1 Weierstrass-Gleichungen

Es bezeichne K einen Körper und $\overline{K}$ seinen algebraischen Abschluss.

Definition 1: *Eine Weierstrass-Gleichung ist eine Gleichung der Form*

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

Eine solche Gleichung enthält genau einen Punkt der unendlich fernen Geraden $Z = 0$, nämlich $\mathcal{O} = [0 : 1 : 0]$. Wir betrachten die dehomogenisierte Gleichung mit $x = X/Z$ und $y = Y/Z$:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Für den Rest der Ausarbeitung bezeichne $f(x, y) = y^2+a_1xy+a_3y-(x^3+a_2x^2+a_4x+a_6)$ das Polynom, das diese Gleichung liefert. Wir definierten ferner die folgenden Größen

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= \frac{c_4^3}{\Delta}, \text{ falls } \Delta \neq 0,\\
\omega &= \frac{\mathrm{d}x}{(2y + a_1x + a_3)} = \frac{\mathrm{d}y}{(3x^2 + 2a_2x + a_4 - a_1y}.
\end{aligned}$$

Definition 2: *Wir nennen Δ die Diskrimante, j die j-Invariante und ω das invariante Differential der Weierstrass-Gleichung.*

Falls $\mathrm{char}(K) \neq 2$, liefert die Variablentransformation $y \mapsto \frac{1}{2}(y-a_1x-a_3)$ die einfachere Gleichung

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Mit wohlbekannten Formeln lässt sich überprüfen, dass die Diskriminante des Polynoms auf der rechten Seite der Gleichung gerade $\frac{1}{16}\Delta$ ist. Falls zusätzlich $\mathrm{char}(K) \neq 3$, so können wir die Gleichung via $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ weiter vereinfachen zu

$$y^2 = x^3 - 27c_4x - 54c_6.$$

2 Singuläre Punkte

Es sei E eine Kurve, die durch eine Weierstass-Gleichung gegeben ist. Wir wollen uns zunächst mit singulären Punkten auf E beschäftigen. Ist F ein Polynom, das die homogene Weierstrass-Gleichung liefert, so ist wegen $\frac{\partial F}{\partial Z}(\mathcal{O}) = 1$ der Punkt $\mathcal{O}$ im Unendlichen

niemals singulär ist. Wir können uns daher auf den affinen Teil der Kurve beschränken, den man durch Dehomogenisierung nach Z erhält. Sei also $P = (x_0, y_0)$ ein Punkt auf E, der singulär ist, d.h.

$$\frac{\partial f}{\partial x}(P) = 0 = \frac{\partial f}{\partial y}(P).$$

Dann hat die formale Taylor-Entwicklung von f um P die Form

$$f(x,y) = [(y-y_0) - \alpha(x-x_0)][(y-y_0) - \beta(x-x_0)] - (x-x_0)^3$$

für gewisse $\alpha, \beta \in \overline{K}$.

Definition 3: *P heißt Doppelpunkt, falls $\alpha \neq \beta$. In diesem Fall sind*

$$y - y_0 = \alpha(x-x_0), \qquad\qquad y - y_0 = \beta(x-x_0)$$

die Tangenten an P. Der Punkt P heißt Spitze, falls $\alpha = \beta$ und in diesen Fall ist

$$y - y_0 = \beta(x-x_0)$$

die Tangente an P.

Proposition 4: *(i) E ist singulär $\Leftrightarrow \Delta = 0$.*

(ii) E hat einen Doppelpunkt $\Leftrightarrow \Delta = 0$ und $c_4 \neq 0$.

(iii) E hat eine Spitze $\Leftrightarrow \Delta = 0 = c_4$.

(iv) E hat höchstens eine Singularität.

Beweis: Sei $P \in E$ ein singulärer Punkt. Da $\mathcal{O}$ nicht singulär ist, hat P die Form $P = (x_0, y_0)$. Die Substitution $x = x' + x_0$, $y = y' + y_0$ lässt Δ und c_4 invariant. Somit können wir ohne Einschränkung $P = (0,0)$ annehmen. Damit folgt

$$a_6 = f(0,0) = 0, \qquad a_4 = \frac{\partial f}{\partial x}(0,0) = 0, \qquad a_3 = \frac{\partial f}{\partial y}(0,0) = 0,$$

sodass die Gleichung die einfachere Form

$$E\colon y^2 + a_1xy - a_2x^2 - x^3 = 0$$

erhält. Die zugehörigen Größen sind dann $c_4 = (a_1^2 + 4a_2)^2$ und $\Delta = 0$. per Definition hat E bei $(0,0)$ genau dann einen Doppelpunkt, wenn $y^2 + a_1xy - a_3x^2$ als Polynom in y betrachtet verschiedene Nullstellen hat. Dies ist genau dann der Fall, wenn $a_1 + 4a_2 \neq 0$. Um den Beweis zu vervollständigen, muss nun noch gezeigt werden, dass $\Delta \neq 0$, falls E nicht singulär ist, sowie dass E höchsten eine Singularität hat. Der Einfachheit halber nehmen wir hierzu $\mathrm{char}(K) \neq 2$ an. Dann hat E eine Gleichung der Form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Ein Punkt $P = (x_0, y_0)$ auf E ist genau dann singulär, wenn

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0,$$

d.h. genau dann wenn $P = (x_0, 0)$, wobei x_0 eine doppelte Nullstelle von $4x^3 + b_2x^2 + 2b_4x + b_6$ ist. Die Determinante dieses Polynoms ist $\frac{1}{16}\Delta$ und damit hat es eine doppelte Nullstelle genau dann wenn $\Delta \neq 0$. Da es höchstens eine doppelte Nullstelle geben kann, hat E außerdem höchstens eine Singularität. ∎

Proposition 5: *Ist E singulär, so ist E birational äquivalent zu $\mathbb{P}^1_K$.*

Beweis: Ohne Einschränkung ist der singuläre Punkt $(0, 0)$. Genau wie im vorangegangenen Beweis erhält man

$$E\colon y^2 + a_1xy = x^3 + a_2x^2.$$

Damit hat

$$E \dashrightarrow \mathbb{P}^1_K,\ (x, y) \mapsto [x : y]$$

als Inverse

$$\mathbb{P}^1_K \dashrightarrow E,\ [1 : t] \mapsto (t^2 + a_1t - a_2, t^2 + a_1t^2 - a_2t).$$

3 j-Invariante und invariantes Differential

Proposition 6: *(i) Zwei durch Weierstrass-Gleichungen gegebene Kurven E und E' sind genau dann isomorph, wenn sie die gleiche j-Invariante haben.*

(ii) Zu $j_0 \in \overline{K}$ gibt es eine nicht singuläre Weierstrassgleichung mit j-Invariante j_0.

Beweis: (i) Sei E isomorph zu E'. Die Gleichung stehen dann in Verbindung durch einen Variablenwechsel der Form

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

mit $u, r, s, t \in \overline{K}, u \neq 0$ (diese Tatsache wird in Vortrag 3 bewiesen). Man errechnet hiermit sofort $j(E) = j(E')$.

Gelte andersherum, dass E und E' die gleiche j-Invariante haben. Um zu folgern, dass $E \cong E'$ gilt, nehmen wir (wieder der Einfachheit halber) an, dass $\mathrm{char}(K) \neq 2, 3$. Die Kurven haben dann Gleichungen der Form

$$E\colon y^2 = x^3 + Ax + B,$$
$$E'\colon (y')^2 = (x')^3 + A'x' + B'.$$

Da die j-Invarianten gleich sind, erhält man

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

und hieraus durch Umformung $A^3B'^2 = A'^3B^2$. Wir können hiermit einen Isomorphismus der Form $(x, y) \mapsto (u^2x, u^3y)$ finden. Dazu machen wir eine Fallunterscheidung.

1. Fall: $A = 0$.
   Da $\Delta \neq 0$ folgt, dass $B \neq 0$. Damit muss $A' = 0$ gelten und analog $B' \neq 0$. Wir wählen $u = \sqrt[6]{\frac{B}{B'}}$.

2. Fall: $B = 0$.
   Genau wie in Fall 1 erhält man $A, A' \neq 0$ und wir können $u = \sqrt[4]{\frac{A}{A'}}$.

3. Fall $AB \neq 0$.
   Dann muss auch $A'B' \neq 0$ gelten und wir wählen $u = \sqrt[6]{\frac{B}{B'}} = \sqrt[4]{\frac{A}{A'}}$.

(ii) Sei zunächst $j_0 \neq 0, 1728$. Dann hat die Kurve

$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

die zugehörigen Größen $\Delta = \frac{j_0^2}{(j_0-1728)^3} \neq 0$ sowie $j = j_0$. Für die Ausnahmen betrachte

$$y^2 + y = x^3,\ \Delta = -27,\ j = 0,$$
$$y^2 = x^3 + x,\ \Delta = -64,\ j = 1728.$$

Hier beachte man, dass im Fall $\mathrm{char}(K) \in \{2, 3\}$ wenigstens eine der beiden Kurven nicht-singulär ist. Dies genügt dann bereits, da in diesen Charakteristiken $0 = 1728$ gilt. ∎

Proposition 7: *Ist E nicht singulär, so ist das invariante Differential holomorph und nullstellenfrei, d.h.* $\mathrm{div}(\omega) = 0$.

Beweis: Sei $P = (x_0, y_0)$ ein Punkt auf E. Dann gilt

$$\omega = \frac{\mathrm{d}(x - x_0)}{\partial f/\partial y} = -\frac{\mathrm{d}(y - y_0)}{\partial f/\partial x}$$

und damit ist P kein Pol von ω, da sonst $\frac{\partial f}{\partial y}(P) = 0 = \frac{\partial f}{\partial x}(P)$. Da die Gerade $x - x_0$ die Kurve in $\mathcal{O}$ schneidet, folgt mit dem Satz von Bézout $\mathrm{ord}_P(x - x_0) \leq 2$ mit Gleichheit genau dann, wenn $f(x_0, y)$ eine doppelte Nullstelle hat. Das heißt es gilt $\mathrm{ord}_P(x - x_0) = 1$ oder aber $\mathrm{ord}_P(x - x_0) = 2$ und $\frac{\partial f}{\partial y}(P) = 0$. Mit den Rechenregeln für Differentiale (vgl. Vortrag 1) können wir in beiden Fällen berechnen:

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(\frac{\partial f}{\partial y}) - 1 = 0.$$

Es verbleibt zu zeigen, dass $P = \mathcal{O}$ weder Pol noch Nulstelle von ω ist. Sei t ein uniformisierender Parameter im lokalen Ring von $\mathcal{O}$. Die Weierstrassgleichung liefert $\mathrm{ord}_P(x) = 2$ und $\mathrm{ord}(y) = 3$, d.h. $x = t^{-2}f$, $y = t^{-3}g$, wobei f, g Funktionen mit $f(\mathcal{O}) \neq 0, \infty \neq g(\mathcal{O})$. Man erhält

$$\omega = \frac{\mathrm{d}x}{(2y + a_1x + a_3)} = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}\mathrm{d}t,$$

wobei $f' = \frac{\mathrm{d}f}{\mathrm{d}t}$. Da f regulär in $\mathcal{O}$ ist, gilt dies nach Vortrag 1 auch für f'. Falls $\mathrm{char}(K) \neq 2$ erhält man also, dass ω bei $\mathcal{O}$ weder einen Pol, noch eine Nullstelle hat. Falls $\mathrm{char}(K) = 2$, so betrachet man die Darstellung $\omega = \frac{\mathrm{d}y}{(3x^2+2a_2x+a_4-a_1y)}$ und folgert das Gewünschte mit einer analogen Rechnung. ∎

Proposition 8: *Die Charakteristik von K sei nicht 2.*

(i) *E ist isomorph zu einer Kurve der Form*

$$E_\lambda \colon y^2 = x(x-1)(x-\lambda)$$

für ein $\lambda \in \overline{K} \setminus \{0,1\}$.

(ii) $j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)3}{\lambda^2(\lambda-1)^2}$.

(iii) *Die Abbildung*

$$\varphi \colon \overline{K} \setminus \{0,1\} \to \overline{K},\ \lambda \mapsto j(E_\lambda)$$

ist surjektiv und es gilt

$$\#\varphi^{-1}(j) = \begin{cases} 6, & \text{falls } j \in \overline{K} \setminus \{0, 1728\} \\ 2, & \text{falls } j = 0, \mathrm{char}(K) \neq 3 \\ 3, & \text{falls } j = 1728, \mathrm{char}(K) \neq 3 \\ 1, & \text{falls } \mathrm{char}(K) = 3, j = 0 = 1728. \end{cases}$$

Beweis: (i) Wegen $\mathrm{char}(K) \neq 2$ hat E die Form

$$E \colon y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Nach dem Variablenwechsel $(x, y) \mapsto (x, 2y)$ erhalten wir

$$E \colon y^2 = (x-e_1)(x-e_2)(x-e_3),$$

wobei die e_i die Nullstellen des Polynoms auf der rechten Seite der ursprünglichen Gleichung sind. Da $\Delta \neq 0$, sind die e_i paarweise verschieden. Die Substitution $x = (e_2-e_1)x'$, $y = \sqrt{(e_3-e_1)^3}y'$ liefert dann E_λ mit $\lambda = \frac{e_3-e_1}{e_2-e_1} \in \overline{K} \setminus \{0,1\}$.

(ii) folgt durch Nachrechnen. Zu (iii): Angenommen $j(E_\lambda) = j(E_\mu)$. Dann gilt nach Proposition 6 (i) $E_\lambda \cong E_\mu$, d.h. die Gleichungen stehen über einen Variablenwechsel der Form

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

in Verbindung, wobei $u, r \in \overline{K}, u \neq 0$. Man erhält daraus

$$x(x-1)(x-\mu) = (x + \frac{r}{u^2})(x + \frac{r-1}{u^2})(x + \frac{r-\lambda}{u^2}).$$

Es gibt sechs Arten die linearen Terme einander zuzuordnen und diese ergeben für μ die Werte

$$\mu \in \{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}.$$

Die Abbildung φ ist folglich 6 zu 1, außer falls zwei oder mehr dieser Ausdrücke übereinstimmen. Falls $\lambda \in \{-1, 2, \frac{1}{2}\}$, so ist die Zuordnung 3 zu 1 und diese Werte entsprechen $j = 1728$. Falls $\lambda^2 - \lambda + 1 = 0$, so ist die Zuordnung 2 zu 1 und diese Werte entsprechen $j = 0$. Falls nun $\mathrm{char}(K) = 3$, so stimmen die Werte von λ in den beiden Fällen überein und wir erhalten $\lambda = -1$ als eindeutige Lösung von $j(E_\lambda) = 0 = 1728$. ∎

4 Das Gruppengesetz

Sei E zunächst als nicht singulär vorausgesetzt. Eine Gerade $L \subseteq \mathbb{P}^2_K$ schneidet E nach dem Satz von Bézout (mit Multiplizität) in genau drei Punkten.

Definition 9 (Gruppengesetz auf E): *Seien $P, Q \in E$ und L deren Verbindungsgerade (die Tangente an P, falls $P = Q$). Sei R der dritte Schnittpunkt mit E und L' die Verbindungsgerade von R und $\mathcal{O}$. Dann ist $P + Q$ der dritte Schnittpunkt von L' mit E.*

Proposition 10: *(i) Die Gerade L schneide E in den Punkten P, Q, R. Dann gilt $(P + Q) + R = \mathcal{O}$.*

(ii) Die Verknüpfung $+$ gibt den Punkten von E die Struktur einer abelschen Gruppe mit neutralem Element $\mathcal{O}$.

(iii) Ist E über K definiert, so ist $E(K) = \{(x, y) \in K^2 \mid (x, y) \in E\} \cup \{\mathcal{O}\}$ eine Untergruppe.

Beweis: (i) und (iii) sind klar. Bedenkt man, dass die Tangente an E im Punkt $\mathcal{O}$ diesen mit Multiplizität 3 schneidt, so ist auch klar, dass $P + \mathcal{O} = \mathcal{O}$ für alle Punkte P von E. Ist ferner R der dritte Schnittpunkt der Verbindungsgeraden eines Punktes P mit $\mathcal{O}$, so gilt nach (i)

$$\mathcal{O} = (P + \mathcal{O}) + R = P + R$$

und damit ist $R = -P$. Die Schwierigkeit ist zu zeigen, dass die Verknüpfung $+$ assoziativ ist. Dies wird in Vortrag 3 bewiesen. ∎

Man kann für das Gruppengesetz Formeln herleiten, die $P + Q$ abhängig von den Koordinaten von P und Q angeben. Wir wollen exemplarisch die Formel für $-P$ herleiten. Um den Punkt zu finden gehen wir nach dem soeben geführten Beweis vor. Ist also $P = (x_0, y_0)$ ein Punkte auf E, so ist die Gerade durch P und $\mathcal{O}$ gegeben durch $x - x_0 = 0$. Wir suchen nun den dritten Schnittpunkt dieser Gerade mit E. Das Polynom $f(x_0, y)$ hat die Nullstellen y_0 und y_0', wobei $-P = (x_0, y_0')$. Wir haben also $f(x_0, y) = (y - y_0)(y - y_0')$ und ein Koeffizientenvergleich liefert dann $y_0' = -y_0 - a_1 x_0 - a_3$ woraus sich insgesamt $-P = (x_0, -y_0 - a_1 x_0 - a_3)$ ergibt.

Korollar 11: *Wir nennen eine Funktion $f \in \overline{K}(E) = \overline{K}(x, y)$ gerade, falls $f(P) = f(-P)$ für alle Punkte P von E. Es gilt*

$$f \text{ ist gerade } \Leftrightarrow f \in \overline{K}(x).$$

Beweis: Dass jedes $f \in \overline{K}(x)$ gerade ist, ist aus der Formel für $-P$ direkt ersichtlich. Sei andersherum f gerade. Die Weierstrassgleichung besagt $[\overline{K}(x,y) : \overline{K}(x)] = 2$, d.h. $f(x,y) = g(x) + h(x)y$ für gewisse $g, h \in \overline{K}(x)$. Wir erhalten

$$\begin{aligned} g(x) + h(x)y = f(x,y) &= f((x, -y - a_1x - a_3) \\ &= g(x) - (y + a_1x - a_3)h(x), \end{aligned}$$

was äquivalent ist zu $(2y + a_1x + a_3)h(x) = 0$. Hieraus folgt $h = 0$ oder $2 = a_1 = a_3 = 0$. Letzteres aber würde $\Delta = 0$ implizieren, sodass man $h = 0$ und damit $f = g \in \overline{K}(x)$ erhält. ∎

Bisher haben wir E als nicht-singulär vorausgesetzt. Dennoch treten auch singuläre Weierstrass-Gleichungen natürlich auf.

Beispiel 12: Betrachte die Kurve $E\colon y^2 + x^3 + 17$, definiert über $K = \mathbb{Q}$. Dann hat E Diskriminante $\Delta = 2^4 \cdot 3^3 \cdot 17$ und ist damit nicht-singulär. Betrachtet man nun die Gleichung der Kurve modulo einer Primzahl $p \in \{2, 3, 17\}$, so ist die resultierende Gleichung noch immer eine Weierstrass-Gleichung aber die Diskriminante verschwindet, sodass die davon gegebene Kurve singulär wird.

Wir würden gerne auch die Struktur der Lösungsmenge von singulären Weierstrass-Gleichungen genauer kennen. Es stellt sich heraus, dass wir das Gruppengesetz von nicht-singulären Kurven dieser Art übernehmen können und dass die Gruppenstruktur in diesem Fall sogar recht einfach ist.

Definition 13: *Sei E nun möglicherweise singulär. Der nicht-singuläre Teil E_{ns} von E ist die Menge der nicht-singulären Punkte von E.*

Proposition 14: *Die Kurve E sei durch eine Weierstrass-Gleichung gegeben und habe den singulären Punkt $S = (x_0, y_0)$. Dann ist E_{ns} mit der bereits definierten Verknüpfung $+$ eine abelsche Gruppe und es gilt:*

(i) Ist S ein Doppelpunkt und sind $y = \alpha_1 x + \beta_1$ und $y = \alpha_2 x + \beta_2$ die verschiedenen Tangenten an E in S, so ist

$$E_{ns} \to \overline{K}^*,\ (x,y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

ein Isomorphismus von abelschen Gruppen.

(ii) Ist S eine Spitze mit Tangente $y = \alpha x + \beta$ an E in S, so ist

$$E_{ns} \to \overline{K}^+,\ (x,y) \to \frac{x - x_0}{y - \alpha x - \beta}$$

ein Isomorphismus von abelschen Gruppen.

Beweis: Beachte zunächst, dass der Punkt $\mathcal{O}$ in E_{ns} liegt. Dass E_{ns} unter der Verknüpfung + sowie unter Inversenbildung abgeschlossen ist, folgt aus dem Satz von Bézout. In der Tat kann die Verbindungsgerade von zwei nicht-singulären Punkten als dritten Schnittpunkt nicht den singulären Punkt S haben, da sonst die Summe der Schnittmultiplizitäten 3 übersteigen würde. Da nun die Verknüpfung auf E_{ns} sowie die involvierten Abbildungen durch Geraden definiert sind, genügt es die Aussage der Proposition nach einem linearen Variablenwechsel zu zeigen. Wir können also ohne Einschränkung $S = (0, 0)$ annehmen und erhalten wie zuvor bereits

$$E\colon y^2 + a_1xy = x^3 + a_2x^2.$$

Sei $s \in \overline{K}$ ein Element, das die Relation $s^2 + a_1s - a_2 = 0$ erfüllt. Dann liefert der Variablenwechsel $(x, y) \mapsto (x, y + sx)$ die Gleichung (in homogenen Koordinaten)

$$E\colon Y^2Z + AXYZ - X^3 = 0.$$

In dieser Darstellung können wir nun die Tangentengleichungen einfach ablesen.

a) Ist S ein Doppelpunkt, so ist $A \neq 0$ und die Tangenten sind $Y = 0$ und $Y + AX = 0$. Die fragliche Abbildung ist somit

$$E_{ns} \to \overline{K}^*,\ [X, Y, Z] \mapsto 1 + \frac{AX}{Y}.$$

Der Variablenwechsel

$$X = A^2(X' - Y'), \qquad Y = A^3Y', \qquad Z = Z'$$

liefert die weiter vereinfachte Gleichung

$$E\colon XYZ - (X - Y)^3.$$

Wir wollen nun die Singularität S in die Unendlichkeit schieben und dehomogenisieren die Gleichung daher nach Y. Mit $x = X/Y$ und $z = Z/Y$ erhalten wir dann

$$E\colon xz - (x - 1)^3 = 0$$

und die fragliche Abbildung wird zu

$$E_{ns} \to \overline{K}^*,\ (x, z) \mapsto x.$$

Diese ist offenbar eine Bijektion mit Umkehrabbildung $t \mapsto (t, (t-1)^3/t)$. Zu überprüfen bleibt, dass die Abbildung mit der Gruppenstruktur verträglich ist. Sei L ein Gerade, die E nicht in S schneidet. Seien $(x_i, z_i), i = 1, 2, 3$ die Schnittpunkte mit E. Die Gerade L hat die Form $z = ax + b$, d.h. die x_i sind die Nullstellen von

$$x(ax + b) - (x - 1)^3 = 0.$$

Ein Vergleich mit dem konstanten Koeffizienten liefert $x_1x_2x_3 = 1$. Diese Gleichung besagt gerade die Verträglichkeit der Abbildung mit der Gruppenstruktur (vgl. Proposition 10 (i)).

(ii) Sei nun S eine Spitze. Dann ist $A = 0$ und die Tangete an E in S ist $Y = 0$. Wir müssen also die Abbildung

$$E_{ns} \to \overline{K}^+,\ [X, Y, Z] \mapsto \frac{X}{Y}$$

betrachten. Wir dehomogenisieren wieder nach Y und erhalten

$$E\colon z - x^3 = 0$$

mit zugehöriger Abbildung

$$E_{ns} \to \overline{K}^+,\ (x, z) \mapsto x.$$

Die Umkehrabbildung ist offenbar $t \mapsto (t, t^3)$, sodass wir eine Bijektion haben. Ist $L\colon z = ax + b$ eine Gerade, die mit E die Schnittpunkte $(x_i, z_i), i = 1, 2, 3$ hat, so sind die x_i Nullstellen von

$$(ax + b) - x^3 = 0.$$

Ein Vergleich mit dem (fehlenden) Koeffizienten von x^2 liefert $x_1 + x_2 + x_3 = 0$ und genau wie in (i) folgt hieraus die Verträglichkeit mit der Gruppenstruktur. ∎