ELLIPTISCHE KURVEN UND ABELSCHE VARIETÄTEN

MARTIN BIDLINGMAIER

1. Varietäten als Schemata

In bisherigen Vorträgen wurde stets die klassische Sprache der algebraischen Geometrie genutzt. In diesem Abschnitt wird erklärt, wie klassische Begriffe sich im Schema-Formalismus formulieren lassen. Besonderes Augenmerk wird auf die Definition einer „Varietät über k“, k ein nicht notwendig algebraisch abgeschlossener Körper, und deren k-rationalen Punkten gelegt.

Satz 1.1. *Sei k ein Körper, V eine über k definierte affine (projektive) Varietät im Sinne von [4, Kap. I].*
V ist also Nullstellenmenge eines (homogenen) Primideals $\mathfrak{p} \subseteq k[\underline{X}]$ in $\mathbb{A}^n_K$ bzw. $\mathbb{P}^n_K$.
Sei $X = \operatorname{Spec} k[X_1, \dots, X_n]/\mathfrak{p}$ bzw. $X = \operatorname{Proj} k[X_1, \dots, X_n]/\mathfrak{p}$. Dann ist für jede algebraische Erweiterung $L|k$

$$V(L) = \{P \in V \mid P \text{ ist } L\text{-rational}\} \cong \operatorname{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L, X_L).$$

Dabei bezeichnet $X_L = X \times_{\operatorname{Spec} k} \operatorname{Spec} L$ den Basiswechsel nach $\operatorname{Spec} L$.

Beweis. Sei zunächst V affin. Dann ist

$$X_L = \operatorname{Spec} k[X_1, \dots, X_n]/\mathfrak{p} \otimes_k L = \operatorname{Spec} L[X_1, \dots, X_n]/\mathfrak{p}_L,$$

wobei $\mathfrak{p}_L$ das von $\mathfrak{p}$ in $L[X_1, \dots, X_n]$ erzeugte Ideal sei. Man erhält Bijektionen (siehe [1, §3 Prop. 3.8])

$$\begin{aligned}
\operatorname{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L, X) &\cong \{(P, i) \mid P \in X, i\colon \kappa(P) \to L \text{ Morphismus von } L\text{-Algebren}\} \\
&\cong \{P \in X \mid \kappa(P) \cong L\} \\
&\cong \{P \in X \mid P = (X_1 - a_1, \dots, X_n - a_n) \text{ für gewisse } a_1, \dots, a_n \in L\} \\
&\cong V(L).
\end{aligned}$$

Der Fall V projektiv lässt sich einfach durch eine offene affine Überdeckung des $\mathbb{P}^n$ auf den affinen Fall zurückführen. □

Für $L = k$ erhält man insbesondere eine Charakterisierung der k-rationalen Punkte von V:

$$V(k) \cong \operatorname{Hom}_{\operatorname{Spec} k}(\operatorname{Spec} k, X)$$

Bemerkung 1.2. Für beliebige Primideale $\mathfrak{p} \subset k[X_1, \dots X_n]$ ist (in der Notation von 1.1) X_L nicht notwendig irreduzibel. Das Ideal $\mathfrak{p} = (X^2 + 1) \subset \mathbb{R}[X]$ ist irreduzibel, nach Übergang zu $\mathbb{C}$ zerfällt es jedoch.
Schemata, die nach Basiswechsel zu beliebigen Erweiterungskörpern irreduzibel bleiben, heißen auch *geometrisch irreduzibel*. Analog definiert man auch *geometrisch zusammenhängend*, *geometrisch reduziert*, usw..

2. Jakobische Varietät

Eine Besonderheit elliptischer Kurven ist die Tatsache, dass diese Kurven ihre eigene Jakobische sind. Die Jakobische einer Kurve ist eine Varietät, deren k-rationale Punkte eine zur Pic^0-Gruppe der Kurve isomorphe Gruppenstruktur tragen. Der Beweis der Existenz der Jakobischen allgemeiner Kurven erfordert fortgeschrittene Techniken; im Falle von elliptischen Kurven, die über die im letzten Vortrag vorgestellte Gruppenstruktur ihre eigene Jakobischen sind, aber mit unseren Mitteln möglich. In diesem Abschnitt wird (ohne Beweise) ein kurzer Einblick in die Theorie der Jakobischen gegeben. Für eine ausführlichere Abhandlung siehe etwa [2] oder [3].
Jakobische Varietäten sind Gruppenobjekte in der Kategorie der Schemata über k. Unter einem Gruppenobjekt kann anschaulich ein Objekt einer Kategorie verstanden werden, das die Struktur einer Gruppe trägt. Da Objekte in allgemeinen Kategorien nicht notwendig Elemente besitzen, muss diese Struktur „elementfrei“ durch Angabe von Morphismen gegeben werden.

Definition 2.1. Sei C eine Kategorie, in der endliche Produkte existieren. Insbesondere besitzt C ein terminales Objekt $*$. Ein Objekt $G \in C$ zusammen mit Morphismen

$$\begin{aligned} m &\colon E \times E \to E \\ i &\colon E \to E \\ e &\colon * \to E \end{aligned}$$

so, dass die Diagramme

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathrm{id}_G \times m} & G \times G \\ \downarrow{\scriptstyle m \times \mathrm{id}_G} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{\quad m \quad} & G \end{array} \qquad \text{„Assoziativität“}$$

$$\begin{array}{ccc} G \times * & \xrightarrow{\langle \mathrm{id}_G, e \rangle} & G \times G \\ \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\quad \mathrm{id}_G \quad} & G \end{array} \qquad \text{„Neutrales Element“}$$

$$\begin{array}{ccc} G & \xrightarrow{\langle \mathrm{id}_G, i \rangle} & G \times G \\ \downarrow{\scriptstyle \mathrm{id}_G} & & \downarrow{\scriptstyle m} \\ * & \xrightarrow{\quad e \quad} & G \end{array} \qquad \text{„Inverses Element“}$$

kommutieren, heißt *Gruppenobjekt*. Kommutiert auch

$$\begin{array}{ccc} G \times G & \xrightarrow{\langle \pi_2, \pi_1 \rangle} & G \times G \\ \downarrow{\scriptstyle \mathrm{id}_{G \times G}} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{\quad m \quad} & G \end{array} \qquad \text{„Kommutativität“},$$

so heißt G *abelsches* Gruppenobjekt.

Bemerkung 2.2. Ein Gruppenobjekt G kann über die Yoneda-Einbettung auch folgendermaßen charakterisiert werden:
Ist $S \in C$ ein beliebiges Objekt, so wird $\mathrm{Hom}(S, G)$ vermöge

$$\begin{aligned} f \cdot g &\coloneqq m \circ (f \times g) \\ 1 &= e \circ (S \to *) \\ f^{-1} &= i \circ f \end{aligned}$$

für $f, g \in \mathrm{Hom}(S, G)$ zur Gruppe. Ein Morphismus $\phi \in \mathrm{Hom}(S, T)$ ergibt mit dieser Definition einen Gruppenhomomorphismus

$$- \circ \phi \colon \mathrm{Hom}(T, G) \to \mathrm{Hom}(S, G).$$

Ist umgekehrt für alle $S \in C$ eine in S funktorielle (abelsche) Gruppenstruktur auf $\mathrm{Hom}(S, G)$ gegeben, so ergeben die natürlichen Transformationen

$$\begin{aligned} \eta_m &\colon \begin{cases} \mathrm{Hom}(-, G) \times \mathrm{Hom}(-, G) \to \mathrm{Hom}(-, G) \\ \mathrm{Hom}(S, G) \times \mathrm{Hom}(S, G) \ni (f, g) \mapsto f + g \in \mathrm{Hom}(S, G) \end{cases} \\ \eta_i &\colon \begin{cases} \mathrm{Hom}(-, G) \to \mathrm{Hom}(-, G) \\ \mathrm{Hom}(S, G) \ni f \mapsto f^{-1} \in \mathrm{Hom}(S, G) \end{cases} \\ \eta_e &\colon \begin{cases} \mathrm{Hom}(-, *) \to \mathrm{Hom}(-, G) \\ \mathrm{Hom}(S, *) \ni f \mapsto 1 \in \mathrm{Hom}(S, G) \end{cases} \end{aligned}$$

nach dem Yoneda-Lemma

$$X \mapsto \mathrm{Hom}(-, X) \text{ ist voll-treue Einbettung in die Funktorkategorie } \mathrm{Mor}(C, \mathrm{Set})$$

die Morphismen m, i und e wie in 2.1.

Definition 2.3. Ein Gruppenobjekt in der Kategorie der Schemata über einem Schema S heißt *algebraische Gruppe über S.*

Definition 2.4. Sei k ein Körper. Eine algebraische Gruppe A über k heißt *abelsche Varietät über k*, falls A geometrische integer und eigentlich über k ist.

Die Bezeichnung *abelsche* Varietät ist durch folgenden Satz gerechtfertigt:

Satz 2.5. *Eine abelsche Varietät über k ist notwendig projektiv und ein abelsches Gruppenobjekt.* □

Nun stehen alle Begriffe bereit, um die Existenz der Jakobischen zu formulieren:

Satz 2.6. *Sei C eine glatte, geometrische zusammenhängende, projektive Kurve über k vom Geschlecht g. Dann existiert eine abelsche Varietät J über k der Dimension g so, dass*

$$J(L) \cong \mathrm{Pic}^0(C_L)$$

für jede Körpererweiterung $L|k$ mit $C(L) \neq \varnothing$, funktoriell in L. □

3. Elliptische Kurven

In diesem Abschnitt wird die Gleichheit elliptischer Kurven und ihrer Jakobischen bewiesen. Zu Beginn werden elliptische Kurven als nichtsinguläre Kurven vom Geschlecht 1 mit einem ausgezeichneten Basispunkt definiert. Bis auf Isomorphie erfüllen diese Bedingung genau die nichtsingulären, durch eine Weierstraß-Gleichung gegebenen Kurven.
Im zweiten Teil wird eine Isomorphie der Pic^0-Gruppe mit der durch die im letzten Vortrag kennen gelernten Addition auf einer elliptischen Kurve gegebenen Gruppenstruktur bewiesen werden. Da die Addition auf elliptischen Kurven sich als Morphismus herausstellen wird, ist die elliptische Kurve damit ihre eigene Jakobische. Dieser Abschnitt ist wieder in der klassischen Sprache der Varietäten in Anlehnung an [4] forumiert, woraus dieser auch weitgehend übernommen wurde.

Definition 3.1. Ein Paar (E, O), wobei E eine nichtsinguläre Kurve vom Geschlecht 1, $O \in E$ ein Punkt sind, heißt *elliptische Kurve*. Eine elliptische Kurve heißt *definiert über k*, falls E über k definiert ist und $O \in E(k)$. Insbesondere besitzt E dann einen k-rationalen Punkt.

Notation. Im Folgenden sei stets k ein Körper mit algebraischem Abschluss K, (E, O) eine über k definierte elliptische Kurve. Statt (E, O) schreiben wir auch häufig E, womit implizit eine elliptische Kurve mit Basispunkt O gemeint ist.

Satz 3.2. *Es existieren $x, y \in k(E)$ so, dass*

$$\phi = [x, y, 1] : E \to C$$

ein Basispunkt-erhaltender Isomorphismus von E mit einer durch eine Weierstraß-Gleichung definierten Kurve $C \subset \mathbb{P}^2$ über k ist.
C ist also gegeben durch

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

mit $a_1, \ldots, a_6 \in k$ und

$$\phi(O) = (0 : 1 : 0).$$

Beweis. Nach dem Satz von Riemann-Roch und $O \in E(k)$ ist für $n \geqslant 1$

$$\dim \mathcal{L}(n(O)) = \dim \mathcal{L}(n(O)) \cap k(E) = n.$$

Es existiert also $x \in E(k)$ so, dass $\{1, x\}$ eine Basis von $\mathcal{L}(2(O))$ ist. Das linear unabhängige System $\{1, x\}$ lässt sich nun in $\mathcal{L}(3(O))$ um ein $y \in E(k)$ zu einer Basis dieses Vektorraums ergänzen. Wegen $\mathrm{ord}_O\, x = -2$, $\mathrm{ord}_O\, y = -3$ ist

$$1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6(O))$$

Da $\dim \mathcal{L}(6(O)) = 6$ existiert eine nichttriviale Kombination der Null

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

für gewisse $A_1, \dots, A_7 \in k$, nicht alle 0. Die Systeme

$$\{1, x, y, x^2, xy, y^2\}$$
$$\{1, x, y, x^2, xy, x^3\}$$

sind beide linear unabhängig, es muss also $A_6 A_7 \neq 0$ gelten. Ein Variablenwechsel

$$x \mapsto -A_6 A_7 x$$
$$y \mapsto -A_6 A_7^2 y$$

gefolgt von einer Division der Gleichung durch $A_6^3 A_7^4 \neq 0$ führt zu einer Weierstraß-Gleichung in x und y. Die Bilder unter

$$\phi = [x, y, 1] \to \mathbb{P}^2$$

erfüllen die oben konstruierte Weierstraß-Gleichung und liegen daher auf der durch diese gegebenen Kurve $C \subset \mathbb{P}^2$. ϕ ist als nichtkonstante rationale Abbildung von Kurven ein Morphismus und surjektiv. Da y in O höhere Polordnung hat, als x, ist $\phi(O) = (0 : 1 : 0)$.
Es ist noch zu zeigen, dass ϕ ein Isomorphismus ist. Wir gehen in zwei Schritten vor:

(i) $\deg \phi = 1$
(ii) C ist glatt

Dann ist ϕ als Morphismus glatter Kurven vom Grad 1 ein Isomorphismus.
(i). Wegen $\phi^* K(C) = K(x, y)$ ist zu zeigen, dass

$$[K(E) : K(x, y)] = 1.$$

Sei $\psi = [x, 1] \colon E \to \mathbb{P}^1$. Da x nur in O einen Pol hat, ist $\psi^{-1}(\{(1 : 0)\}) = \{O\}$. Wir wollen nun den Verzweigungsgrad von ψ in O bestimmen. Sei $s \in K(E)$ ein uniformisierender Parameter in O. $t = Y/X \in K(\mathbb{P}^1)$ ist uniformisierender Parameter in $(1 : 0)$. Wegen $\operatorname{ord}_O x = -2$ hat ψ in einer Umgebung von O die Gestalt $P \mapsto ((s^2 x)(P) : s^2(P))$. Man erhält

$$e_\psi(O) = \operatorname{ord}_O \psi^*(t) = \operatorname{ord}_O \frac{s^2}{s^2 x} = 2.$$

Damit gilt

$$\deg \phi = \sum_{P \in \phi^{-1}(\{(1:0\})} e_\phi(P) = 2,$$

also wegen $\phi^* K(C) = K(x)$

$$[K(E) : K(x)] = 2.$$

Analog verfährt man mit y und erhält $[K(E) : K(y)] = 3$. Es ergibt sich $[K(E) : K(x, y)] \mid 2, 3$, d.h.

$$[K(E) : K(x, y)] = 1.$$

(ii). Angenommen, C wäre singulär. Dann existierte $\theta : C \to \mathbb{P}^1$, eine rationale Abbildung vom Grad 1 (siehe [4, III. 1.6]). Die Komposition $\theta \circ \phi : E \to \mathbb{P}^1$ wäre dann eine rationale Abbildung Abbildung glatter Kurven vom Grad 1, also ein Isomorphismus. $E \cong \mathbb{P}^1$ steht aber im Widerspruch zu

$$\text{Geschlecht}(E) = 1 \neq 0 = \text{Geschlecht}(\mathbb{P}^1).$$

□

Definition 3.3. $x, y \in k(E)$ wie in 3.2 heißen *Weierstraß-Koordinaten.*

Um die verschiedenen Weierstraß-Koordinaten einer elliptischen Kurve zu klassifizieren, wird eine kurze Rechnung benötigt:

Lemma 3.4. *Sei $C \subset \mathbb{P}^2$ eine nichtsinguläre, durch eine Weierstraß-Gleichung gegebene Kurve, $O = (0 : 1 : 0)$. Dann gilt*

$$\operatorname{ord}_O X/Z = -2$$
$$\operatorname{ord}_O Y/Z = -3.$$

Beweis. Die homogene Weierstraß-Gleichung hat die Form

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

Der Punkt O liegt im affinen Bereich $Y \neq 0$, es bietet sich also Dehomogenisierung nach Y an. Umstellen dieser Gleichung nach Z ergibt

$$Z = X^3 - a_2X^2Z + a_4XZ^2 + a_6Z^3 - a_1XZ - a_3Z^2.$$

Der affine Punkt $(0,0)$ in affinen Koordinaten entspricht dem projektiven Punkt O.
Das Ideal $M_{(0,0)} \subset k[X,Z]$ der in $(0,0)$ verschwindenden Polynome wird von X, Z erzeugt. Aus obiger Gleichung ließt man ab, dass $\operatorname{ord}_{(0,0)} Z \geqslant 2$ gilt, da sich Z als Summe von Elementen aus $M^2_{(0,0)}$ schreiben lässt. Aber dann hat jeder der Summanden auf der rechten Seite sogar eine dreifache Nullstelle in $(0,0)$, also auch Z. Da C nichtsingulär ist, ist eine der das Verschwindungsideal $M_{(0,0)}$ erzeugenden Funktionen X, Z ein uniformisierender Parameter in $(0,0)$ mit Ordnung 1. Es muss also $\operatorname{ord}_{(0,0)} X = 1$ gelten. Die Annahme $\operatorname{ord}_{(0,0)} Z > 3$ führt dann durch Umstellen der Weierstraß-Gleichung nach X^3 sofort zum Widerspruch. Man erhält

$$\operatorname{ord}_{(0,0)} X/Z = -2$$
$$\operatorname{ord}_{(0,0)} 1/Z = -3$$

und diese Funktionen entsprechen den projektiven Funktionen X/Z und Y/Z. □

Satz 3.5. *Seien (x_1, y_1), (x_2, y_2) zwei Paare von Weierstraß-Koordinaten. Dann existieren $u, r, s, t \in k, u \neq 0$ so, dass*

$$x_1 = u^2x_2 + r$$
$$y_1 = u^3y_2 + su^2x_2 + t.$$

Beweis. Da die Abbildungen $[x_i, y_i, 1]$ Isomorphismen sind, gilt

$$\operatorname{ord}_O x_i = \operatorname{ord}_{(0:1:0)} X/Z = -2$$
$$\operatorname{ord}_O y_i = \operatorname{ord}_{(0:1:0)} Y/Z = -3.$$

$\{1, x_i\}$ bildet also jeweils eine Basis von $\mathcal{L}(2(O))$ und analog $\{1, x_i, y_i\}$ eine Basis von $\mathcal{L}(3(O))$. Man findet daher Koeffizienten $v, w, r, s', t \in k, v, w \neq 0$ so, dass

$$x_1 = vx_2 + r$$
$$y_1 = wy_2 + s'x_2 + t.$$

Einsetzen in die Weierstraß-Gleichung, die x_1, y_1 erfüllen, ergibt eine kubische Gleichung C in x_2, y_2. Da x_2, y_2 selbst bereits eine Weierstraß-Gleichung erfüllen, erfüllen die Bilder unter $[x_2, y_2, 1]$ beide Gleichungen, liegen also im Schnitt dieser elliptischen Kurve und C. Unendlichen Schnitt haben Kurven nur, wenn sie eine gemeinsame Komponente haben, C muss daher ein Vielfaches der (irreduziblen) Weierstraß-Gleichung sein. Man erhält $v^3 = w^2$, da die Koeffizienten von Y^2 und X^3 einer Weierstraß-Gleichung identisch 1 sind. Setzt man $u = w/v$, $s = s'/u^2$, haben die Gleichungen die gewünschte Form. □

Die Beschreibung elliptischer Kurven durch Weierstraß-Gleichungen wollen wir mit einer einfachen Folgerungen vorheriger Vorträge abschließen, die besagt, dass auch umgekehrt nichtsinguläre Weierstraß-Gleichungen elliptische Kurven sind.

Satz 3.6. *Sei C eine nichtsinguläre Kurve über k, gegeben durch eine Weierstraß-Gleichung. Dann ist $(C, (0:1:0))$ eine elliptische Kurve.*

Beweis. Das invariante Differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

erfüllt $\operatorname{div}\omega = 0$ ([4, III. 1.5]). Nach dem Satz von Riemann-Roch gilt damit

$$2\,\text{Geschlecht}(C) - 2 = \deg \operatorname{div}\omega = 0,$$

also $\text{Geschlecht}(C) = 1$. □

Im Folgenden kann davon ausgegangen werden, dass die Punkte der elliptischen Kurve vermöge der geometrischen Addition von Punkten die Struktur einer abeslchen Gruppe tragen. Wir werden diese Gruppenoperation nun eingehender untersuchen und die eingangs erwähnte Isomorphie mit der Picard-Gruppe konstruieren.

Lemma 3.7. *Seien $P, Q \in E$. Dann gilt*

$$(P) \sim (Q) \Leftrightarrow P = Q.$$

Beweis. Gelte $(P) \sim (Q)$, d.h.

$$(P) - (Q) = \operatorname{div} f$$

für ein gewisses $f \in K(E)$. Dann ist $f \in \mathcal{L}((Q))$. Da $1 \in \mathcal{L}((Q))$ und $\dim \mathcal{L}((Q)) = 1$ ist, gilt $f \in K$, also $\operatorname{div} f = 0$ und damit $P = Q$. □

Satz 3.8. *Die Funktion*

$$\kappa\colon \begin{cases} E \to \operatorname{Pic}^0(E) \\ P \mapsto \overline{(P) - (O)} \end{cases}$$

ist ein Isomorphismus abelscher Gruppen.

Beweis. κ ist surjektiv. Sei $D \in \operatorname{Div}^0(E)$. Nach dem Satz von Riemann-Roch ist der Vektorraum

$$\mathcal{L}(D + (O)) = \langle f \rangle$$

erzeugt von einem Element $f \in K(E)$. Per Definition ist dann $\operatorname{div} f \geqslant -D - (O)$, also

$$0 = \deg \operatorname{div} f \geqslant \deg -D - (O) = -1.$$

Dies ist nur möglich, falls

$$\operatorname{div} f = -D - (O) + P$$

für ein gewisses $P \in E$, d.h.

$$D \sim (P) - (O).$$

κ ist injektiv. Für $P, Q \in E$ gilt

$$\begin{aligned} & \kappa(P) = \kappa(Q) \\ \Leftrightarrow\ & (P) - (O) \sim (Q) - (O) \\ \Leftrightarrow\ & (P) \sim (Q) \\ \Leftrightarrow\ & P = Q \end{aligned}$$

nach 3.7.

κ ist ein Gruppenhomomorphismus. Seien wieder $P, Q \in E$. Sei die Gerade durch P und Q durch $f \in K[X, Y, Z]$ gegeben und R ihr dritter Schnittpunkt mit E; die Gerade durch R und O sei durch $g \in K[X, Y, Z]$ gegeben. Der Punkt $P + Q$ ist dann der dritte Schnittpunkt dieser Geraden mit E. Man erhält

$$\begin{aligned} \operatorname{div} f &= (P) + (Q) + (R) \\ \operatorname{div} g &= (R) + (O) + (P + Q) \end{aligned}$$

und damit

$$(P) + (Q) \sim (P + Q) + (O),$$

also

$$(P) - (O) + (Q) - (O) \sim (P + Q) - (O),$$

was

$$\kappa(P) + \kappa(Q) = \kappa(P + Q)$$

zur Folge hat. □

Satz 3.9. *Die kanonische Abbildung*

$$\operatorname{Div}_k^0 \mapsto \operatorname{Pic}_k^0(E)$$

ist surjektiv. κ aus 3.8 beschränkt sich zu

$$E(k) \xrightarrow{\sim} \operatorname{Pic}_k^0(E).$$

Beweis. Wir zeigen zunächst die Aussage über κ. Wegen $O \in E(k)$ ist $\kappa(E(k)) \subseteq \mathrm{Pic}_k^0(E)$. Sei $\overline{D} \in Pic_k^0(E)$. Dann ist für ein $P \in E$

$$\overline{D} = \kappa(P) = \overline{(P) - (O)}.$$

Nach Definition ist $\overline{D}$ unter Galoisoperation invariant. Für beliebiges $\sigma \in \mathrm{Gal}(K|k)$ ist also unter Beachtung von $O \in E(k)$

$$\begin{aligned}\overline{D} &= \overline{(P) - (O)} \\ &= \overline{(P^\sigma) - (O)}.\end{aligned}$$

Man erhält $(P) \sim (P^\sigma)$, nach 3.7 $P = P^\sigma \in E(k)$ und damit

$$\overline{D} = \overline{(P) - (O)} \in \kappa(E(k)).$$

Wegen $O \in E(k)$ folgt nun unmittelbar auch die Surjektivität der Abbildung $\mathrm{Div}_k^0 \to \mathrm{Pic}_k^0$. □

Korollar 3.10. *Die Sequenz*

$$1 \to k(E)^\times \to \mathrm{Div}_k^0(E) \to \mathrm{Pic}_k^0(E) \to 0$$

ist exakt. □

Um zu zeigen, dass eine elliptische Kurve ihre eigene Jakobische ist, muss nur noch bewiesen werden, dass die Addition von Punkten der elliptische Kurve ein Morphismus $E \times E \to E$ ist. Mit $E \times E$ ist hier das Produkt in der Kategorie der Varietäten über k gemeint. Dieses Produkt lässt sich für nicht algebraisch abgeschlossene Körper in der klassischen Sprache nur schwer formulieren. Wir zeigen das Resultat daher nur für den algebraischen Abschluss K. In der Kategorie der Varietäten über K lässt sich das Produkt $E \times E$ über die Segre-Einbettung als Menge mit dem kartesischen Produkt der einzelnen Trägermengen identifizieren.

Satz 3.11. *Die Abbildungen*

$$(+)\colon \begin{cases} E \times_K E \to E \\ (P, Q) \mapsto P + Q \end{cases}$$

$$(-)\colon \begin{cases} E \to E \\ P \mapsto -P \end{cases}$$

$$(0)\colon \begin{cases} \mathbb{A}^0 \to E \\ 0 \mapsto O \end{cases}$$

sind Morphismen von Varietäten. E wird vermöge dieser Abbildungen zum Gruppenobjekt in der Kategorie der Varietäten über K.

Beweis. Da jede elliptische Kurve zu einer durch eine Weierstraß-Gleichung gegebenen elliptischen Kurve isomorph ist, genügt es, die Behauptung für solche Kurven zu zeigen. Im letzten Vortrag wurden in diesem Fall explizite Formeln zur Berechnung der Summe und des Inversen zweier Punkte bestimmt (siehe auch [4, III. 2.3]). Durch diese polynomiellen Gleichungen definierte Abbildungen sind somit unmittelbar rational. Es ist zu zeigen, dass sie tatsächlich überall definiert sind. [4, II. Th. 2.3], das garantiert, dass rationale Abbildungen zwischen Kurven sogar Morphismen sind, ist für die Addition $(+)$ nicht anwendbar, da $E \times E$ eine Fläche ist. Trotzdem kann dieses Theorem genutzt werden, um explizite Rechnungen zu vermeiden.

Wir beginnen mit $(-)$. Für $P = (x : y : 1) \neq O$ ist $-P$ gegeben durch

$$-P = (x : -y - a_1 x - a_3 : 1)$$

Eine entsprechend definierte Abbildung ist überall außer eventuell in O definiert, also rational und damit doch in O definiert.

Analog zeigt man, dass für festes $Q \in E$ die Abbildung

$$\tau_Q : \begin{cases} E \to E \\ P \mapsto P + Q \end{cases}$$

ein Morphismus ist. Die Abbildung $(+)$ lässt sich auf

$$E \times E - \{(P, O), (O, P), (P, P), (P, -P) \mid P \in E\}$$

als Morphismus schreiben, wie man aus den expliziten Additionsformeln entnimmt. Um zu zeigen, dass $(+)$ in einem beliebig gewählten Punkt definiert ist, schreibt man für gewisse $Q_1, Q_2 \in E$

$$(+) = \tau_{-Q_1} \circ \tau_{-Q_2} \circ (+) \circ (\tau_{Q_1} \times \tau_{Q_2})$$

Dadurch werden eventuell undefinierte Stellen „verschoben“, sodass $(+)$ auch auf

$$E \times E - \{(P - Q_1, -Q_2), (-Q_1, P - Q_2), (P - Q_1, P - Q_2), (P - Q_1, -P - Q_2) \mid P \in E\}$$

definiert ist. Für jeden Punkt $(P_1, P_2) \in E \times E$ lassen sich offenbar $Q_1, Q_2 \in E$ (fast beliebig) so wählen, dass obiges Verschiebungsargument auch die Definiertheit von $(+)$ in (P_1, P_2) liefert. □

Literatur

[1] U. Görtz und T. Wedhorn. *Algebraic Geometry 1*. 1. Aufl. Vieweg+Teubner, 2010.
[2] R. Hartshorne. *Algebraic Geometry*. 1. Aufl. Springer, 1977.
[3] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. 1. Aufl. Oxford University Press, 2002.
[4] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 2. Aufl. Springer, 2009.