Jürgen Böhm

Elliptische Kurven

3. Mai 2020

Vorwort

Dieses Buch ist eine Einführung in die Theorie der elliptischen Kurven.

Das Buch orientiert sich an Silverman, „The Arithmetic of Elliptic Curves“ [1].

Der Autor freut sich über Rückmeldungen an

mathematik@juergenboehm.net

mit allgemeinen Kommentaren zu dem Buch, besonders aber mit Meldungen über gefundene Fehler und problematische Stellen.

Wilhermsdorf, 2016 - *Jürgen Böhm*

Inhaltsverzeichnis

1

Algebraische Kurven

1.1 Grundlagen

1.1.1 Definition

Definition 1.1.1. *Ein integres Schema X/k, separiert über einem Körper k mit* $\dim X = 1$ *heißt* algebraische Kurve *über k. Ist überdies X/k eigentlich, so heißt X* vollständige Kurve.

1.2 Morphismen

1.2.1 Allgemeine Eigenschaften

Proposition 1.2.1. *Es sei $f : X \to Y$ ein nichtkonstanter Morphismus vollständiger Kurven. Dann ist f selbst eigentlich, affin, ganz und flach.*

Beweis. Da f eigentlich ist, ist für jedes $y \in Y$ und jede kohärente Garbe $\mathcal{F}$ auf X:

$$(R^p f_* \mathcal{F})_y\widehat{\ } \xrightarrow{\sim} \varprojlim_n H^p(X_y^{(n)}, \mathcal{F})$$

Also $R^p f_* \mathcal{F} = 0$ für $p > 0$, denn $X_y^{(n)} = X \times_Y \mathcal{O}_{Y,y}/\mathfrak{m}_y^n$ ist nulldimensional.

Wir betrachten jetzt die eigentliche Abbildung $f' : U \to V$ mit $V \subseteq Y$ offen, affin und $U = f^{-1}(V)$, die durch Einschränkung von f auf U entsteht. Weiter sei $\mathcal{F}$ eine kohärente Garbe auf U.

Wir haben die Leray-Spektralsequenz

$$H^p(V, R^q f'_* \mathcal{F}) \Rightarrow H^{p+q}(U, \mathcal{F})$$

Nach der Eingangsbemerkung ist nun immer $R^q f'_* \mathcal{F} = 0$ für $q > 0$. Weiterhin ist $H^p(V, f'_* \mathcal{F}) = 0$ für $p > 0$, denn $f'_* \mathcal{F}$ ist kohärent und V affin. Also ist $H^1(U, \mathcal{F}) = 0$ als Grenzwert der Spektralsequenz und damit U nach dem üblichen kohomologischen Kriterium affin.

Nun ist aber $f'_* \mathcal{O}_U$ eine kohärente $\mathcal{O}_V$-Garbe, weil f' eigentlich. Also ist mit $U = \operatorname{Spec}(B)$ und $V = \operatorname{Spec}(A)$, der A-Modul B ein endlich erzeugter A-Modul.

Somit ist f eine affine, endliche und als surjektive Abbildung eindimensionaler integrer Schemata auch flache Abbildung.

1.2.2 Verzweigungsindex

Es sei $f : X \to Y$ ein Morphismus von Kurven und $f(P) = Q$ eine Abbildung von abgeschlossenen Punkten. Weiter sei $k(Q) = \mathcal{O}_{Y,Q}/\mathfrak{m}_Q$ und $B = \mathcal{O}_{X,P}/f^\sharp(\mathfrak{m}_Q)$ mit der kanonischen, injektiven Abbildung $f^\sharp : \mathcal{O}_{Y,Q} \to \mathcal{O}_{X,P}$.

Definition 1.2.1. *Mit den eben eingeführten Bezeichnunen sei* $e_P = e_P(f) = \dim_{k(Q)} B$ *der* Verzweigungsindex von f in P

1.2.3 Frobenius–Morphismus

Es sei $X = \mathbb{A}^n_k$ der affine Raum über einem Körper k mit $\operatorname{char} k = p$ und $A = k[x_1, \ldots, x_n]$, sein Koordinatenring. Das Ideal $I \subseteq A$ definiere ein Unterschema $Y \subseteq X$.

Wir betrachten die Abbildung

$$F : (x_1 : \ldots : x_n) \to (x_1^q : \ldots : x_n^q) \tag{1.1}$$

auf den abgeschlossenen Punkten $X(\bar{k})$.

Definition 1.2.2. *Die so definierte Abbildung F heißt* (geometrische) Frobeniusabbildung.

Auf Ringebene wird F durch den Morphismus

$$\Phi : A \to A, \quad x_i \mapsto x_i^q \tag{1.2}$$

gebildet. Es handelt sich um einen Morphismus von k–Algebren.

Es sei $f = \sum a_J x_1^{J_1} \cdot \cdots \cdot x_n^{J_n}$ ein Polynom aus A. Dann sei

$$f^{(q)} = \sum a_J^q x_1^{J_1} \cdot \cdots \cdot x_n^{J_n} \tag{1.3}$$

Lemma 1.2.1. *Es seien $f, g \in A$ zwei Polynome. Dann ist $(f+g)^{(q)} = f^{(q)} + g^{(q)}$ und $(fg)^{(q)} = f^{(q)} g^{(q)}$. Weiterhin gilt $\Phi(f^{(q)}) = f^q$.*

Mit $I^{(q)}$ sei das von den $f^{(q)}$ für alle $f \in I$ erzeugte Ideal bezeichnet. Es gilt dann

Lemma 1.2.2. *Ist k ein perfekter Körper, so ist die Abbildung $g \mapsto g^{(q)}$ eine Surjektion $A \to A$.*

Weiterhin ist $I^{(q)} = \{f^{(q)} \mid f \in I\}$ wobei die rechts stehende Menge bereits ein Ideal ist, sowie

$$\Phi(I^{(q)}) \subseteq I^q \subseteq I$$

Beweis. Es sei $g = \sum_J a_J \underline{x}^J$. Dann ist $a_J = b_J^q$, weil k perfekt. Also ist $g = h^{(q)}$ mit $h = \sum_J b_J \underline{x}^J$.

Ist $f \in I^{(q)}$, so ist $f = \sum_i g_i h_i^{(q)}$. Nun ist aber $g_i = (g_i')^{(q)}$ und damit nach vorigem Lemma $f = \left(\sum_i g_i' h_i\right)^{(q)}$.

Ist schließlich $f^{(q)} = \sum a_J^q \underline{x}^J \in I^{(q)}$ mit $f = \sum a_J \underline{x}^J \in I$, so ist $\Phi(f^{(q)}) = \sum a_J^q \underline{x}^{qJ} = f^q \in I^q$

Lemma 1.2.3. *Es sei k ein perfekter Körper und I ein Primideal von A. Dann ist auch $I^{(q)}$ ein Primideal von A.*

Beweis. Es sei $f, g \in A$ und $f^{(q)}g^{(q)} \in I^{(q)}$. Dann ist $\Phi(f^{(q)}g^{(q)}) = f^q g^q \in I$, also oBdA $f \in I$. Somit ist $f^{(q)} \in I^{(q)}$ und damit $I^{(q)}$ prim.

Weiter sei

$$Y^{(q)} = V(I^{(q)}) = \operatorname{Spec}\left(A/I^{(q)}\right) \tag{1.4}$$

Für $x_1, \ldots, x_n \in B$, mit einer k–Algebra B, gilt

$$f^{(q)}(x_1^q, \ldots, x_n^q) = f(x_1, \ldots, x_n)^q \tag{1.5}$$

Ist insbesondere $x_1, \ldots, x_n \in \bar{k}$ und $f(x_1, \ldots, x_n) = 0$, so ist $f^{(q)}(x_1^q, \ldots, x_n^q) = 0$. Der Frobenius F induziert also eine Abbildung $F : Y \to Y^{(q)}$.

Auf Ringebene hat man die Abbildungen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^{(q)} & \longrightarrow & A & \longrightarrow & A/I^{(q)} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I & \longrightarrow & A & \longrightarrow & A/I & \longrightarrow & 0 \end{array} \tag{1.6}$$

mit $\Phi(I^{(q)}) \subseteq I^q$.

Lemma 1.2.4. *Es sei k ein perfekter Körper und $\Phi : A \to A$ die oben eingeführte Frobeniusabbildung. Dann ist $\Phi^*(I) \stackrel{def}{=} \Phi^{-1}(I) = I^{(q)}$ für $I \subseteq A$ prim und die Abbildung*

$$\{I \mid I \subseteq A,\ prim\} \xrightarrow{\Phi^*} \{I^{(q)} \mid I^{(q)} \subseteq A,\ prim\} \tag{1.7}$$

ist eine inklusionserhaltende Bijektion.

Beweis. Es sei $f^{(q)} \in \Phi^{-1}(I)$, also $\Phi(f^{(q)}) = f^q \in I$, also $f \in I$, also $f^{(q)} \in I^{(q)}$. Umgekehrt ist für $f^{(q)} \in I^{(q)}$ das Bild $\Phi(f^{(q)}) = f^q \in I^q \subseteq I$.

Weiterhin ist Φ^* injektiv: Es sei für $I, J \subseteq A$ prim, $I^{(q)} = J^{(q)}$. Mit $f \in I$ gilt $f^{(q)} \in I^{(q)} = J^{(q)}$, also $\Phi(f^{(q)}) = f^q \in J$, also $f \in J$.

Korollar 1.2.1. *Ist k ein perfekter Körper, und I prim, so ist die Abbildung $\Phi : A/I^{(q)} \to A/I$ injektiv.*

Lemma 1.2.5. *Es sei k perfekt und $\Phi : A \to A$ wie oben sowie $I \subseteq A$ prim. Es sei $\Phi : A/I^{(q)} \to A/I$ auch die Bezeichnung für die induzierte Abbildung sowie die auf den Quotientenkörpern $Q(A/I^{(q)}) \to Q(A/I)$ induzierte Abbildung.*

Ist $\alpha \in Q(A/I^{(q)})$ ganz über $A/I^{(q)}$, so ist $\Phi(\alpha)$ ganz über A/I.

Beweis. Es sei $\alpha \in Q(A/I^{(q)})$ und

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

mit $a_i \in A/I^{(q)}$.

Da $\Phi(a_i) \in A/I$, ist $\Phi(\alpha)$ ganz über A/I in $Q(A/I)$

Proposition 1.2.2. *Es sei $\Phi : A \to A$ und $I \subseteq A$, prim, wie im vorigen Lemma. Ist dann A/I ganz abgeschlossen in $Q(A/I)$, so ist $A/I^{(q)}$ ganz abgeschlossen in $Q(A/I^{(q)})$.*

Beweis. Es sei $\alpha = \frac{f^{(q)}}{g^{(q)}} \in Q(A/I^{(q)})$ ganz über $A/I^{(q)}$. Dann ist $\Phi(\alpha) = \left(\frac{f}{g}\right)^q$ ganz über A/I, also f/g ganz über A/I, also $f/g = h \in A/I$, also $f = gh$ in A/I. Damit ist $f^{(q)} = g^{(q)}h^{(q)}$ in $A/I^{(q)}$, also $\alpha = f^{(q)}/g^{(q)} = h^{(q)} \in A/I^{(q)}$, also $A/I^{(q)}$ ganz abgeschlossen in seinem Quotientenkörper.

Proposition 1.2.3. *Es sei $\Phi : A \to A$ und $I \subseteq A$, prim, wie oben. Dann ist A/I ganz über $A/I^{(q)}$ unter der Einbettung $\Phi : A/I^{(q)} \to A/I$.*

Beweis. Es gilt für $x_i + I \in A/I$, daß $(x_i + I)^q - \Phi(x_i + I^{(q)}) = 0$ ist. Also ist A/I ganz über $A/I^{(q)}$.

Korollar 1.2.2. *Es gilt für die Krulldimension*

$$\dim A/I = \dim A/I^{(q)} \tag{1.8}$$

Korollar 1.2.3. *Ist A/I ein Dedekindring, so gilt dies auch für $A/I^{(q)}$.*

Proposition 1.2.4. *Es sei C eine algebraische Kurve über einem perfekten Körper k mit* $\operatorname{char} k = p$. *Es sei $F : C \to C^{(q)}$ der geometrische Frobeniusmorphismus.*

Dann gilt

1. Man hat ein Dreieck

$$\begin{array}{ccc} K(C) & \xleftarrow{\quad\supseteq\quad} & K(C)^q \\ & {\scriptstyle\Phi}\nwarrow \quad \nearrow{\scriptstyle\simeq} & \\ & K(C^{(q)}) & \end{array} \tag{1.9}$$

2. Es ist $[K(C) : K(C)^q]$ rein inseparabel vom Grad q.

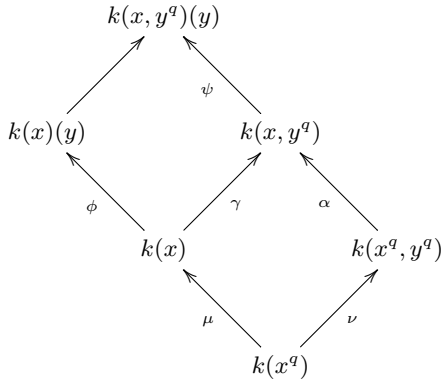
Beweis. 1. Es sei $A = k[x_1, \ldots, x_s]$ und $K(C) = Q(A/I)$ mit einem Primideal $I \subseteq A$. Es ist dann $K(C^{(q)}) = Q(A/I^{(q)})$.

Die Abbildung $\Phi : K(C^{(q)}) \to K(C)$ wird nun von der injektiven Abbildung $\Phi : A/I^{(q)} \to A/I$ induziert.

Ein Element $f + I^{(q)} \in A/I^{(q)}$ kann als $f_1^{(q)} + I^{(q)}$ geschrieben werden und man hat $\Phi(f + I^{(q)}) = f_1^q + I$. Also ist $\Phi(K(C^{(q)})) \subseteq K(C)^q$. Weiterhin ist $x_i^q + I = \Phi(x_i + I^{(q)})$ und somit und wegen der Perfektheit von k auch $\Phi : A \to A^q$ surjektiv. Damit ist auch $\Phi(K(C^{(q)})) \to K(C)^q$ surjektiv, also $\Phi : K(C^{(q)}) \to K(C)^q$ der behauptete Isomorphismus.

2. Es sei $K(C) = k(x, y)$ mit y separabel über $k(x)$. Eine solche Darstellung kann man immer finden, denn weil k perfekt, enthält jedes endliche Erzeugendensystem von $K(C)$ eine separierende Transzendenzbasis.

Es ist dann weiterhin $K(C)^q = k(x^q, y^q)$ und damit $K(C)/K(C)^q$ rein inseparabel, da für jedes $z \in K(C)$ immer $z^q \in K(C)^q$ ist. Betrachte nun das Diagramm



(1.10)

Da ϕ eine separable Erweiterung darstellt, ist auch die Erweiterung ψ mit $k(x, y^q)$ separabel. Andererseits ist $\psi \circ \alpha$, nach dem eben Bemerkten, eine rein inseparable Erweiterung. Also ist die Inklusion ψ die Identität und $K(C) : K(C)^q = k(x, y^q) : k(x^q, y^q)$.

Die Einbettung γ ist separabel vom Grad d, dem Grad des Minimalpolynoms von y über $k(x)$, und μ ist rein inseparabel vom Grad q. Die Erweiterung α ist rein inseparabel vom Grad $q' \leqslant q$ und ν ist vom Grad $d' \leqslant d$, wie man erkennt, indem man das Minimalpolynom $G(y, x)$ von y über $k(x)$ zur q–ten Potenz erhebt. Aus der Multiplikativität von Separabilitäts– und Inseparabilitätsgraden folgt, daß für den Separabilitätsgrad $d'' \leqslant d'$ von ν die Beziehung $d'' \geqslant d$ gelten muß. Also ist $d'' = d' = d$ und $q' = q$.

1.3 Riemann–Roch

Lemma 1.3.1. *Es sei X/k eine algebraische Kurve und D ein Divisor auf X. Dann ist äquivalent*

a) D hat keine Basispunkte.
b) Für jeden Punkt $P \in X$ ist $\dim H^0(X, \mathcal{O}_X(D - P)) < \dim H^0(X, \mathcal{O}_X(D))$.

Beweis. Es ist P ein Basispunkt für D, wenn für jedes $s \in \mathcal{O}_X(D)(X)$ immer $s_P \in \mathfrak{m}_P \mathcal{O}_X(D)_P$ gilt.

Betrachte nun mit $\mathfrak{m}_P = \mathcal{O}_X(-P)$ die exakte Sequenz

$$0 \to \mathcal{O}_X(-P) \to \mathcal{O}_X \to k(P) \to 0$$

Tensorieren mit $\mathcal{O}_X(D)$ und Bilden der globalen Schnitte $\Gamma(X, -)$ ergibt

$$0 \to \mathcal{O}_X(D - P)(X) \to \mathcal{O}_X(D)(X) \to k(P)$$

Genau wenn P ein Basispunkt von D ist, wird jeder globale Schnitt $s \in \mathcal{O}_X(D)(X)$ auf $s(P) = 0$ abgebildet. Genau dann ist die Abbildung links surjektiv, also äquivalent $H^0(X, \mathcal{O}_X(D - P)) = H^0(X, \mathcal{O}_X(D))$.

1.4 Differentialmodule

Es sei im folgenden $B/A/k$ eine separable Erweiterung von geometrischen Dedekindringen und M ein B–Modul.

Lemma 1.4.1. *Für einen B–Torsionsmodul M und maximale Ideale $\mathfrak{q} \subseteq B$ über $\mathfrak{p} \subseteq A$ gilt die Beziehung*

$$\operatorname{len} M_{\mathfrak{q}} = \dim_{k(\mathfrak{p})}(M \otimes_A k(\mathfrak{p}))_{\mathfrak{q}} \tag{1.11}$$

Beweis. Es gilt ja mit $B' = B_{\mathfrak{q}}$ eine Gleichheit $M_{\mathfrak{q}} = \sum_i B'/(\mathfrak{q}B')^{e_i}$. Aus

$$\dim_{k(\mathfrak{p})} \mathfrak{q}^j B'/\mathfrak{q}^{j+1}B' = \dim_{k(\mathfrak{p})} B'/\mathfrak{q} = f(k(\mathfrak{q})/k(\mathfrak{p})) = 1$$

folgt die Behauptung

Lemma 1.4.2. *Es seien $\mathfrak{q} \subseteq B$ über $\mathfrak{p} \subseteq A$ zwei maximale Ideale. Weiter sei $A' = A_{\mathfrak{p}}$ und $B' = B_{\mathfrak{q}}$.*

Dann ist

$$\Omega_{B|A} \otimes_A k(\mathfrak{p}) = \Omega_{B'|A'} \otimes_{A'} k(\mathfrak{p})$$

Ist B/A wie oben und A ein diskreter Bewertungsring, so existiert ein monisches $f(T) \in A[T]$ mit $B = A[T]/(f(T))$.

Lemma 1.4.3. *Es sei $B = A[T]/(f(T))$ wie oben. Dann ist*

$$\Omega_{B|A} = A[T]/(f(T), f'(T))dT \tag{1.12}$$

Es sei $B = A[T]/(f(T)) = A[t]$ mit den obengenannten Bezeichnungen und es sei

$$\bar{f}(T) = \prod_i (T - x_i)^{e_i} \in k(\mathfrak{p})[T]$$

das Bild von $f(T)$ unter $A[T] \to k(\mathfrak{p})[T]$ mit $x_i \in k$. Dann sind die Primideale von B über $\mathfrak{p}$ gleich

$$\mathfrak{q}_i = (\mathfrak{p}, t - x_i)$$

es ist

$$\mathfrak{p}B = \prod_i \mathfrak{q}^{e_i}$$

und es ist e_i der Verzweigungsgrad bei $\mathfrak{q}_i$ der Abbildung $A \to B$.

Weiterhin ist mit $k = k(A) = k(\mathfrak{p})$

$$\begin{aligned}
\Omega_{B|A} \otimes_A k(A) = k[T]/\left(\bar{f}(T), \bar{f}'(T)\right) = \\
= \bigoplus_i k[T]/\left((T - x_i)^{e_i}, \bar{f}'(T)\right) = \\
= \bigoplus_i k[T]/\left((T - x_i)^{e_i}, e_i(T - x_i)^{e_i - 1} \prod_{j \neq i} (T - x_j)^{e_j}\right) = \\
= \bigoplus_i k[T]/\left((T - x_i)^{e_i}, e_i(T - x_i)^{e_i - 1}\right)
\end{aligned} \tag{1.13}$$

(beachte: $a(T)(T-x_i)^{e_i}+b(T)(T-x_j)^{e_j}=1$ mit geeigneten $a(T),b(T)$). Ist $\operatorname{char} k \nmid e_i$ für alle i, so ist dies gleich

$$\bigoplus_i k[T]/\left((T-x_i)^{e_i-1}\right) \tag{1.14}$$

wobei

$$k[T]/\left((T-x_i)^{e_i-1}\right) = (\Omega_{B|A})_{\mathfrak{q}_i} \otimes_A k(A) \tag{1.15}$$

also

$$\dim_{k(A)}(\Omega_{B|A})_{\mathfrak{q}_i} \otimes_A k(A) = e_i - 1 \tag{1.16}$$

ist.

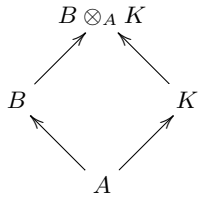
Proposition 1.4.1. *Ist $f : X \to Y$ ein separabler Morphismus nichtsingulärer Kurven, so ist $\Omega_{X|Y}$ ein $\mathcal{O}_X$–Torsionsmodul. Es gilt dann*

$$\Omega_{X|Y} = \sum_{P\in X} \mathcal{O}_{X,P}/\mathfrak{m}_P^{e_P-1} \tag{1.17}$$

wenn $\operatorname{char} k \nmid e_P$ für alle $P \in X$.

Beweis. Lokal ist f gegeben durch eine Erweiterung von Dedekindringen B/A mit Quotientenkörpern L/K und $U = \operatorname{Spec}(B) \subseteq X$ sowie $V = \operatorname{Spec}(A) \subseteq Y$.

Betrachte das cartesische Diagramm



mit $B \otimes_A K = L$

Aus dem Diagramm folgt $\Omega_{B|A} \otimes_B L = \Omega_{L|K} = 0$ weil L/K separabel. Also ist $\Omega_{B|A}$ ein B–Torsionsmodul und damit auch $\Omega_{X|Y}$ ein $\mathcal{O}_X$–Torsionsodul

Die Behauptung folgt dann aus den vorangegangenen Überlegungen über B–Torsionsmoduln M im allgemeinen und den Modul $\Omega_{B|A} \otimes_A k(A)$ im besonderen.

1.5 Hurwitz–Formel

Es sei $f : X \to Y$ eine Abbildung vom Überlagerungsgrad n von nichtsingulären Kurven über k. Weiter seien g_X und g_Y die Geschlechter von X und Y, sowie e_P für $P \in X$ der Verzeigungsgrad von f bei P. Es gelte $\operatorname{char} k \nmid e_P$ für alle $P \in X$.

Proposition 1.5.1 (Hurwitz). *Mit den obigen Begriffen gilt:*

$$(2g_X - 2) = n\,(2g_Y - 2) + \sum_{P\in X} (e_P - 1)$$

Beweis. Es ist $\Omega_{X|k}$ und $\Omega_{Y|k}$ lokal freier $\mathcal{O}_X$– bzw. $\mathcal{O}_Y$–Modul (Linienbündel). Weiter ist $\Omega_{X|k} = \mathcal{O}_X(K_X)$ und $\Omega_{Y|k} = \mathcal{O}_Y(K_Y)$ per definitionem.

Man hat die Sequenz

$$0 \to f^*\Omega_{Y|k} \to \Omega_{X|k} \to \Omega_{X|Y} \to 0$$

Nur die 0 links ist zu begründen: Ist lokal $\mathcal{O}_{Y,y} = A$ und $\mathcal{O}_{X,x} = B$, so ist $\Omega_{Y|k,y} = A$ und $\Omega_{X|k,x} = B$. Man hat also links eine B–lineare Abbildung $B \otimes_A A \to B$. Gäbe es einen Kern, so hätte man $0 \to \mathfrak{b} \to B \to B$ mit $\mathfrak{b} \supsetneq (0)$. Also $B/\mathfrak{b} \hookrightarrow B$. Betrachtet man Ass_B auf beiden Seiten, so stünde links $\mathfrak{m}_B$ und rechts (0). Da aber $\operatorname{Ass} B/\mathfrak{b} \subseteq \operatorname{Ass} B$ wäre das ein Widerspruch. Also steht links die 0. ($\mathfrak{b} = B$ ist ausgeschlossen, da sonst $\Omega_{X|Y,x} = \Omega_{X,x} = B$ und damit $\Omega_{X|Y}$ keine Torsionsgarbe wäre).

$\Omega_{X|Y}$ ist eine Torsionsgarbe

$$\Omega_{X|Y} = \sum_{P \in X} \mathcal{O}_{X,P}/\mathfrak{m}_P^{e_P - 1}$$

mit Träger den Punkten $P \in X$ für die $e_P > 0$ ist.

Man tensoriere nun die obige Sequenz mit $\Omega_{X|k}^{-1}$ und erhalte

$$0 \to \Omega_{X|k}^{-1} \otimes f^*\Omega_{Y|k} \to \mathcal{O}_X \to \Omega_{X|Y} \to 0$$

Der $\operatorname{supp} \Omega_{X|Y}$ ist gleich dem effektiven Divisor $R = \sum_{P \in X}(e_P - 1)P$.

Dann ist $\Omega_{X|k}^{-1} \otimes f^*\Omega_{Y|k} = \mathcal{O}_X(-R)$. Also wenn man deg anwendet

$$-(2g_X - 2) + n\,(2g_Y - 2) = -\sum_{P \in X}(e_P - 1)$$

also

$$(2g_X - 2) = n\,(2g_Y - 2) + \sum_{P \in X}(e_P - 1)$$

Das ist die Hurwitzformel.

2

Geometrie der elliptischen Kurven

2.1 Weierstraß–Normalform

Es sei X/k eine algebraische Kurve vom Geschlecht $g(X) = 1$ über einem algebraisch abgeschlossenen Körper k.

Lemma 2.1.1. *Es sei $D = P + Q$ ein Divisor auf X. Dann definiert D eine $2-1$ Überlagerung $X \to \mathbb{P}^1_k$*

Beweis. Wegen $l(D) = \deg D + 1 - g = \deg D$ für $\deg D > 1$ (beachte $\deg K = 2g - 2 = 0$) ist $l(D - R) < l(D)$ für jeden Punkt $R \in X$, also D basispunktfrei. Es gibt also eine nichtkonstante meromorphe Funktion $f \in K(X)$, die höchstens P und Q als Pole aufweist. Ein einfacher Pol einer solchen meromorphen Funktion kann nicht vorkommen, da sonst $X \cong \mathbb{P}^1_k$ wäre. Also ist $P+Q = f^{-1}(\infty)$ und $W \mapsto f(W)$ definiert eine $2-1$ Überlagerung $X \to \mathbb{P}^1_k$.

Lemma 2.1.2. *Es seien $P, Q \in X$ zwei Punkte auf X. Dann existiert ein Isomorphismus $\sigma : X \to X$ mit $Q = \sigma(P)$, $\sigma^2 = \mathrm{id}_X$ und $R + \sigma(R) \sim P + Q$.*

Beweis. Setze $D = P+Q$ und erhalte nach vorigem Lemma eine $2-1$ Überlagerung $\pi : X \to \mathbb{P}^1_k$. Die Punkte P und Q sind die Urbilder von $\infty \in \mathbb{P}^1_k$. Die Überlagerung π definiert eine Körpererweiterung $k(x) \subseteq K(X)$ mit $k(x) = K(\mathbb{P}^1_k)$ vom Grad 2. Es gibt also einen Körperautomorphismus $\sigma' : K(X) \to K(X)$ über $k(x)$. Dieser korrespondiert mit einem Kurvenmorphismus $\sigma : X \to X$ mit $\pi \circ \sigma = \pi$. Also ist $\sigma(P) = Q$ und $\sigma(Q) = P$, sowie generell $\sigma^2 = \mathrm{id}_X$, weil $\sigma'^2 = \mathrm{id}_{K(X)}$.

Schließlich ist für jedes $R \in X$ immer $\pi(R) = \pi(\sigma(R)) = W \in \mathbb{P}^1_k$, also $R + \sigma(R) = \pi^{-1}(W)$. Aufgrund allgemeiner Sätze über Divisoren auf Kurven ist damit schon $R + \sigma(R) \sim \pi^{-1}(\infty) = P + Q$ gezeigt.

Lemma 2.1.3. *Es sei X wie oben und $f_1, f_2 : X \to \mathbb{P}^1_k$ zwei $2-1$ Überlagerungen. Dann existieren immer Automorphismen $\sigma : X \to X$ und $\tau : \mathbb{P}^1_k \to \mathbb{P}^1_k$, so daß*

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle f_2} \\ \mathbb{P}^1_k & \xrightarrow{\tau} & \mathbb{P}^1_k \end{array}$$

kommutiert.

Beweis. Man wendet zunächst Automorphismen τ_1 und τ_2 an, so daß f_1 und f_2 über ∞ verzweigt mit Verzweigungsindex 2 sind. Es ist also dann $f_i^{-1}(\infty) = 2P_i$ mit $P_i \in X$. Wähle dann nach vorigem Lemma ein $\sigma : X \to X$ mit $\sigma(P_1) = P_2$. Man kann dann also annehmen, daß $f_1^{-1}(\infty) = 2P = f_2^{-1}(P)$ ist. Es werden also dann f_1, f_2 durch meromorphe Schnitte ξ_1, ξ_2 von $\mathcal{O}_X(2P)$ gegeben, für die $\xi_i(P) = \infty$ ist. Da $l(2P) = 2$ ist, gibt es also immer Konstanten $a, b \in k$ mit $\xi_2 = a\xi_1 + b$ und somit unterscheiden sich f_1 und f_2 um einen Automorphismus $\tau(z) = az + b$ für eine Koordinate z von $\mathbb{P}^1_k$ mit $z(\infty) = \infty$.

Proposition 2.1.1. *Es sei X eine Kurve, wie oben. Dann exisiert eine abgeschlossene Immersion*

$$i : X \to \mathbb{P}^2_k$$

für die $i(X) = \overline{V(f)}$ mit $\lambda \in k$ und einem Polynom

$$f(x, y) = y^2 - x(x-1)(x-\lambda)$$

ist, wobei $\overline{V(f)}$ für den Abschluß in $\mathbb{P}^2_k$ der affinen Verschwindungsmenge von f in $\mathbb{A}^2_k \subseteq \mathbb{P}^2_k$ steht. In diesem Abschluß tritt noch ein Punkt $i(P_0) = [0:1:0]$ zu $V(f)$ hinzu.

2.2 Gruppengesetz

2.3 Isogenien

Es seien (E_1, O_1) und (E_2, O_2) zwei elliptische Kurven über K.

Definition 2.3.1. *Es sei $f : E_1 \to E_2$ ein Morphismus von algebraischen Kurven über K mit $f(O_1) = O_2$. Dann heißt f eine* Isogenie von E_1 nach E_2 über K *und E_1 und E_2 heißen* isogen.

Proposition 2.3.1. *Es sei $f : E_1 \to E_2$ eine Isogenie. Dann ist f sogar ein Gruppenhomomorphismus, also*

$$f(P + Q) = f(P) + f(Q) \tag{2.1}$$

für alle $P, Q \in E_1$. Anders gesagt

$$\begin{array}{ccc} E_1 \times E_1 & \xrightarrow{(f,f)} & E_2 \times E_2 \\ {\scriptstyle \mu_1}\downarrow & & \downarrow{\scriptstyle \mu_2} \\ E_1 & \xrightarrow{f} & E_2 \end{array} \tag{2.2}$$

kommutiert.

Beweis. Die Abbildung $h = \mu_2 \circ (f, f) - f \circ \mu_1 : E_1 \times E_1 \to E_2$ hat die Eigenschaft $h(P, 0) = h(0, P) = 0$ für alle $P \in E_1$. Da E_1 eigentlich ist, folgt nach dem „Rigidity Lemma“, daß $h(P, Q) = 0$ für alle $P, Q \in E_1$.

Lemma 2.3.1. *Es seien $f : E_1 \to E_2$ und $g : E_2 \to E_3$ Isogenien. Dann ist auch $g \circ f : E_1 \to E_3$ eine Isogenie.*

Lemma 2.3.2. *Die Abbildung $-\mathrm{id}_E : P \mapsto -P$ ist eine Isogenie auf der elliptischen Kurve E.*

Es seien $f, g : E_1 \to E_2$ zwei Isogenien. Dann sind auch $f+g = \mu_2 \circ (f, g) \circ \Delta$ mit $\Delta : E_1 \to E_1 \times E_1$, der Diagonaleinbettung, und $-f = -\mathrm{id}_{E_2} \circ f$ Isogenien.

Proposition 2.3.2. *Die Menge $\mathrm{Hom}_K(E_1, E_2)$ der Isogenien über K von E_1 nach E_2 ist eine abelsche Gruppe.*

Anmerkung 2.3.1. Mit $\mathrm{End}_K(E)$ bezeichnen wir $\mathrm{Hom}_K(E, E)$ und mit $\mathrm{Aut}_K(E)$ die $f \in \mathrm{End}_K(E)$ für die ein $g \in \mathrm{End}_K(E)$ existiert mit $f \circ g = g \circ f = \mathrm{id}_E$.

Es sei E eine elliptische Kurve. Dann sei $[0] : E \to E$ die Isogenie $f(P) = 0_E$ und $[N] : E \to E$ definiert durch $[N] = [N-1] + \mathrm{id}_E$. für alle $N > 0$ und durch $[N] = -[-N]$ für $N < 0$.

Definition 2.3.2. *Die Isogenie $[N] : E \to E$ heißt* Multiplikation mit N.

Lemma 2.3.3. *Es sei E eine elliptische Kurve und $[2] : E \to E$ die Multiplikation mit 2. Dann ist $[2]$ surjektiv und es gibt $P \neq O_E \in E$ mit $2P = 0$.*

Proposition 2.3.3. *Die Isogenie $[N] : E \to E$ ist für alle $N \geqslant 1$ von Null verschieden und surjektiv.*

Beweis. Es sei $N = 2N'$ und $N' P \neq 0$. Nach vorigem Lemma ist $P = 2\,Q$ und damit $N\,Q = N' 2\,Q = N'\,P \neq 0$.

Es sei $N = 2N' + 1$. Wäre $N\,P = 0$ für alle P, so wäre $2N'\,P = -P$ für alle $P \in P$. Sei nun $2\,P = 0$ mit $P \neq O_E$, so folgte $-P = O_E$, Widerspruch.

2.4 Invariantes Differential

Es sei E eine elliptische Kurve mit $y^2 = x^3 + Ax + B$ als Weierstraßgleichung. Dann ist

$$\omega = \frac{dx}{y} \in \Omega_{K(E)|k}$$

ein invariantes Differential, das heißt für jedes $P \in X$ ist $\tau_P^* \omega = \omega$

Proposition 2.4.1. *Es sei E eine elliptische Kurve mit Gruppengesetz $\mu : E \times E \to E$. und Projektionen $p_i : E \times E \to E$ mit $i = 1, 2$.*

Dann gilt die Gleichheit

$$p_1^* \omega + p_2^* \omega = \mu^* \omega \tag{2.3}$$

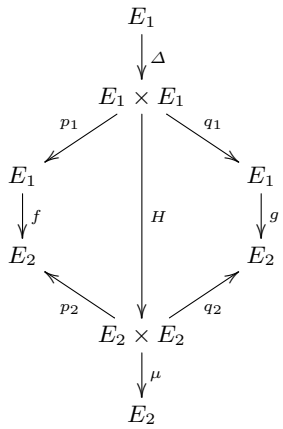
in $\Omega_{K(E \times E)|k}$.

Proposition 2.4.2. *Es seien $f, g : E_1 \to E_2$ zwei Isogenien elliptischer Kurven. Dann gilt für ein invariantes Differential $\omega \in \Omega_{K(E_2)|k}$ die Beziehung*

$$(f+g)^*\omega = f^*\omega + g^*\omega \tag{2.4}$$

in $\Omega_{K(E_1)|k}$.

Beweis. Betrachte das Diagramm:



(2.5)

Es ist $(f+g)^*\omega = \Delta^* H^* \mu^* \omega$. Nun ist nach voriger Proposition

$$H^*(\mu^*\omega) = H^*(p_2^*\omega + q_2^*\omega) = p_1^* f^*\omega + q_1^* g^*\omega \tag{2.6}$$

und deshalb

$$\Delta^* H^* \mu^*(\omega) = \Delta^* p_1^* f^*\omega + \Delta^* q_1^* g^*\omega = f^*\omega + g^*\omega \tag{2.7}$$

Es folgt die Behauptung.

2.5 Duale Isogenien

Proposition 2.5.1. *Es sei (E, O_E) eine elliptische Kurve und $\mathrm{Pic}^0(E)$ die Gruppe der Divisoren vom Grad 0 auf E. Dann ist die Zuordnung*

$$\Phi_E : E \to \mathrm{Pic}^0(E), \quad P \mapsto [P] - [O_E] \tag{2.8}$$

ein Gruppenisomorphismus

Definition 2.5.1. *Es sei $f : E_1 \to E_2$ eine Isogenie elliptischer Kurven. Das Diagramm*

$$\begin{array}{ccc} \mathrm{Pic}^0(E_1) & \xleftarrow[\Phi_{E_1}]{} & E_1 \\ {\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle \widehat{f}} \\ \mathrm{Pic}^0(E_2) & \xleftarrow[\Phi_{E_2}]{} & E_2 \end{array} \tag{2.9}$$

definiert eine Isogenie $\widehat{f} : E_2 \to E_1$, die duale Isogenie.

Es sei E/k eine elliptische Kurve über dem Körper k. Weiter sei

$$\mu : E \times_k E \to E \tag{2.10}$$

der Morphismus der Addition auf der elliptischen Kurve.

Es seien $p_1, p_2 : E \times_k E \to E$ die kanonischen Projektionen auf den ersten und zweiten Faktor und es sei $\mathcal{L} = \mathcal{L}(D)$ das Linienbündel auf E zu einem Divisor D auf E vom Grad $\deg D = 0$.

Lemma 2.5.1. *Es sei*

$$\mathcal{L} \in \mathrm{Pic}^0(E) \tag{2.11}$$

Dann gilt mit obigen Bezeichnungen die Beziehung

$$\mu^*\mathcal{L} = p_1^*\mathcal{L} \otimes p_2^*\mathcal{L} \tag{2.12}$$

Beweis. Wir zeigen zunächst, daß $\mu^*\mathcal{L} \otimes (p_1^*\mathcal{L})^{-1}$ auf den Fasern $p_2^{-1}(P) = E \times P$ für einen Punkt $P \in E$ immer trivial ist, also

$$\left(\mu^*\mathcal{L} \otimes (p_1^*\mathcal{L})^{-1}\right)|_{E\times P} \cong \mathcal{O}_{E\times P} \tag{2.13}$$

ist.

Es ist nämlich $\mu^*\mathcal{L}|_{E\times P} \cong \tau_P^*\mathcal{L}|_E$, wobei $\tau_P : E \to E$ die Abbildung $Q \mapsto P + Q$ ist.

Weiterhin ist $(p_1^*\mathcal{L})|_{E\times P} \cong \mathcal{L}|_E$. Nun ist aber der Divisor D, der zu $\mathcal{L}$ gehört vom Grad 0, also

$$D = \sum_i n_i P_i, \quad \sum_i n_i = 0 \tag{2.14}$$

Damit ist $\tau_P^*(D) = \sum_i n_i(P_i - P) \sim \sum_i n_i P_i = D$. Also ist $\tau_P^*\mathcal{L} = \mathcal{L}$ auf E und damit $\left(\mu^*\mathcal{L} \otimes (p_1^*\mathcal{L})^{-1}\right)|_{E\times P} = \mathcal{O}_{E\times P}$ wie behauptet.

Nach den Halbstetigkeitssätzen ist dann

$$\mu^*\mathcal{L} \otimes (p_1^*\mathcal{L})^{-1} = p_2^*\mathcal{N} \tag{2.15}$$

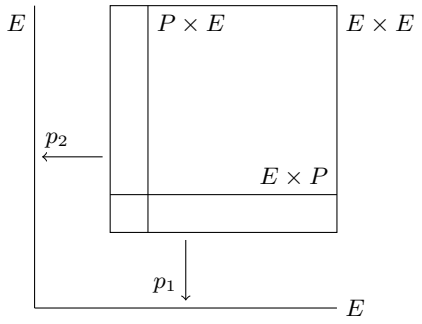
mit einem zunächst unbekannten Linienbündel $\mathcal{N}$ auf E.

Wir betrachten nun $(p_2^*\mathcal{N})|_{P\times E}$. Es ist $\mu^*\mathcal{L}|_{P\times E} = \tau_P^*\mathcal{L}|_E = \mathcal{L}|_E = p_2^*\mathcal{L}|_{P\times E}$. Weiter ist $p_1^*\mathcal{L}|_{P\times E} = \mathcal{O}_{P\times E}$, da $p_1^{-1}(P) = P \times E$ ist. Also ist $p_2^*\mathcal{N}|_{P\times E} = p_2^*\mathcal{L}|_{P\times E}$ für alle $P \in E$ und damit

$$\mu^*\mathcal{L} \otimes (p_1^*\mathcal{L})^{-1} = p_2^*\mathcal{L} \tag{2.16}$$

was offensichtlich äquivalent zur Behauptung ist.

Siehe zur Veranschaulichung der einzelnen Abbildungen und Einschränkungen auf die Fasern auch das folgende Bild:



Proposition 2.5.2. *Es seien $f, g : E_1 \to E_2$ zwei Isogenien. Dann ist*

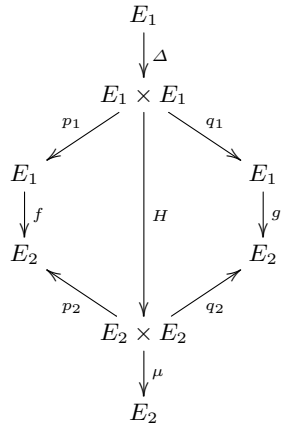
$$(f+g)\widehat{\ } = \widehat{f} + \widehat{g}$$

Beweis. Es ist zu zeigen, daß für jedes $\mathcal{L} \in \mathrm{Pic}^0(E_2)$ immer

$$(f+g)^*\mathcal{L} = f^*\mathcal{L} \otimes_{\mathcal{O}_{E_1}} g^*\mathcal{L}$$

ist.

Betrachte das Diagramm



(2.17)

Es ist

$$(f+g)^*\mathcal{L} = \Delta^* H^* \mu^* \mathcal{L} = \Delta^* H^* (p_2^*\mathcal{L} \otimes q_2^*\mathcal{L}).$$

Weiterhin ist aber auch $p_2 \circ H \circ \Delta = f \circ p_1 \circ \Delta = f$ und $q_2 \circ H \circ \Delta = g \circ q_1 \circ \Delta = g$. Also $\Delta^* H^* p_2^*\mathcal{L} = f^*\mathcal{L}$ und $\Delta^* H^* q_2^*\mathcal{L} = g^*\mathcal{L}$. Insgesamt also

$$\Delta^* H^* (p_2^*\mathcal{L} \otimes q_2^*\mathcal{L}) = f^*\mathcal{L} \otimes g^*\mathcal{L}$$

2.6 Weilpaarung

Es sei E/K eine elliptische Kurve und $[m] : E \to E$ die Multiplikation mit m. Wir wollen für $S, T \in E[m]$ eine Weilpaarung $e(S,T) \in \mu_m(K)$ definieren.

Die Details der Definition der Weilpaarung sind am einfachsten rückwärts zu merken:

Wir wollen für ein $S \in E[m]$ eine Funktion $g(X) \in K(E)$ definieren, die von einem $T \in E[m]$ abhängt und für die

$$(g(X+S)/g(X))^m = 1$$

gilt. Es wird dann $e(S,T) = g(X+S)/g(X)$ eine m-te Wurzel in K, die *Weilpaarung von S und T* sein. Eine solche Funktion g ist zum Beispiel eine, die

$$g(X)^m = f([m]X)$$

für eine geeignete Funktion $f = f_T$ erfüllt, denn es ist dann ja

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

Wir brauchen also eine Funktion $f(X)$, so daß man aus $f([m]X)$ die m-te Wurzel in $K(E)$ ausziehen kann.

Diese ist aber durch $\operatorname{div}(f) = m\,[T] - m\,[0] = m\,([T] - [0])$ definierbar. Es ist ja mit einem T', für das $[m]T' = T$ gilt

$$\operatorname{div} f([m]X) = m\left(\sum_{W \in E[m]} [T'+W] - \sum_{W \in E[m]} [W]\right),$$

da man für $\operatorname{div} f([m]X)$ die Urbilder von T und 0 unter $[m]$ aufzusuchen hat. Zwei Urbilder $[m]T' = T$ und $[m]T'' = T$ unterscheiden sich dann um ein $T' - T''$ mit $[m](T' - T'') = 0$. Daher die obige Formel.

Nun definiert aber schon der Divisor

$$D_g = \sum_{W \in E[m]} [T'+W] - \sum_{W \in E[m]} [W]$$

eine Funktion $g = g_T$, denn die Summe der Punkte der Divisoren addieren sich zu $0_E \in E$, weil $[m^2]T' = 0$ und auch die Koeffizienten addieren sich zu $0 \in \mathbb{Z}$.

Für diese Funktion g mit $\operatorname{div} g = D_g$ gilt dann unser gewünschtes

$$g(X)^m = f([m]X)$$

Definition 2.6.1. *Die Abbildung*

$$e : E[m] \times E[m] \to \mu_m, \quad (S,T) \mapsto e(S,T)$$

ist die sogenannte Weilpaarung.

Proposition 2.6.1. *Die Weilpaarung erfüllt folgende Beziehungen:*

1. Bilinearität:

$$e(S+S',T) = e(S,T)e(S',T)$$
$$e(S,T+T') = e(S,T)e(S,T')$$

für $S, S', T, T' \in E[m]$.

2. Antisymmetrie:

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

für $S, T \in E[m]$.

3. Verträglichkeit mit der Galoisoperation von $G_{\bar{K}|K}$:

$$e(S,T)^\sigma = e(S^\sigma, T^\sigma) \tag{2.18}$$

für $\sigma \in G_{\bar{K}|K}$ und $S, T \in E[m]$.

Beweis. 1. Es ist zunächst

$$\begin{aligned} e(S+S',T) &= g_T(X+S+S')/g_T(X) = \\ &= \big(g_T(X+S+S')/g_T(X+S)\big)\,(g_T(X+S)/g_T(X)) = e(S',T)e(S,T) \end{aligned}$$

denn es ist $g_T(X+S+S')/g_T(X+S) = g_T(Y+S')/g_T(Y) = e(S',T)$.

Weiterhin ist $g_{T+T'}(X)$ definiert durch den Divisor

$$\sum_{W\in E[m]} [\tilde{T}+\tilde{T}'+W] - \sum_{W\in E[m]} [W] = \\ (\sum_W [\tilde{T}+\tilde{T}'+W] - \sum_W [\tilde{T}'+W]) + (\sum_W [\tilde{T}'+W] - \sum_W [W])$$

für $[m]\tilde{T} = T$ und $[m]\tilde{T}' = T'$. Das ist aber der Divisor von $g_T(X-\tilde{T}')g_{T'}(X)$, also gilt

$$g_{T+T'}(X) = c g_T(X-\tilde{T}')g_{T'}(X)$$

und somit

$$\begin{aligned} e(S,T+T') &= g_{T+T'}(X+S)/g_{T+T'}(X) = \\ &= g_T(X-\tilde{T}'+S)/g_T(X-\tilde{T}')g_{T'}(X+S)/g_{T'}(X) = e(S,T)e(S,T'). \end{aligned}$$

2. Es gilt nach 1.

$$e(S+T,S+T) = e(S,S)e(S,T)e(T,S)e(T,T).$$

Also genügt es zu zeigen, daß $e(T,T) = 1$ für alle $T \in E[m]$ ist.

Betrachte die Funktion

$$w(X) = g(X)g(X+T')\cdot\dots\cdot g(X+(m-1)T')$$

mit $g(X) = g_T(X)$ und $[m]T' = T$. Es ist

$$w(X)^m = f_T(mX)f_T(mX+T)\cdot\dots\cdot f_T(mX+(m-1)T)$$

Nun ist aber mit $v(y) = f_T(y)f_T(y+T)\cdot\dots\cdot f_T(y+(m-1)T)$ auch

$$\operatorname{div} v = \sum_{i=0}^{m-1} (X+iT)^*(m([T]-[0])) = m\sum_{i=0}^{m-1}([(1-i)T]-[-iT]) = 0$$

Also ist $v(y) = c$ konstant, also $w(X)^m = v([m]X) = c$ ebenfalls konstant. Damit ist auch $w(X)$ konstant und wir haben

$$w(X) = w(X+T').$$

Streicht man die rechts und links gleichen Terme $g(X+iT')$ so entsteht $g(X) = g(X+T)$, also $e(T,T) = 1$, was zu beweisen war.

3

Elliptische Kurven über endlichen Körpern

4

Elliptische Kurven über lokalen Körpern

5

Theorie der Höhen

6

Elliptische Kurven über globalen Körpern

Literaturverzeichnis

[1] Silverman, Joseph H.: *The arithmetic of elliptic curves.* 1986