Ruprecht-Karls-Universität Heidelberg

Seminar

Einführung in die Theorie der elliptischen Kurven

Vortrag Gruppengesetz und Weierstraß-Gleichungen

Christian Theisen

8. November 2012

Betreuer:
Prof. Dr. Kay Wingberg
Katharina Hübner

In diesem Seminar geht es um elliptische Kurven; das sind projektive, glatte Kurven vom Geschlecht 1. Man kann zeigen, dass elliptische Kurven isomorph zu glatten projektiven Kurven sind, die durch sogenannte Weierstraß-Gleichungen definiert werden. Dieser Vortrag behandelt projektive Kurven, die durch solche Weierstraß-Gleichungen definiert sind, und die Tatsache, dass die glatten Punkte auf solchen Kurven eine Gruppe bilden.

1 Weierstraß-Gleichungen

Definition 1 (Weierstraß-Gleichung) *Sei K ein Körper. Eine Gleichung der Form*

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

mit Koeffizienten $a_1, \ldots, a_6 \in K$ heißt Weierstraß-Gleichung über K.

Bemerkung 2 *Sei E eine projektive Kurve, die durch eine Weierstraß-Gleichung*

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

definiert ist. Setzt man die Gleichung der Geraden $Z = 0$ in die Weierstraß-Gleichung ein, dann erhält man $X^3 = 0$. Damit ist $O = [0, 1, 0]$ der einzige Punkt in $E \cap (Z = 0)$ und es gilt $I(O, P \cap (Z = 0)) = 3$.
Die Kurve E ist glatt in O, denn $\frac{\partial(Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2+a_6Z^3)}{\partial Z}(O) = 1 \neq 0.$

Bemerkung 3 *Um die Notation einer Weierstraß-Gleichung zu vereinfachen, verwendet man die inhomogenen Koordinaten $x = X/Z$ und $y = X/Z$. Dies führt auf die Gleichung:*

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

Bei dieser Schreibweise ist zu beachten, dass eine Kurve, die durch eine solche Gleichung definiert ist, zusätzlich den Punkt $O = [0, 1, 0]$ im Unendlichen besitzt nach Bemerkung 2.
Ist $\mathrm{char}(K) \neq 2$*, so kann man die Substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ durchführen und erhält*

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

wobei $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$.
Für den Fall $\mathrm{char}(K) \neq 2, 3$ *kann man den x^2 Term durch die Subsitution $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ eliminieren und man erhält:*

$$E : y^2 = x^3 - 27c_4x - 54c_6,$$

wobei $c_4 = b_2^2 - 24b_4$ und $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

Definition 4 *Für eine Weierstraß-Gleichung $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ heißt*

i) $\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ *Diskriminante,*

ii) $j := \frac{c_4^3}{\Delta}$ *j-Invariante für* $\Delta \neq 0$*,*

iii) $\omega := \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$ *heißt invariantes Differential.*

Hierbei sind die Koeffizienten b_2, b_4, b_6, c_4, c_6 wie in der Bemerkung 3 definiert und b_8 durch

$$b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

Bemerkung 5 *Es gilt:* $4b_8 = b_2b_6 - b_4^2$ *und* $1728\Delta = c_4^3 - c_2^6$*. Dies überprüft man durch Nachrechnen.*

Bemerkung 6 *Mit Hilfe der Diskriminante kann man überprüfen, ob eine Kurve, die durch eine Weierstraß-Gleichung gegeben ist, singulär oder glatt ist. Die j-Invariante legt die Isomorphie-Klasse einer elliptischen Kurve fest.*

Bemerkung 7 *Für eine Kurve E, die durch eine Weierstraß-Gleichung definiert sind, gibt es nur zwei Arten von Singularitäten.*

Beweis: Sei $P = (x_0, y_0)$ eine Singularität auf einer Kurve E, die durch $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ definiert ist, d.h.

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

Es ist $\frac{\partial^3 f/\partial x^3}{3!} = -1$ und $\frac{\partial^2 f/\partial y^2}{2!} = 1$. Daher gibt es $\alpha, \beta \in \overline{K}$, sodass die Taylorentwicklung von f in P folgende Form hat:

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

Definition 8 (Knoten, Spitze) *Es gelte die Notation der Bemerkung 7.*

i) Der singuläre Punkt P von E heißt Knoten, falls $\alpha \neq \beta$. Die Geraden

$$y - y_0 = \alpha(x - x_0) \text{ und } y - y_0 = \beta(x - x_0)$$

sind die Tangenten an E in P.

ii) Der singuläre Punkt P von E heißt Spitze, falls $\alpha = \beta$. In diesem Fall ist die Gerade

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

die Tangente an E in P.

Bemerkung 9 *Der einzige Koordinatenwechsel, der den Punkt $O = [0, 1, 0]$ festhält und die Form einer Weierstraß-Gleichung bewahrt, ist*

$$x = u^2x' + r \text{ und } y = u^3y' + u^2sx' + t,$$

wobei $u, r, s, t \in \overline{K}$ und $u \neq 0$.

In der folgenden Tabelle sind die Größen der Weierstraß-Gleichung aufgelistet, die durch den Koordinatenwechsel entsteht.

Satz 10 *Für eine Kurve E, die durch eine Weierstraß-Gleichung gegeben ist, gilt:*

i) E ist glatt $\Leftrightarrow \Delta \neq 0$.

ii) Ist $\Delta = 0$, so besitzt E genau eine Singularität.

iii) E hat einen Knoten $\Leftrightarrow \Delta = 0$ und $c_4 \neq 0$.

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

$ua_1' = a_1 + 2s$
$u^2a_2' = a_2 - sa_1 + 3r - s^2$
$u^3a_3' = a_3 + ra_1 + 2t$
$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2b_2' = b_2 + 12r$
$u^4b_4' = b_4 + rb_2 + 6r^2$
$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$
$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
$u^4c_4' = c_4$
$u^6c_6' = c_6$
$u^{12}\Delta' = \Delta$
$j' = j$
$u^{-1}\omega = \omega$

Tabelle 1: Koordinatenwechselformeln für Weierstraß-Gleichungen

Beweis: i) Sei E gegeben durch eine Weierstraß-Gleichung

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Der Punkt im Unendlichen $O = [0, 1, 0]$ ist ein glatter Punkt von E nach Bemerkung 2. Also muss eine Singularität von E im affinen Teil der Kurve liegen.
"$\Leftarrow$": Sei E eine singuläre Kurve und $P = (x_0, y_0)$ ihr singulärer Punkt. Nach der Bemerkung 9 kann man ohne Einschränkung die Substitution

$$x = x' + x_0 \text{ und } y = y' + y_0$$

durchführen, unter der nach Tabelle 1 Δ und c_4 invariant sind, und damit den singulären Punkt P in $(0, 0)$ verschieben. Dann gilt:

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

Die Weierstraß-Gleichung von E hat also die Form

$$E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0$$

Es ist $b_4 = 0, b_6 = 0, b_8 = 0$ und damit $c_4 = b_2^2 = (a_1^2 + 4a_2)^2$ sowie $\Delta = 0$.
"$\Rightarrow$": Sei E eine glatte Kurve. Um die Rechnung zu vereinfachen, nimmt man $\text{char}(K) \neq 2$ an. Die Behauptung gilt auch für $\text{char}(K) = 2$ (siehe [Si] Appendix A Proposition 1.2). Dann hat die Weierstraß-Gleichung von E die Form

$$E : y^2 = 4x^3 + b^2x^2 + 2b_4x + b_6.$$

E ist genau dann singulär, wenn es einen singulären Punkt $P = (x_0, y_0) \in E$ gibt. Für diesen singulären Punkt P gilt dann:

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

Also ist $P = (x_0, 0)$, wobei x_0 eine doppelte Nullstelle des Polynoms
$g = 4x^3 + b_2x^2 + 2b_4x + b_6$ ist. Wegen $\deg(g) = 3$ hat g höchstens eine doppelte Nullstelle und damit kann E höchstens eine Singularität besitzen. Daraus folgt *ii)*. Die Diskriminante von g ist gleich 16Δ, denn
$16\Delta = -4b_2^2(b_2b_6 - b_4^2) - 16 \cdot 8b_4^3 - 16 \cdot 27b_6^2 + 16 \cdot 9b_2b_4b_6 = \operatorname{disc}(g)$.
Da E als nicht-singulär vorausgesetzt wurde, ist $\operatorname{disc}(g) \neq 0$ und damit $\Delta \neq 0$.
iii), iv) Nach *i)* hat E genau dann eine Singularität P, wenn $\Delta = 0$. Man kann P ohne Einschränkung in $(0, 0)$ verschieben. Diese Singularität P ist genau dann ein Knoten bzw. eine Spitze, wenn der homogene Summand von mininalem Grad von
$f = y^2 + a_1xy - a_2x^2 - x^3$, in diesem Fall $f_2 = y^2 + a_1xy - a_2x^2$, zwei verschiedene bzw. einen Linearfaktor(en) besitzt, d.h. wenn $\operatorname{disc}(f_2) = a_1^2 + 4a_2 = 0$ bzw. $\operatorname{disc}(f_2) \neq 0$. Also ist die Singularität P von E genau dann ein Knoten bzw. eine Spitze, wenn $\Delta = 0$ und $c_4 = (a_1^2 + 4a_2)^2 = 0$ bzw. $c_4 \neq 0$.

Beispiel 11 *Sei* $K = \mathbb{C}$

i) Ein Beispiel für eine glatte elliptische Kurve ist

$$A : y^2 = x^3 + 17.$$

Es ist $\Delta = -124848 \neq 0$ *und* $j = 0$.

ii) Ein Beispiel für eine singuläre Kurve, die durch eine Weierstraß-Gleichung gegeben ist und eine Spitze hat, ist

$$B : y^2 = x^3$$

Die Tangente durch den singulären Punkt $P = (0, 0)$ *ist durch* $y = 0$ *gegeben. Es ist* $\Delta = 0$.

iii) Ein Beispiel für eine singuläre Kurve, die durch eine Weierstraß-Kurve gegeben ist und einen Knoten hat, ist

$$C : y^2 = x^3 + x^2.$$

Die Tangenten durch den singulären Punkt $P = (0, 0)$ *sind gegeben durch* $y = x$ *und* $y = -x$. *Es gilt:* $\Delta = 0$.

Bemerkung 12 *Ist* $\operatorname{char}(K) \neq 2, 3$, *dann haben Weierstraß-Gleichungen nach Bemerkung 3 die Form*

$$y^2 = x^3 + Ax + B \text{ mit } A, B \in K \text{ und}$$
$$\Delta = -16(4A^3 + 27B^2)$$
$$j = -1728\frac{(4A)^3}{\Delta} \text{ für } \Delta \neq 0$$

Der einzige Koordinatenwechsel, der diese Form der Gleichung erhält, ist

$$x = u^2x' \text{ und } y = u^3y'$$

für ein $u \in \overline{K}^*$ *und dann gilt:*

$$u^4A' = A, u^6B' = B, u^{12}\Delta' = \Delta$$

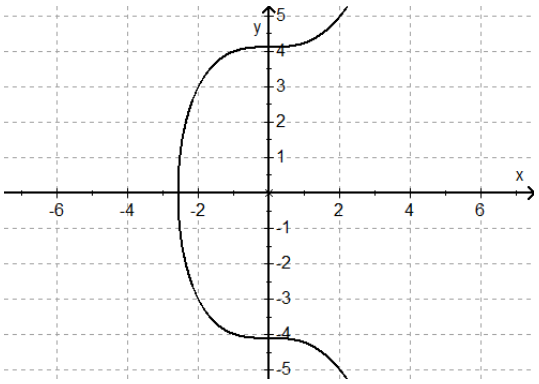

Abbildung 1: $A \cap \mathbb{A}^2_{\mathbb{R}}$

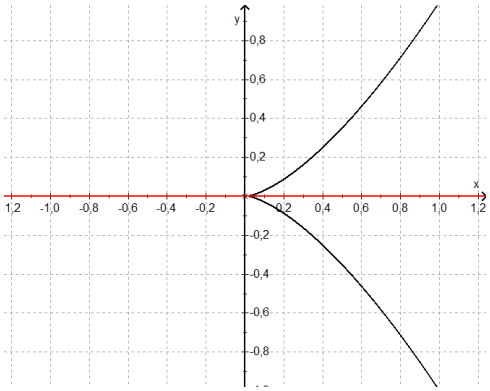

Abbildung 2: $B \cap \mathbb{A}^2_{\mathbb{R}}$

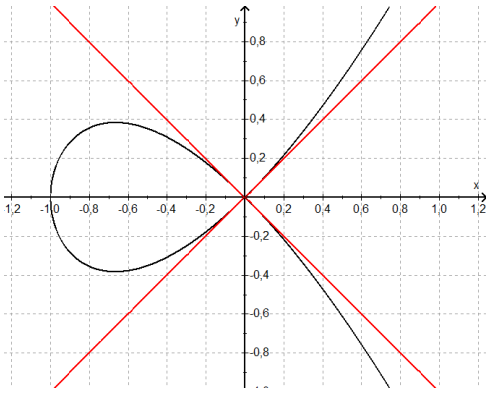

Abbildung 3: $C \cap \mathbb{A}^2_{\mathbb{R}}$

Satz 13 *Zwei elliptische Kurven E und E' sind isomorph über $\overline{K}$ genau dann, wenn sie beide dieselbe j-Invariante besitzen.*

Beweis: Da die Kurven als glatt vorausgesetzt werden, sind die zugehörigen j-Invarianten definiert.
"$\Leftarrow$": Wenn zwei elliptische Kurven isomorph sind, so muss der Isomorphismus ein Koordinatenwechsel sein wie in Bemerkung 9. In Tabelle 1 kann man nun ablesen, dass bei dieser Transformation die j-Invariante invariant ist.
"$\Rightarrow$": Um die Rechnung zu vereinfachen nimmt man an, dass $\mathrm{char}(K) \geq 5$. Die Behauptung gilt aber auch für $\mathrm{char}(K) = 2, 3$ (siehe [Si] Appendix A Proposition 1.2). Seien

$$E : y^2 = x^3 + Ax + B \text{ und } E' : y'^2 = x'^3 + A'x' + B'$$

zwei elliptische Kurven mit derselben j-Invariante. Dann gilt nach Bemerkung 12:

$$j(E) = j(E') \Rightarrow \frac{1728(4A)^3}{16(4A^3 + 27B^2)} = \frac{1728(4A')^3}{16(4A'^3 + 27B'^2)} \Rightarrow \frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$
$$\Rightarrow (4A)^3(4A'^3 + 27B'^2) = (4A')^3(4A^3 + 27B^2) \Rightarrow A^3B'^2 = A'^3B^2$$

Nach Bemerkung 12 muss der Isomorphismus zwischen E und E' von der Form

$$x = u^2x' \text{ und } y = u^3y' \text{ mit } u \in \overline{K}^*$$

sein. Für die folgenden drei Fälle wird ein solcher konstruiert:

Fall 1 $A = 0$ und damit $j = 0$. Da E glatt ist, d.h. $\Delta = -16(4A^3 + 27B^2) \neq 0$, muss $B \neq 0$ sein. Aus $A'^3B^2 = 0$ folgt also $A' = 0$. Wegen $\Delta' \neq 0$ ist auch $B' \neq 0$. Setzt man $u = (B/B')^{\frac{1}{6}} \in \overline{K}^*$. Dann gilt $u^4A' = A = 0$, $u^6B' = B$. Der gesuchte Isomorphismus ist also gefunden.

Fall 2 $B = 0$ und damit $j = 1728$. Da E glatt ist, d.h. $\Delta \neq 0$, ist $A \neq 0$. Aus $A^3B'^2 = 0$ folgt $B' = 0$. Wegen $\Delta' \neq 0$ ist $A' \neq 0$. Man setzt $u = (\frac{A}{A'})^{\frac{1}{4}} \in \overline{K}^*$. Dann gilt $u^4A' = A$ und $u^6B' = B = 0$. Der gesuchte Isomorphismus ist also gefunden.

Fall 3 $AB \neq 0$ und damit $j \neq 0, 1728$. Wegen $A^3B'^2 = A'^3B^2$ ist entweder $A', B' \neq 0$ oder $A', B' = 0$. Wären $A', B' = 0$, so wäre $\Delta' = 0$. Dies ist aber ein Widerspruch dazu, dass E' eine glatte Kurve ist. Also muss $A', B' \neq 0$ sein. Setzt man $u = (\frac{A}{A'})^{\frac{1}{4}} \in \overline{K}^*$, so ist $u^4A' = A$.
Es gilt: $A^3B'^2 = A'^3B^2 \Rightarrow B^2 = u^{12}B'^2 \Rightarrow B = u^6B'$ oder $B = -u^6B'$. Im Fall $B = -u^6B'$ ersetzt man u durch $\sqrt{-1}u \in \overline{K}^*$. Der gesuchte Isomorphismus ist damit gefunden. q.e.d.

Satz 14 *Sei $j_0 \in \overline{K}$. Dann gibt es eine elliptische Kurve E, die über $K(j_0)$ definiert ist, mit $j(E) = j_0$.*

Beweis: Man behandelt zunächsten den Fall $j_0 \neq 0, 1728$ und betrachtet die Kurve

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

Dann ist $\Delta = \frac{j_0^2}{j_0 - 1728)^3} \neq 0$ und wohldefiniert. Also ist E glatt und damit eine elliptische Kurve. Weiterhin ist $j(E) = j_0$. Es verbleiben noch die Fälle $j_0 = 0$ und $j_0 = 1728$. Hierfür benutzt man die beiden Kurven

$$E_1 : y^2 + y = x^3 \text{ mit } \Delta = -27, j(E) = 0$$
$$E_2 : y^2 = x^3 + x \text{ mit } \Delta = -64, j(E) = 1728$$

Ist $\mathrm{char}(K) \neq 2, 3$, dann sind E_1 und E_2 glatte Kurven. Für $\mathrm{char}(K) = 2$ oder 3 ist $1728 = 0$. Weil E_1 für $\mathrm{char}(K) = 2$ glatt und E_2 für $\mathrm{char}(K) = 3$ glatt ist, werden auch diese Fälle abgedeckt.

Lemma 15 *Sei P ein glatter Punkt auf einer Kurve C und L eine beliebige Gerade durch P. Dann gilt* $\mathrm{ord}_P(L) = 1$*, wenn L nicht tangential zu C in P verläuft.*

Beweis: Korollar 1.4 in Vortrag 4 des Seminars Einführung in die Theorie der algebraischen Kurven.

Lemma 16 *Seien C eine projektive Kurve, $P \in C$ ein glatter Punkt und $t \in \overline{K}(C)$ ein uniformisierendes Element in P.*

i) Ist $f \in \overline{K}(C)$ regulär in P, dann ist auch df/dt regulär in P.

ii) Seien $x, f \in \overline{K}(C)$ mit $x(P) = 0$ und $p = \mathrm{char}(K)$. Dann gilt:
$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1$*, wenn $p = 0$ oder $p \nmid \mathrm{ord}_P(x)$.*

Beweis: [Si] II.4.3.

Definition 17 *Sei C eine projektive Kurve. Ein Differential $\omega \in \Omega_C$ ist regulär, wenn* $\mathrm{ord}_P(\omega) \geq 0\ \forall P \in C$ *und nichtverschwindend, wenn* $\mathrm{ord}_P(\omega) \leq 0\ \forall P \in C$.

Satz 18 *Sei E eine elliptische Kurve. Dann ist das zur Weierstraß-Gleichung von E zugehörige invariante Differential ω regulär und nichtverschwindend.*

Beweis: Zunächst betrachtet man die Punkte im affinen Teil der Kurve E.
Sei $P = (x_0, y_0) \in E$ und

$$E : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

Wegen $d(x - x_0) = dx - dx_0 = dx$ und $d(y - y_0) = dy - dy_0 = dy$ ist

$$\omega = \frac{d(x - x_0)}{F_y(x, y)} = -\frac{d(y - y_0)}{F_x(x, y)}.$$

das invariante Differential der Weierstraß-Gleichung von E.
E ist glatt in P, also $F_x(P) \neq 0$ oder $F_y(P)$.
Sei ohne Einschränkung $F_x(P) \neq 0$. Dann ist $\mathrm{ord}_P(F_x) = 0$. Weil $F_x(P) \neq 0$ ist, kann $y - y_0$ keine Tangente an E in P sein, d.h. $\mathrm{ord}_P(y - y_0) = 1$ nach Lemma 15.
Wegen $y - y_0(P) = 0$ und $\mathrm{char}(K) \nmid 1 = \mathrm{ord}_P(y - y_0)$ gilt nach Lemma 16:

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(y - y_0) - \mathrm{ord}_P(F_x) - 1 = 1 - 0 - 1 = 0$$

Folglich hat ω weder Nullstellen noch Polstellen der Form (x_0, y_0).
Es verbleibt noch der Punkt $O = [0, 1, 0]$ im Unendlichen.
Sei $t \in \overline{K}(E)$ ein uniformisierendes Element in O, d.h. $\mathrm{ord}_O(t) = 1$. Es gilt $\mathrm{ord}_O(x) = -2$ und $\mathrm{ord}_O(y) = -3$. Daher ist $x = t^{-2}f$ und $y = t^{-3}g$ für $f, g \in \overline{K}(E)$ mit $f(O), g(O) \neq 0, \infty$. Man erhält:

$$\omega = \frac{dx}{F_y(x,y)} = \frac{d(t^2 f)dt}{2y + a_1 x + a_3} = \frac{-2t^3 f + t^{-2}(df/dt)}{2t^{-3}g + a_1 t^{-2} f + a_3} dt = \frac{-2f + t(dt/dt)}{2g + a_1 t f + a_3 t^3} dt.$$

Mit f ist auch df/dt regulär in P nach Lemma 16 und es gilt $f(O), g(O) \neq 0, \infty$. Für $\mathrm{char}(K) \neq 2$ hat die Funktion $\frac{-2f+t(dt/dt)}{2g+a_1 t f+a_3 t^3}$ also weder eine Nullstelle noch einen Pol in O.
Für $\mathrm{char}(K) = 2$ ist $\omega = -dy/F_x(x,y) = \frac{-3g+t(dg/dt)}{3f^2+a_4 t^4-a_1 tg+2a_2 t^2} dt$. Mit einer analogen Argumenation wie im Fall $\mathrm{char}(K) \neq 2$ erhält man, dass die Funktion $\frac{-3g+t(dg/dt)}{3f^2+a_4 t^4-a_1 tg+2a_2 t^2}$ weder eine Nullstelle noch einen Pol in O hat.
Insgesamt ist also ω holomorph und nicht-verschwindend. q.e.d.

Definition 19 (Legendre-Form) *Eine Weierstraß-Gleichung ist in Legendre-Form, wenn sie geschrieben werden kann als*

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

für ein $\lambda \in \overline{K}$.

Satz 20 *Sei* $\mathrm{char}(K) \neq 2$. *Dann gilt:*

a) Jede elliptische Kurve ist isomorph über $\overline{K}$ *zu einer Kurve in Legendre-Form*

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

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

b) Die j-Invariante von E_λ *ist*

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

c) *Die Abbildung*

$$\phi : \overline{K}\backslash\{0,1\} \to \overline{K}, \lambda \mapsto j(E_\lambda)$$

ist surjektiv.
Für $j \neq 0, 1728$ *ist* $\#\phi^{-1}(j(E_\lambda)) = 6$.
Für $j = 0$, $\mathrm{char}(K) \neq 3$ *ist* $\#\phi^{-1}(j(E_\lambda)) = 2$.
Für $j = 1728$, $\mathrm{char}(K) \neq 3$ *ist* $\#\phi^{-1}(j(E_\lambda)) = 3$.
Für $\mathrm{char}(K) = 3, j = 0 = 1728$ *ist* $\#\phi^{-1}(j(E_\lambda)) = 1$.

Beweis:

a) Wegen $\mathrm{char}(K) \neq 2$ hat E eine Weierstraß-Gleichung der Form

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

Ersetzt man (x, y) durch $(x, 2y)$ und zerlegt man das kubische Polynom über $\overline{K}$ auf der rechten Seite in Linearfaktoren, dann hat die Weierstraß-Gleichung die Form

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

für $e_1, e_2, e_3 \in \overline{K}$. Da E eine glatte Kurve ist, sind e_1, e_2, e_3 paarweise veschieden. Der Koordinatenwechsel

$$x = (e_2 - e_1)x' + e_1 \text{ und } y = (e_2 - e_1)^{\frac{3}{2}}y'$$

ist nach Bemerkung 9 von der erlaubten Form und damit ein Isomorphismus zwischen elliptischen Kurven. Man erhält mit diesem Koordinatenwechsel:

$$(y'(e_2 - e_1)^{\frac{3}{2}})^2 = ((e_2 - e_1)x' + e_1 - e_1)((e_2 - e_1)x' - (e_2 - e_1))(e_2 - e_1)x' + e_1 - e_3)$$
$$\Rightarrow y'^2 = x'(x' - 1)(x' - \frac{e_3 - e_1}{e_2 - e_1})$$

mit $\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \overline{K}\backslash\{0, 1\}$.

b) Es ist $b_2 = -4(1 + \lambda)$, $b_4 = 2\lambda$ und damit $c_4 = 16(\lambda^2 - \lambda + 1)$ und $\Delta = 16\lambda^4 - 32\lambda^3 + 16\lambda^2 = 16\lambda^2(\lambda - 1)^2$. Somit ist

$$j(E_\lambda) = \frac{c_4^3}{\Delta} = \frac{2^{12}(\lambda^2 - \lambda + 1)^3}{2^4\lambda^2(\lambda - 1)^2} = 2^8\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

c) Da $\overline{K}$ algebraisch abgeschlossen ist, folgt mit b), dass ϕ surjektiv ist.
Seien E_λ und E_μ elliptische Kurven mit Weierstraß-Gleichungen in Legendre-Form mit Parameter $\lambda, \mu \in \overline{K}\backslash\{0, 1\}$. Ist nun $j(E_\lambda) = j(E_\mu)$, dann gilt nach Satz 13 $E_\lambda \cong E_\mu$. Daher gehen die Weierstraß-Gleichungen von E_λ und E_μ durch die Variablentransformation $x = u^2x' + r$ und $y = u^3y'$ ineinander über. Durch die Gleichung

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

erhält man sechs Möglichkeiten für den Wert von μ in Abhängigkeit von λ.

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

Daher ist die $\#\phi^{-1}(j) = 6$, außer wenn zwei oder mehr dieser Werte für μ zusammenfallen. Letzteres ist genau dann der Fall, wenn

$$\lambda \in \{-1, 2, \frac{1}{2}\} \Rightarrow \mu \in \{-1, 2, \frac{1}{2}\} \Rightarrow \ \#\phi^{-1}(j) = 3$$

oder

$$\lambda^2 - \lambda + 1 = 0 \Rightarrow \ \#\phi^{-1}(j) = 2$$

Diese Werte von λ entsprechen den Werten $j(E_\lambda) = 1728$ und $j(E_\lambda) = 0$. Ist $\mathrm{char}(K) = 3$, dann stimmen diese Werte für λ alle überein und die Gleichung $j(E_\lambda) = 0$ hat die eindeutige Lösung $\lambda = -1$. q.e.d.

2 Gruppengesetz

Bemerkung 21 *Das Besondere an elliptischen Kurven ist, dass man auf ihren Punkten eine Gruppenstruktur definieren kann.*

Bemerkung 22 *Sei E eine elliptische Kurve, die durch eine Weierstraß-Gleichung gegeben ist. Sei $L \subset \mathbb{P}^2$ eine Gerade. Da $\deg(E) = 3$ und $\deg(L) = 1$, besteht $L \cap E$ mit Vielfachheiten gezählt aus drei Punkten nach dem Satz von Bezout.*

Definition 23 (Kompositionsgesetz) *Seien E eine elliptische Kurve, $P, Q \in E$ und L eine Gerade durch P und Q. Wenn $P = Q$, dann sei L die Tangente an E in P. Sei R der dritte Schnittpunkt von $E \cap L$ neben P und Q. Sei L' die Gerade durch R und $O = [0, 1, 0]$. Dann schneidet L' die Kurve E in den Punkten R, O und in einem dritten Punkt, den mit $P + Q$ bezeichnet.*

Bemerkung 24 (Gerade durch den Punkt im Unendlichen) *Seien $P = [x_0, y_0, 1] \in \mathbb{P}^2$ und $L : \alpha X + \beta Y + \gamma Z$ die Gerade durch P und $O = [0, 1, 0]$. Das lineare Gleichungssystem*

$$\begin{pmatrix} x_0 & y_0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ hat die Lösung } \begin{pmatrix} 1 \\ 0 \\ -x_0 \end{pmatrix}$$

Die Gerade L ist also gegeben durch $X - x_0 Z = 0$. Damit ist $L \cap \mathbb{A}^2 : x - x_0$.

Satz 25 *Das Kompositionsgesetz hat die folgenden Eigenschaften:*

a) Wenn eine Gerade L die Kurve E in nicht notwendigerweise verschiedenen Punkten P, Q, R schneidet, dann gilt: $(P + Q) + R = O$.

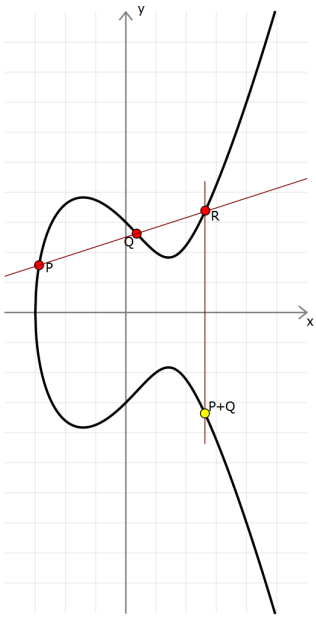

Abbildung 4: Beispiel für das Kompositionsgesetz

b) $\forall P \in E : P + O = P$.

c) $\forall P, Q \in E : P + Q = Q + P$

d) Sei $P \in E$. *Dann existiert ein Punkt* $-P \in E$ *mit* $P + (-P) = O$.

e) $\forall P, Q, R \in E : (P + Q) + R = P + (Q + R)$.

f) Ist E *über dem Körper* K *definiert, dann ist*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

ist eine Untergruppe von E.

Beweis:

a) Seien $P, Q \in E$ und L die Gerade durch P und Q. Der dritte Schnittpunkt von L und E sei R. Sei L' die Gerade durch R und O. Der dritte Schnittpunkt von L' und E ist $P + Q$. Nun addiert man $P + Q$ und R. L' ist die Gerade durch $P + Q$ und R. Der dritte Schnittpunkt von L' und E ist also O. Die Tangente $Z = 0$ an E in O schneidet E nach der Bemerkung 2 drei Mal in O. Also ist $(P + Q) + R = O$.

b) Seien $P \in E$, L die Gerade durch P und O und sei Q der dritte Schnittpunkt von L und E. Die Gerade durch Q und O ist wieder L und der dritte Schnittpunkt von L und E ist daher P. Folglich ist $P + O = P$.

c) Die Konstruktion von $P+Q$ ist symmetrisch in P und Q.

d) Sei $P \in E$ und sei $-P$ der dritte Schnittpunkt der Geraden durch P und O. Dann ist $-P \in E$. Da $O, P, -P$ auf einer Geraden liegen, gilt nach $a)$ und $b)$ nun $O = (P+O)+(-P) = P+(-P)$.

e) Dies kann mit dem Gruppengesetz-Algorithmus nachgerechnet werden, der noch folgen wird. Es wird auch im nächsten Vortrag daraus folgen, dass E mit dem Kompostionsgesetz isomorph zur Picardgruppe der Divisoren vom Grad 0 von E ist.

f) Diese Behauptung wird aus dem Gruppengesetzalgorithmus folgen.

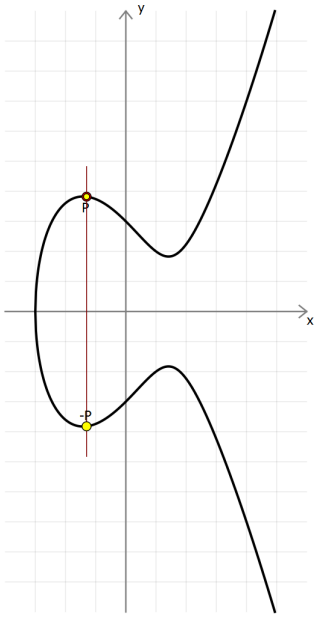

Abbildung 5: Punkt P mit inversem Element $-P$

Bemerkung 26 *Die Behauptungen $a) - e)$ in Satz 25 sagen aus, dass E durch das Gruppengesetz zu einer abelschen Gruppen mit neutralem Element O wird.*

Bemerkung 27 *Ist eine elliptische Kurve E über $\mathbb{Q}$ definiert, so bilden nach dem letzten Satz die rationalen Punkte auf E eine Gruppe. Das ist interessant, wenn man sich mit diophantischen Gleichungen in 2 Variablen beschäftigt. Die rationalen Lösungen von quadratischen diophantischen Gleichungen hat man im Griff durch den Satz von Hasse-Minkowski. Solche quadratischen Gleichungen definieren projektive Kurven vom Geschlecht 0. Aber schon die rationalen Lösungen von Gleichungen, die Kurven vom Geschlecht 1 definieren, sind nicht so leicht in den Griff zu bekommen. Immerhin weiß man nun, dass die rationalen Punkte von diesen Gleichungen eine Gruppe bilden.*

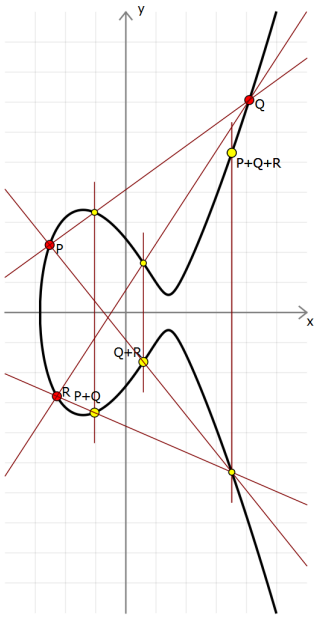

Abbildung 6: Beispiel für das Assoziativgesetz

Definition 28 *Sei E eine elliptische Kurve. Für $m \in \mathbb{Z}$ und $P \in E$ definiert man*

$$[m]P := \underbrace{P + \ldots + P}_{m-mal,\ wenn\ m>0}, [m]P := \underbrace{-P - \ldots - P}_{|m|-mal,\ wenn\ m<0}, [0]P := O$$

Algorithmus 29 (Gruppengesetz-Algorithmus) *Sei E eine elliptische Kurve, die gegeben ist durch eine Weierstraß-Gleichung*

$$E : F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

a) Sei $P_0 = (x_0, y_0) \in E$. Dann ist $-P_0 = (x_0, -y_0 - a_1x_0 - a_3) \in E$.

b) Seien $P_1, P_2, P_3 \in E$ mit $P_1 + P_2 = P_3$ und $P_i = (x_i, y_i)$ für $i = 1, 2, 3$.
Wenn $x_1 = x_2$ und $y_1 + y_2 + a_1x_2 + a_3 = 0$, dann ist $P_1 + P_2 = O$.
Andernfalls definiert man λ und ν durch die folgenden Formeln:

	λ	ν
$x_1 \neq x_2$	$\frac{y_2-y_1}{x_2-x_1}$	$\frac{y_1x_2-y_2x_1}{x_2-x_1}$
$x_1 = x_2$	$\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$	$\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$

Dann ist $y = \lambda x + \nu$ die Gerade durch P_1 und P_2 oder die Tangente an E, falls $P_1 = P_2$.

c) Mit der Notation von b) hat $P_3 = P_1 + P_2$ die Koordinaten

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

d) Als Spezialfall für c) erhält man für $P_1 \neq \pm P_2$

$$x(P_1+P_2) = (\frac{y_2-y_1}{x_2-x_1})^2 + a_1(\frac{y_2-y_1}{x_2-x_1}) - a_2 - x_1 - x_2$$

und die Duplikationsformel für $P=(x,y) \in E$:

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

wobei b_2, b_4, b_6, b_8 definiert sind wie in Bemerkung 3.

Beweis:

a) Sei $P_0 = (x_0, y_0) \in E$. Die Gerade durch P und $O = [0,1,0]$ ist $L : x - x_0 = 0$ nach Bemerkung 24. Der Punkt $-P$ ist der dritte Schnittpunkt von $L \cap E$ neben P und O nach dem Beweis von Satz 25 e). Setzt man die Gleichung von L in die Gleichung für E ein, so erhält man ein quadratisches Polynom $F(x_0, y)$ mit den Nullstellen y_0, denn $P \in E \cap L$, und y_0', wobei $-P = (x_0, y_0')$. F hat also die Form:

$$F(x_0, y) = c(y - y_0)(y - y_0')$$

Ein Koeffizientenvergleich der beiden letzten Polynome ergibt $c = 1$ und $y_0' = -y_0 - a_1x_0 - a_3$. Also ist $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

b) Wenn $x_1 = x_2$ und $y_1 + y_2 + a_1x_2 + a_3 = 0 \Leftrightarrow y_2 = -y_1 - a_1x_1 - a_3$, dann ist $P_2 = -P_1$ nach *a)* und daher $P_1 + P_2 = P_1 + (-P_1) = O$.
Andernfalls hat die Gerade L durch P_1 und P_2 oder Tangente an E in P_1, falls $P_1 = P_2$, die Gleichung $L : y = \lambda x + \nu$. Man betrachtet zunächst den Fall $x_1 \neq x_2$: Da P_1 und P_2 auf L liegen, gilt $y_1 = \lambda x_1 + \nu$ und $y_2 = \lambda x_2 + \nu \Rightarrow \lambda(x_2 - x_1) = y_2 - y_1 \Rightarrow \lambda = \frac{y_2-y_1}{x_2-x_1}$. Es folgt: $\nu = y_1 - \lambda x_1 = \frac{y_1x_2 - y_2x_1}{x_2-x_1}$.
Es verbleibt noch der Fall, dass $P_1 = P_2$.
Sei $f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$. Die Tangente an E durch $P_1 = [x_1, y_1, 1]$ ist gegeben durch $\alpha X + \beta Y + \gamma Z$ mit $\alpha = \frac{\partial f}{\partial X}(P) = a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4$, $\beta = \frac{\partial f}{\partial Y}(P) = 2y_1 + a_1x_1 + a_3$,
$\gamma = \frac{\partial f}{\partial Z}(P) = y_1^2 + a_1x_1y_1 + 2a_3y_1 - a_2x_1^2 - 2a_4x_1 - 3a_6$. Es ist $\gamma \neq 0$, denn sonst läge $O = [0,1,0]$ auf L und damit wäre $P_2 = -P_1$. Dieser Fall war aber schon behandelt worden. Also ist die Gerade durch P_1 und P_2 von der Form $y = \lambda x + \nu$ mit $\lambda = -\frac{\alpha}{\beta} = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ und $\nu = -\frac{\gamma}{\beta} = \frac{-y_1^2 - a_1x_1y_1 - 2a_3y_1 + a_2x_1^2 + 2a_4x_1 + 3a_6}{2y_1 + a_1x_1 + a_3} \overset{f(x_1,y_1)=0}{=} \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$.

c) Seien $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$ mit $-P_1 \neq P_2$, denn der Fall $-P_1 = P_2$ wurde schon behandelt. Die Gerade L durch P_1 und P_2 hat nach *b)* die Form $L : y = \lambda x + \nu$. Setzt man die Gleichung von L in die Gleichung von E ein, dann hat $F(x, \lambda x + \nu)$ drei Nullstellen x_1, x_2, x_3 über $\overline{K}$, wobei $\widetilde{P_3} = (x_3, \widetilde{y_3})$ der dritte Punkt von $L \cap E$ ist. Da $P_1, P_2, \widetilde{P_3} \in L$ gilt nach dem Satz

$$P_1 + P_2 + \widetilde{P_3} = O$$

Durch Koeffizientenvergleich in x^3 und x^2 von

$$F(x, \lambda x + \nu) = -x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\nu + a_1\nu + a_3\lambda - a_4)x + (\nu^2 + a_3\nu - a_6)$$
$$= c(x - x_1)(x - x_2)(x - x_3)$$

erhält man $c = -1$ und $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$. Wegen
$P_1 + P_2 + \widetilde{P_3} = O \Rightarrow P_1 + P_2 = -\widetilde{P_3} \Rightarrow P_3 = -\widetilde{P_3}$ und $y_3 = \lambda x_3 + \nu$ liefert die Formel aus a), dass $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$
und $y_3 = -(\lambda + a_1)x_3 - \nu - a_3$.

d) Ergibt sich durch Einsetzen.

Korollar 30 *Sei E eine elliptische Kurve, die durch eine Weierstraß-Gleichung $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ gegeben ist. Eine Funtion $f \in \overline{K}(E) = \overline{K}(x, y)$ heißt gerade, falls $f(P) = f(-P)$ für alle $P \in E$. Dann gilt: f ist gerade $\Leftrightarrow f \in \overline{K}(x)$.*

Beweis: Es gilt: O=[0,1,0]=-O, d.h. $f(O) = f(-O)\ \forall f \in \overline{K}(E)$. Es reicht also die Punkte im affinen Teil von E zu betrachten.
"$\Leftarrow$": Ist $P = (x_0, y_0) \in E$, dann ist nach dem Gruppengesetzalgorithmus
$-P = (x_0, -y_0 - a_1x_0 - a_3)$. Da $x(P) = x(-P)$ ist, ist jedes Element von $\overline{K}(x)$ gerade.
"$\Rightarrow$": Sei $f \in \overline{K}(x, y)$ gerade. Da F bzgl. y den Grad 2 hat, normiert sowie irreduzibel ist, ist $[\overline{K}(x, y) : \overline{K}(x)] = 2$ und folglich $(1, y)$ eine $\overline{K}(x)$-Basis von $\overline{K}(x, y)$. Somit existieren $g, h \in \overline{K}(x)$ mit $f(x, y) = g(x) + h(x)y$. Da f gerade ist, gilt für alle $(x, y) \in E$:

$$g(x) + h(x)y = f(x, y) = f(x, -y - a_1x - a_3) = g(x) + h(x)(-y - a_1x - a_3)$$
$$\Rightarrow (2y + a_1x + a_3)h(x) = 0$$

Angenommen, $h \neq 0$, dann muss $2y + a_1x + a_3 = 0$ sein. Somit gilt $2 = a_1 = a_3 = 0$. Nun ist $b_2 = 4a_2 = 0, b_4 = 2a_4 = 0, b_6 = 4a_6 = 0$. Daher ist $\Delta = 0$. Dies ist aber ein Widerspruch dazu, dass E eine elliptische Kurve ist. Also muss $h = 0$ sein. Also $f(x, y) = g(x) \in \overline{K}(x)$. q.e.d.

Beispiel 31 *Sei $E/\mathbb{Q}$ die elliptische Kurve $E : y^2 = x^3 + 17$. Nach dem Beispiel 11 ist E nicht-singulär. Auf E liegen die ganzzahligen Punkte*

$$P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23), P_6 = (43, 282),$$
$$P_7 = (52, 375), P_8 = (5234, 378661).$$

Auf der Kurve E liegen auch rationale Punkte wie zum Beispiel:

$$[2]P_2 = (\frac{137}{64}, \frac{-2651}{512}), P_2 + P_3 = (-\frac{8}{9}, -\frac{109}{27})$$

Es kann gezeigt werden, dass jeder rationale Punkt $P \in E(\mathbb{Q})$ von der Form $P = [m]P_1 + [n]P_3$ für $m, n \in \mathbb{Z}$ ist. Also gilt: $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}$. Dies ist ein Beispiel für den Satz von Mordell-Weil, der besagt, dass die Gruppe der rationalen Punkte auf einer elliptischen Kurve endlich erzeugt ist.
Die Kurve E hat genau 16 ganzzahlige Punkte, nämlich
$\{\pm P_1, \ldots, \pm P_8\}$. Das ist ein Beispiel für das Theorem von Siegel, das besagt, dass die Menge von ganzzahligen Punkten auf einer elliptischen Kurve endlich ist.

Bemerkung 32 *Oft ist es nützlich die Koeffizienten einer Weierstraß-Gleichung für eine elliptische Kurve E, die über $\mathbb{Q}$ definiert ist, modulo einer Primzahl p zu reduzieren und E als eine Kurve zu betrachten, die über $\mathbb{F}_p$ definiert ist. Für fast alle Primzahlen p, nämlich die mit $p \nmid \Delta$, ist die reduzierte Kurve glatt und daher eine elliptische Kurve über $\mathbb{F}_p$. Für die Primzahlen p mit $p \mid \Delta$ besitzt die reduzierte Kurve eine Singularität. Aber auch die glatten Punkte auf einer solchen singulären Kurve kann man mit Hilfe des Kompositionsgesetzes mit einer Gruppenstruktur versehen.*

Satz 33 *Wenn eine Kurve E, die durch eine Weierstraß-Gleichung gegeben ist, singulär ist, dann gibt es eine rationale Abbildung $\phi : E \to \mathbb{P}^1$ vom Grad 1, d.h. die Kurve E ist birational zu $\mathbb{P}^1$.*

Beweis: Sei E gegeben durch die Weierstraß-Gleichung

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

Man kann ohne Einschränkung einen linearen Koordinatenwechsel durchführen, sodass der singuläre Punkt $(0,0)$ ist. Dann gilt:

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

Daher ist die Weierstraß-Gleichung von der Form

$$E : y^2 + a_1xy = x^3 + a_2^2$$

Die rationale Abbildung

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

hat Grad eins. Um das einzusehen, konstruiert man eine Umkehrabbildung von ϕ.
Seien $x, y \neq 0$ und $t = \frac{y}{x}$. Teilt man die Weierstraß-Gleichung von E durch x^2, so ergibt sich:

$$(\frac{y}{x})^2 + a_1\frac{y}{x} = x + a_2 \Rightarrow t^2 + a_1t = x + a_2 \Rightarrow x = t^2 + a_1t - a_2 \text{ und}$$
$$y = xt = t^3 + a_1t^2 - a_2t$$

Daher sind $x, y \in \overline{K}(t)$. Für $\psi : \mathbb{P}^1 \to E, [1,t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$ gilt jetzt:

$$\phi(\psi([1,t])) = \phi((t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)) = [t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t] = [x,y] = [1,t] \text{ und}$$
$$\psi(\phi((x,y)) = \psi([x,y]) = \psi([1,t]) = (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t) = (x,y).$$

Damit ist ψ eine Umkehrabbildung von ϕ. Folglich induziert ψ eine Umkehrabbildug $\psi^* : \overline{K}(E) \to \overline{K}(\mathbb{P}^1)$ des von ϕ induzierten Körperhomomorphismus $\phi^* : \overline{K}(\mathbb{P}^1) \to \overline{K}(E)$. Also ist ϕ^* ein Isomorphismus und somit $[\overline{K}(E) : \phi^*(\overline{K}(\mathbb{P}^1))] = \deg(\phi) = 1$.

Definition 34 (nicht-singulärer Teil einer Kurve) *Sei E eine möglicherweise singuläre Kurve, die durch eine Weierstraß-Gleichung gegeben ist. Der nicht-singuläre Teil von E, der mit E_{ns} bezeichnet wird, ist die Menge der glatten Punkte von E. Ist E über einem Körper K definiert, dann sei $E_{ns}(K)$ die Menge der glatten Punkte von $E(K)$.*

Satz 35 *Sei E eine Kurve, die durch eine Weierstraß-Gleichung $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ gegeben ist, mit $\Delta = 0$, d.h. E besitzt einen singulären Punkt S. Dann ist E_{ns} mit dem Gruppengesetz eine abelsche Gruppe.*

a) Sei der singuläre Punkt S von E ein Knoten und seien

$$y = \alpha_1 x + \beta_1 \text{ und } y = \alpha_2 x + \beta_2$$

die verschiedenen Tangenten an E in S. Dann ist die Abbildung

$$\phi : E_{ns} \to \overline{K}^*, (x,y) \mapsto \frac{y - a_1x - \beta_1}{y - \alpha_2 - \beta_2}$$

ein Isomorphismus von abelschen Gruppen.

b) Sei der singuläre Punkt S von E eine Spitze und sei

$$y = \alpha x + \beta$$

die Tangente an E in S. Dann ist die Abbildung

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

ein Isomorphismus von abelschen Gruppen.

Beweis: Weil die glatten Punkte von E nicht auf den Tangenten der Singularität von E liegen, sind die Abbildungen ϕ und ψ wohldefiniert.
E_{ns} ist abgeschlossen unter dem Kompositionsgesetz. Schneidet eine Gerade L den nichtsingulären Anteil E_{ns} in zwei nicht notwendigerweise verschiedenen Punkten, dann kann der singuläre Punkt S von E nicht auf S liegen. Denn nach den Eigenschaften der Schnittzahlen gilt für den singulären Punkt $I(S, L \cap E) \geq 2$. Daher würde $L \cap E$ vier Punkte mit Vielfachheit gezählt enthalten, was aber dem Satz von Bezout widerspricht, da $\deg(E) = 3$ und $\deg(L) = 1$ ist.
Schneidet eine Gerade L, die nicht S enthält, E_{ns} in drei nicht notwendigerweise verschiedenen Punkten P, Q, R, dann gilt nach Satz 25 $P + Q + R = O$. Um einzusehen, dass die Abbildungen in a) und b) Gruppenhomomorphismen sind, reicht es also zu zeigen, dass die Bilder von P, Q, R unter ϕ miteinander multipliziert 1 ergeben bzw. unter ψ zusammenaddiert 0 ergeben.
Da das Gruppengesetz und die Abbildungen in a) und b) in Termen von Geraden in $\mathbb{P}^2$ definiert sind, kann man ohne Einschränkung eine lineare Koordiantentransformation durchführen, sodass der singuläre Punkt S in $(0,0)$ liegt. Dann gilt:

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

Daher hat E die Weierstraß-Gleichung

$$y^2 + a_1xy = x^3 + a_2x^2$$

Sei $s \in \overline{K}$ eine Nullstelle von $s^2 + a_1 s - a_2$. Führt man die Substitution $y \mapsto y + sx$ durch, so erhält man

$$y^2 + (s^2 + a_1 s - a_2)x^2 + (2s + a_1)xy - x^3 = y^2 + \underbrace{(2s + a_1)}_{:=A} xy - x^3 = 0$$

Die Kurve E hat einen Knoten, wenn $A \neq 0$, und eine Spitze, wenn $A = 0$. Man verwendet nun die homogenen Koordinaten für die Gleichung von E:

$$E : Y^2 Z + AXYZ - X^3 = 0$$

a) Die Singularität $S = [0, 0, 1]$ ist ein Knoten, d.h. $A \neq 0$. Die Tangenten durch $S = [0, 0, 1]$ sind gegeben durch $Y = 0$ und $Y + AX = 0$. Man betrachtet nun die Abbildung

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

Weil $A \neq 0$ ist, kann man die folgende Variablentransformation

$$X = A^2 X' - A^2 Y', Y = A^3 Y', Z = Z'$$

durchführen, um die Gleichung zu vereinfachen. Dann ergibt sich:

$$\begin{gathered} -X'^3 A^6 + 3X'^2 Y'^2 A^6 - 3X' Y'^2 A^6 + X' Y' Z' A^6 + Y'^3 A^6 \\ \Rightarrow X' Y' Z' - (X' - Y')^3 = 0 \text{ und} \\ \phi : E_{ns} \to \overline{K}^*, [X', Y', Z'] \mapsto \frac{X'}{Y'} \end{gathered}$$

Man dehomogenisiert nun, indem man $Y' = 1$, also $x = \frac{X'}{Y'}, z = \frac{X'}{Y'}$ setzt. Das ergibt für die Gleichung von E

$$E : g(x, z) = xz - (x - 1)^3 = 0$$

und:

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

Hierbei sollte man beachten, dass der singuläre Punkt S nun der einzige Punkt im Unendlichen und damit der affine Teil von E der nicht-singuläre Teil von E ist. Diese Abbildung ϕ besitzt eine Umkehrabbildung

$$\widetilde{\phi} : \overline{K}^* \to E_{ns}, t \mapsto (t, \frac{(t-1)^3}{t}),$$

denn

$$\phi(\widetilde{\phi}(t)) = \phi((t, \frac{(t-1)^3}{t})) = t \text{ und } \widetilde{\phi}(\phi(x, z)) = \widetilde{\phi}(x) = (x, \frac{(x-1)^3}{x}) \overset{g(x,y)=0}{=} (x, z)$$

Somit hat man eine Bijektion zwischen den Mengen E_{ns} und $\overline{K}^*$.
Es bleibt noch zu zeigen: Wenn eine Gerade L mit $S \notin L$ den nicht-singulären Teil

E_{ns} in drei Punkten $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ schneidet, dann gilt $x_1x_2x_3 = 1$. L ist von der Form $z = ax + b$. Weil $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in E_{ns} \cap L$, sind $x_1, x_2, x_3 \in \overline{K}$ die Nullstellen des Polynoms

$$x(ax + b) - (x - 1)^3$$

Koeffizientenvergleich dieses Polynoms mit $c(x - x_1)(x - x_2)(x - x_3)$ in x^3 und im konstanten Term liefert $c = -1$ und $x_1x_2x_3 = 1$.
b) In diesem Fall ist $A = 0$ und die Tangente an E in $S = [0, 0, 1]$ ist $Y = 0$. Es ist $x(S) = 0$. Man betrachtet also die Abbildung

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

Man dehomoginisiert, indem man $Y = 1$ (also $x = \frac{X}{Y}, z = \frac{Z}{Y}$) setzt, und erhält:

$$E : z - x^3 = 0$$
$$\psi : E_{ns} \to \overline{K}^+, (x, z) \mapsto x$$

Auch hier ist nun wie in a) in diesem Koordinatensystem der affine Teil von E der nichtsinguläre Teil von E.
Die Umkehrabbildung von ψ ist $\widetilde{\psi} : \overline{K}^+ \to E_{ns}, t \mapsto (t, t^3)$, denn

$$\psi(\widetilde{\psi}(t)) = \psi((t, t^3)) = t \text{ und } \widetilde{\psi}(\psi((x, z)) = \widetilde{\psi}(x) = (x, x^3) \overset{x^3=z}{=} (x, z)$$

Schneidet eine Gerade $L : z = ax+b$, die S nicht enthält, E_{ns} in den Punkten $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, so sind x_1, x_2, x_3 Nullstellen des Polynoms $(ax + b) - x^3$. Führt man einen Koeffizientenvergleich zwischen dem lezten Polynom und $c(x - x_1)(x - x_2)(x - x_3)$ in x^3 und x^2 durch, dann erhält man $c = -1$ und $x_1 + x_2 + x_3 = 0$ q.e.d.

Literatur

[Si] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.