungen von $T_\ell(E_1)$ nach $T_\ell(E_2)$, die mit der durch die ℓ-adische Darstellung gegebenen Operation von $G_{\bar{K}/K}$ kommutieren. Wir erhalten also einen Homomorphismus

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2)),$$

der nach Satz 1.7 injektiv ist. In vielen Fällen ist diese Abbildung sogar ein Isomorphismus. Wir wollen ohne Beweis im folgenden Satz die wichtigsten Fälle angeben.

1.11. Satz. *Die natürliche Abbildung*

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$$

ist ein Isomorphismus, falls K ein endlicher Körper oder ein Zahlkörper ist.

2. Die Weil-Paarung

Sei E/K eine elliptische Kurve. Im folgenden Abschnitt sei $m \geq 2$ eine ganze Zahl, die teilerfremd zur $\mathrm{char}(K)$ ist, falls $\mathrm{char}(K) > 0$. Wir werden in diesem Abschnitt häufig das folgende Lemma benutzen.

2.1. Lemma. *Sei E eine elliptische Kurve und $D = \sum n_P(P) \in \mathrm{Div}(E)$. Dann ist D ein Hauptdivisor genau dann, wenn $\sum n_P = 0$ und $\sum [n_P]P = O$.*

Beweis. Siehe Vortrag 5. □

Sei nun $T \in E[m]$. Dann existiert nach dem obigen Lemma eine Funktion $f \in \bar{K}(E)$, sodass

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

Sei nun $T' \in E$ mit $[m]T' = T$. Dann existiert eine Funktion $g \in \bar{K}(E)$, sodass

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R),$$

da $|E[m]| = m^2$ und $[m^2]T' = O$. Man sieht nun, dass die Funktionen $f \circ [m]$ und g^m den gleichen Divisor haben und sich somit nur um ein Element aus $\bar{K}^\times$ unterscheiden. Wir können also nach Multiplikation von f mit einem Element aus $\bar{K}^\times$ annehmen, dass

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

Sei nun $S \in E[m]$ ein weiterer m-Torsionspunkt. Dann gilt für jeden Punkt $X \in E$,

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

Wir können also die *Weil-e_m-Paarung*

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

durch

$$e_m(S,T) = g(X+S)/g(X)$$

definieren, wobei $X \in E$ ein beliebiger Punkt ist, sodass $g(X+S)$ und $g(X)$ beide definiert und von Null verschieden sind. Obwohl g nur bis auf Multiplikation mit einem Element aus $\bar{K}^\times$ definiert ist, ist dies wohldefiniert. Wir wollen nun grundlegende Eigenschaften dieser Paarung herleiten.

2.2. Proposition. *Die Weil-e_m-Paarung ist:*

(a) Bilinear:

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

(b) Alternierend: $e_m(T,T) = 1$, insbesondere gilt $e_m(S,T) = e_m(T,S)^{-1}$.

(c) Nicht-degeneriert: Falls $e_m(S,T) = 1$ für alle $S \in E[m]$, so gilt $T = O$.

(d) Galois-invariant: $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$ für alle $\sigma \in G_{\bar{K}/K}$.

(e) Kompatibel: Für $S \in E[mm']$ und $T \in E[m]$ gilt $e_{mm'}(S,T) = e_m([m']S,T)$.

Beweis. (a) Linearität im ersten Faktor folgt direkt.

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

Für die Linearität im zweiten Faktor seien $f_1, f_2, f_3, g_1, g_2, g_3$ Funktionen wie oben für T_1, T_2 und $T_3 = T_1 + T_2$. Wir wählen nun $h \in \bar{K}(E)$ mit Divisor

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

Damit gilt

$$\mathrm{div}(f_3/f_1f_2) = m\mathrm{div}(h),$$

also gibt es ein $c \in \bar{K}^\times$, sodass

$$f_3 = cf_1f_2h^m.$$

Durch Verknüpfung mit $[m]$ und mit der Identität $f_i \circ [m] = g_i^m$ erhalten wir

$$g_3 = c'g_1g_2(h \circ [m]).$$

Somit gilt

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

(b) Aus (a) erhalten wir, dass

$$e_m(S+T,S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T),$$

es genügt also $e_m(T,T) = 1$ für alle $T \in E[m]$ zu zeigen. Sei dazu für $P \in E$ wie im letzten Vortrag $\tau_P : E \longrightarrow E$ die zu P gehörige Translationsabbildung. Damit gilt

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\sum_{i=0}^{m-1}([1-i]T) - ([-i]T) = 0.$$

Also ist $\prod_{i=0}^{m-1} f\circ\tau_{[i]T}$ konstant. Sei nun $T' \in E$ mit $[m]T' = T$. Dann ist auch das Produkt $\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$ konstant, da die m-te Potenz gerade dem obigen Produkt entspicht. Wir werten dieses Produkt nun in X und $X+T'$ aus und erhalten

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

Nach Kürzung haben wir also

$$g(X) = g(X+[m]T') = g(X+T),$$

womit $e_m(1,1) = 1$ gezeigt ist.
(c) Falls $e_m(S,T) = 1$ für alle $S \in E[m]$, so haben wir $g(X+S) = g(X)$ für alle $S \in E[m]$. Aus dem vorherigen Vortrag erhalten wir, dass $g = h \circ [m]$ für eine Funktion $h \in \bar{K}(E)$. Damit haben wir

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

und somit $f = h^m$. Damit gilt

$$m\operatorname{div}(h) = \operatorname{div}(f) = m(T) - m(O),$$

und folglich

$$\operatorname{div}(h) = (T) - (O).$$

Mit Vortrag 5 folgt $T = O$.
(d) Sei $\sigma \in G_{\bar{K}/K}$. Wenn f, g die zu T gehörigen Funktionen sind, so sind offenbar f^σ, g^σ die zugehörigen Funktionen zu T^σ. Damit gilt

$$e_m(S^\sigma,T^\sigma) = \frac{g^\sigma(X^\sigma+S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_m(S,T)^\sigma.$$

(e) Mit f, g wie oben haben wir

$$\operatorname{div}(f^{m'}) = mm'(T) - mm'(O)$$

und

$$(g\circ[m'])^{mm'} = (f\circ[mm'])^{m'}.$$

Damit erhalten wir

$$e_{mm'}(S,T) = \frac{g\circ[m'](X+S)}{g\circ[m'](X)} = \frac{g(Y+[m']S)}{g(Y)} = e_m([m']S,T).$$

□

Aus diesen Eigenschaften folgt die Surjektivität der Weil-Paarung, was wir im Folgenden zeigen.

2.3. Korollar. *Es existieren Punkte $S, T \in E[m]$, sodass $e_m(S,T)$ eine primitive m-te Einheitswurzel ist. Insbesondere folgt aus $E[m] \subset E(K)$, dass $\mu_m \subset K^\times$.*

Beweis. Das Bild von $e_m(S,T)$ ist eine Unterguppe von μ_m, also μ_d für ein d mit $d|n$. Es gilt also für alle $S, T \in E[m]$, dass

$$1 = e_m(S,T)^d = e_m([d]S, T).$$

Da die Weil-e_m-Paarung nicht-degeneriert ist, folgt $[d]S = O$ und, da S beliebig ist, erhalten wir aus dem vorherigen Vortrag, dass $d = m$, womit die Aussage bewiesen ist. Sei also $E[m] \subset E(K)$, dann folgt aus der Galois-Invarianz, dass $e_m(S,T) \in K^\times$ für alle $S, T \in E[m]$. Damit haben wir $\mu_m \subset K^\times$. □

Wir wollen nun zeigen, dass eine Isogenie $\phi : E_1 \longrightarrow E_2$ bezüglich der Weil-Paarung adjungiert zu ihrer dualen Isogenie $\hat{\phi} : E_2 \longrightarrow E_1$ ist.

2.4. Proposition. *Seien $S \in E_1[m]$, $T \in E_2[m]$ und $\phi : E_1 \longrightarrow E_2$ eine Isogenie. Dann gilt*

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

Beweis. Seien wie oben

$$\mathrm{div}(f) = m(T) - m(O) \text{ und } f \circ [m] = g^m.$$

Wir haben also

$$e_m(\phi S, T) = g(X + \phi S)/g(X).$$

Wir finden nun eine Funktion $h \in \bar{K}(E_1)$, sodass

$$\phi^*((T)) - \phi^*((O)) = (\hat{\phi}T) - (O) + \mathrm{div}(h),$$

da $\hat{\phi}T$ gerade die Summe der Punkte des Divisors auf der linken Seite der Gleichung ist. Damit haben wir

$$\begin{aligned} \mathrm{div}\left(\frac{f \circ \phi}{h^m}\right) &= \phi^* \mathrm{div}(f) - m\mathrm{div}(h) \\ &= m(\hat{\phi}T) - m(O), \end{aligned}$$

und

$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = \left(\frac{f \circ \phi}{h^m}\right) \circ [m].$$

Nach Definition der Weil-e_m-Paarung gilt also

$$\begin{aligned} e_m(S, \hat{\phi}T) &= \frac{(g \circ \phi / h \circ [m](X+S)}{(g \circ \phi / h \circ [m])(X)} \\ &= \frac{g(\phi X + \phi S)}{g(\phi X)} \frac{h([m]X)}{h([m]X + [m]S)} \\ &= e_m(\phi S, T). \end{aligned}$$

□

Sei nun ℓ eine von $\mathrm{char}(K)$ verschiedene Primzahl. Wir wollen die Paarungen

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \longrightarrow \mu_{\ell^n}$$

für alle $n = 1, 2, \ldots$ zu einer *ℓ-adischen Weil-Paarung* auf dem Tate-Modul

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu).$$

Die projektiven Limiten $T_\ell(E)$ und $T_\ell(\mu)$ wurden bezüglich der Abbildungen

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \text{ und } \mu_{\ell^{n+1}} \xrightarrow{\ell} \mu_{\ell^n}$$

gebildet. Um zu zeigen, dass die Weil-e_{ℓ^n}-Paarungen kompatibel sind, müssen wir also zeigen, dass für alle $S, T \in E[\ell^{n+1}]$,

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

Wegen der Bilinearität haben wir

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

und die Behauptung folgt aus der Kompatibilität. Damit ist e wohldefiniert und alle Eigenschaften aus Proposition 2.2 übertragen sich. Zusammengefasst haben wir also das Folgende gezeigt.

2.5. Satz. *Es existiert eine bilineare, alternierende, nicht-degenerierte, Galois-invariante Paarung*

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu).$$

Weiterhin gilt für eine Isogenie $\phi : E_1 \longrightarrow E_2$: ϕ und die duale Isogenie $\hat{\phi}$ adjungiert bezüglich der Paarung.

3. Der Endomorphismenring

Sei E/K eine elliptische Kurve. Wir wollen nun die Ringe charakterisieren, die als Endomorphismenringe von E auftreten können. Bisher haben wir die folgenden Informationen über $\mathrm{End}(E)$:

(i) $\mathrm{End}(E)$ ist nullteilerfreier Ring der Charakteristik 0 von Rang kleiner oder gleich 4 über $\mathbb{Z}$.

(ii) $\mathrm{End}(E)$ besitzt eine Anti-Involution $\phi \mapsto \hat{\phi}$.

(iii) Für $\phi \in \mathrm{End}(E)$, haben wir $\phi\hat{\phi} \in \mathbb{Z}$, $\phi\hat{\phi} \geq 0$ und $\phi\hat{\phi} = 0$ genau dann, wenn $\phi = 0$.

Wir werden nun zeigen, dass ein Ring mit diesen Eigenschaften bereits von einer sehr speziellen Sorte ist. Wir werden dazu einen allgemeinen Klassifizierungssatz für Ringe mit den Eigenschaften (i)-(iii) beweisen.

3.1. Definition. *Sei $\mathcal{K}$ eine (nicht notwendigerweise kommutative) Algebra, die über $\mathbb{Q}$ endlich erzeugt ist. Eine **Ordnung** $\mathcal{R}$ von $\mathcal{K}$ ist ein Unterring von $\mathcal{K}$, der als $\mathbb{Z}$-Modul endlich erzeugt ist und für den gilt $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.*

3.2. Definition. *Eine **Quaternionenalgebra** ist eine Algebra von der Form*

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

mit den Multiplikationsregeln

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Mit diesen Definitionen können wir nun den allgemeinen Klassifizierungssatz formulieren und beweisen.

3.3. Satz. *Sei $\mathcal{R}$ ein nullteilerfreier Ring der Charakteristik 0 mit den folgenden Eigenschaften*

(i) $\mathcal{R}$ hat Rang kleiner oder gleich 4 (als $\mathbb{Z}$-Modul).

(ii) $\mathcal{R}$ besitzt eine Anti-Involution $\alpha \mapsto \hat{\alpha}$.

(iii) Für $\alpha \in \mathcal{R}$ ist $\alpha\hat{\alpha}$ eine nicht-negative ganze Zahl und $\alpha\hat{\alpha} = 0$ gilt genau dann, wenn α=0.

Dann ist $\mathcal{R}$ ein Ring von einer der folgenden drei Klassen.

(a) $\mathcal{R} \cong \mathbb{Z}$.

(b) $\mathcal{R}$ ist eine Ordnung in einer quadratischen imaginären Erweiterung von $\mathbb{Q}$.

(c) $\mathcal{R}$ ist eine Ordnung in einer Quaternionenalgebra über $\mathbb{Q}$.

Beweis. Sei $\mathcal{K} = \mathcal{R} \otimes \mathbb{Q}$. Da $\mathcal{R}$ endlich erzeugt ist, genügt es zu zeigen, dass $\mathcal{K} = \mathbb{Q}$ ist, $\mathcal{K}/\mathbb{Q}$ eine quadratische imaginäre Erweiterung ist oder $\mathcal{K}/\mathbb{Q}$ eine Quaternioenenalgebra ist. Wir erweitern nun die Anti-Involution auf $\mathcal{K}$ und definieren die (reduzierte) *Norm* und *Spur* von $\mathcal{K}$ nach $\mathbb{Q}$ durch

$$N\alpha = \alpha\hat{\alpha} \quad \text{und} \quad T\alpha = \alpha + \hat{\alpha}.$$

Es gilt nun

$$T\alpha = 1 + N\alpha - N(\alpha - 1),$$

und damit $T\alpha \in \mathbb{Q}$. Weiterhin ist die Spur offenbar $\mathbb{Q}$-linear. Für $\alpha \in \mathbb{Q}$ gilt $T\alpha = 2\alpha$. Für $\alpha \in \mathcal{K}$ mit $T\alpha = 0$ gilt

$$0 = (\alpha - \alpha)(\alpha - \hat{\alpha}) = \alpha^2 - (T\alpha)\alpha + N\alpha = \alpha^2 + N\alpha,$$

also $\alpha^2 = -N\alpha$. Damit gilt folglich entweder $\alpha = 0$ oder $\alpha^2 \in \mathbb{Q}$ und $\alpha^2 < 0$.
Falls nun $\mathcal{K} = \mathbb{Q}$ gilt, ist nichts mehr zu zeigen. Andernfalls können wir ein $\alpha \in \mathcal{K}$, $\alpha \notin \mathbb{Q}$

wählen. Wir ersetzen α durch $\alpha - \frac{1}{2}T\alpha$, sodass wir $T\alpha = 0$ annehmen können. Damit haben wir wie oben gesehen $\alpha^2 < 0$ und $\mathbb{Q}(\alpha)$ ist somit ein quadratischer imaginärer Körper. Falls $\mathcal{K} = \mathbb{Q}(\alpha)$ gilt, ist nichts mehr zu zeigen.
Falls $\mathcal{K} \neq \mathbb{Q}(\alpha)$ gilt, können wir $\beta \in \mathcal{K}$, $\beta \notin \mathbb{Q}(\alpha)$ wählen. Wie oben können wir β durch

$$\beta - \tfrac{1}{2}T\beta - \tfrac{1}{2}(T(\alpha\beta)/\alpha^2)\alpha$$

ersetzen und erhalten so, dass $T\beta = T(\alpha\beta) = 0$. Damit gilt wieder $\beta^2 < 0$. Wir haben also

$$\alpha = -\hat{\alpha},\ \beta = \hat{\beta},\ \alpha\beta = -\hat{\beta}\hat{\alpha},$$

und somit

$$\alpha\beta = -\beta\alpha.$$

Damit ist also

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

eine Quaternionenalgebra. Zu zeigen bleibt $\mathbb{Q}[\alpha, \beta] = \mathcal{K}$. Dazu genügt es zu zeigen, dass $1, \alpha, \beta, \alpha\beta$ über $\mathbb{Q}$ linear unabhängig sind, da in diesem Fall $\mathbb{Q}[\alpha, \beta]$ und $\mathcal{K}$ beide Dimension 4 über $\mathbb{Q}$ haben. Angenommen es gilt

$$w + x\alpha + y\beta + z\alpha\beta = 0$$

mit $w, x, y, z \in \mathbb{Q}$ alle von Null verschieden. Durch Bildung der Spur erhalten wir $2w = 0$ und somit $w = 0$. Mit Multiplikation mit α von links und β von rechts folgt

$$(x\alpha^2)\beta + (y\beta^2)\alpha + z\alpha^2\beta^2 = 0,$$

was der $\mathbb{Q}$-linearen Unabhängigkeit von $1, \alpha, \beta$ widerspricht. Damit haben wir $\mathcal{K} = \mathbb{Q}[\alpha, \beta]$. □

3.4. Korollar. *Der Endomorphismenring einer elliptischen Kurven ist entweder $\mathbb{Z}$, eine Ordnung in einem quadratischen imaginären Körper oder eine Ordnung in einer Quaternionenalgebra.*

4. Die Automorphismengruppe

Für eine durch eine Weierstraßgleichung gegebene elliptische Kurve ist die Bestimmung der genauen Struktur des Endomorphismenrings im Allgemeinen sehr aufwendig. Die Bestimmung der Automorphismengruppe ist dagegen wesentlich einfacher, wie wir im Folgenden sehen werden.

4.1. Satz. *Sei E/K eine durch eine Weierstraßgleichung gegebene elliptische Kurve. Dann ist die Automorphismengruppe* $\mathrm{Aut}(E)$ *eine endliche Gruppe, deren Ordnung* 24

teilt. Genauer ist die Ordnung von $\mathrm{Aut}(E)$ *gegeben durch:*

$$\begin{aligned} 2,&\ \textit{falls}\ j(E) \neq 0, 1728 \\ 4,&\ \textit{falls}\ j(E) = 1728\ \textit{und}\ \mathrm{char}(K) \neq 2,3 \\ 6,&\ \textit{falls}\ j(E) = 0\ \textit{und}\ \mathrm{char}(K) \neq 2,3 \\ 12,&\ \textit{falls}\ j(E) = 0 = 1728\ \textit{und}\ \mathrm{char}(K) = 3 \\ 24,&\ \textit{falls}\ j(E) = 0 = 1728\ \textit{und}\ \mathrm{char}(K) = 2. \end{aligned}$$

Beweis. Wir beschränken uns auf den Fall $\mathrm{char}(K) \neq 2, 3$. Dann ist E durch die Gleichung

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

gegeben und jeder Automorphismus ist von der Form

$$x = u^2 x', \quad y = u^3 y'$$

für ein $u \in \bar{K}^\times$. Eine solche Substitution liefert einen Automorphismus von E genau dann, wenn

$$u^{-4} A = A \ \text{ und } \ u^{-6} B = B.$$

Falls also $AB \neq 0$ (also $j(E) \neq 0, 1728$) gilt, sind die einzigen Möglichkeiten $u = \pm 1$. In den Fällen $B = 0$ ($j(E) = 1728$) oder $A = 0$ ($j(E) = 0$) erfüllt u die Gleichung $u^4 = 1$ oder $u^6 = 1$. Somit ist $\mathrm{Aut}(E)$ zyklisch von der Ordnung 4 oder 6. □

In diesem Beweis haben wir sogar zusätzlich gezeigt, dass $\mathrm{Aut}(E)$ ein $G_{\bar{K}/K}$-Modul für $\mathrm{char} \neq 2, 3$ ist und dessen Struktur bestimmt.

4.2. Korollar. *Sei E/K eine durch eine Weierstraßgleichung gegebene elliptische Kurve über einem Körper K mit $\mathrm{char}(K) \neq 2, 3$ und sei n gegeben durch*

$$n = \begin{cases} 2, \textit{ falls } j(E) \neq 0, 1728, \\ 4, \textit{ falls } j(E) = 1728, \\ 6, \textit{ falls } j(E) = 0. \end{cases}$$

Dann gilt als $G_{\bar{K}/K}$-Moduln

$$\mathrm{Aut}(E) \cong \mu_n.$$

Beweis. Im obigen Beweis haben wir gezeigt, dass die Abbildung

$$\mu_n \longrightarrow \mathrm{Aut}(E), \quad \zeta \mapsto [(x, y) \mapsto (\zeta^2 x, \zeta^3 y)]$$

ein Gruppenisomorphismus ist. Diese Abbildung kommutiert offenbar mit der Operation von $G_{\bar{K}/K}$, sodass wir einen Isomorphismus von $G_{\bar{K}/K}$-Moduln erhalten. □

Literatur

[Si] Silverman, J.H.: *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106. Springer Verlag, 2009.