NORMALFORMEN UND DAS ZENTRUM EINER ELLIPTISCHEN KURVE

Diplomarbeit

vorgelegt von
Fabian Sander

Fakultät für Mathematik
Universität Bielefeld

Juni 2011

Datum: 30. August 2011.

Inhaltsverzeichnis

Vorwort 1
1. Separable Quadratische Erweiterungen 3
2. Kubische Gleichungen und Polynome 5
2.1. Das assoziierte Dreieck 5
2.2. Die Normalform einer kubischen Gleichung 7
2.3. Klassifikation 12
2.4. Charakteristische Fixpunkte 16
3. Elliptische Kurven 22
3.1. Grundlagen 22
3.2. Die Normalform einer elliptischen Kurve 25
3.3. Klassifikation 29
3.4. Die assoziierte kubische Gleichung 30
4. Das Zentrum einer elliptischen Kurve 35
4.1. Lage des Zentrums 35
4.2. Fahnen 36
4.3. Die Involution 38
4.4. Schnittpunkte von Polaren 42
Literatur 45

Vorwort

In dieser Arbeit beschäftigen wir uns mit der Konstruktion von Normalformen von kubischen Gleichungen und elliptischen Kurven über beliebigen Körpern, die diese bis auf affine Transformationen eindeutig charakterisieren. Für eine kubische Gleichung über einem Körper K, also eine Gleichung der Form

$$ax^3 + bx^2 + cx + d,\ a, b, c, d \in K,\ a \neq 0,$$

ist für $\mathrm{char}(K) \neq 3$ die Normalform

$$x^3 + ex + f,\ e, f \in K$$

bekannt, deren Lösung mit Hilfe der Cardanischen Formeln berechnet werden können. Diese liefert jedoch neben der Einschränkung der Charakteristik auch keine Klassifizierung bis auf affine Transformationen. In Kapitel 2 konstruieren wir daher in Anlehnung an ein Preprint von Markus Rost [Rost] eine solche klassifizierende Normalform. Einer kubischen Gleichung lässt sich das Tripel der Lösungen über einem algebraischen Abschluss zuordnen, dass wir *das assoziierte Dreieck* nennen. Abgesehen von *speziellen* kubischen Gleichungen, deren assoziiertes Dreieck besondere Symmetrieeigenschaften besitzen, können wir die Normalisierung einer Gleichung nun auf die Normalisierung einer charakteristischen affinen Geraden, der *Basic Line* zurückführen. Eine bestimmte Koordinatenwahl der Basic Line impliziert für jede nichtspezielle kubische Gleichung die Normalform

$$x^3 - x^2 + (9t - 2)x - (4t - 1) = 0,\ t \in K \setminus \left\{\frac{1}{4}, \frac{7}{27}\right\}.$$

Der Parameter t bestimmt eine nicht-spezielle kubische Gleichung also bis auf affine Transformationen. Für elliptische Kurven, also projektive Varietäten der Form

$$Y^Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, a_i \in K,$$

ist eine solche klassifizierende Invariante bereits bekannt, die sogenannte *j-Invariante*. Sie charakterisiert elliptische Kurven eindeutig bis auf $\bar{K}$-Isomorphie, das heißt, bis auf affine Transformationen über einem algebraischen Abschluss $\bar{K}$. Ebenfalls bekannt ist für $\mathrm{char}(K) \neq 2, 3$ die Normalform

$$Y^2Z = X^3 - 27c_4XZ^2 - 54c_6Z^3,\ c_i \in K,$$

die aber wiederum neben der Einschränkung der Charakteristik keinen Aufschluss über den Isomorphietyp der Kurve gibt. In Kapitel 3 konstruieren wir daher für jede elliptische Kurve E über einem beliebigen Körper K mit $j(E) \neq 0, 1728$ die Normalform

$$E(j, a) : \frac{Y^2 - XY - aX^2}{1 + 4a}Z = X^3 - \frac{36X + Z}{j(E) - 1728}Z^2,\ a \in K \setminus \left\{\frac{1}{4}\right\},$$

die nur durch affine Transformationen über K erreicht wird. Des Weiteren entwickeln wir mit Hilfe einiger algebraischen Vorbemerkungen aus Kapitel 1 Kriterien für die Isomorphie zweier ellitischer Kurven der Form $E(j,a)$ und $E(j',a')$. Für $\mathrm{char}(K) \neq 2$ lässt sich einer elliptischen Kurve E über K eine kanonische kubische Gleichung über K zuordnen, deren assoziiertes Dreieck gerade aus den 3 Punkten auf E mit Ordnung 2 bezüglich des Gruppengesetzes auf E besteht. Nun stellt sich die Frage nach einer Beziehung zwischen der j-Invariante einer elliptischen Kurve und der t-Invariante der assoziierten kubischen Gleichung. Tatsächlich erhalten wir eine 1:1-Relation

$$\{\text{Elliptischen Kurven über } K \text{ bis auf } \bar{K}\text{-Isomorphie}\}$$
$$\overset{1:1}{\longleftrightarrow}$$
$$\left\{ \begin{array}{c} \text{Nicht-spezielle kubische Gleichungen} \\ \text{über } K \text{ bis auf affine Transformationen} \end{array} \right\}.$$

Für die t-Invariante erhalten wir in Abhängigkeit der j-Invariante die Relation

$$t = \frac{1}{4} - \frac{16}{j - 1728}.$$

In der Konstruktion der Normalform $E(j,a)$ einer elliptischen Kurve E zeigt sich, dass ein eindeutig bestimmter Punkt $C(E) \in \mathbb{P}^2$ auf den Ursprung verschoben werden muss, um die Normalform zu erreichen. Diesen charakteristischen Punkt nennen wir *das Zentrum von E*. In Kapitel 4 beschäftigen wir uns mit der Lage des Zentrums bezüglich der elliptischen Kurve und entwickeln zwei geometrische Interpretationen dieses Punktes. Dazu definieren wir *die Polare* eines Punktes $P \in \mathbb{P}^2$ bezglich E, eine Kurve, die E genau in den Punkten schneidet, auf deren Tangente P liegt. Für $\mathrm{char}(K) \neq 3$ definieren die Polaren der Punkte auf der Geraden L durch die 3 Punkte auf E mit Ordnung 2 eine kanonische Involution, bei der das Zentrum von E gerade mit dem Punkt im Unendlichen auf L korrespondiert. Die zweite Interpretation beschreibt das Zentrum von E als einzigen affinen Schnittpunkt von Polaren auf einer bestimmten zu E assoziierten Geraden.

1. Separable Quadratische Erweiterungen

Dieses Kapitel dient dazu, einige algebraische Grundlagen zu schaffen, die an späterer Stelle für die Klassifikation von elliptischen Kurven über beliebigen Körpern benötigt werden.

Sei K ein Körper und

$$D_n(K) := \{a \in K \mid 1 - na \in K^*\}$$

die Menge aller Körperelemente, die nicht invers zu einem gegebenen $n \in K$ sind. Für $a \in D_4(K)$ definieren wir das Polynom

$$P_a := t^2 - t + a \in K[t]$$

und die K-Algebra

$$K_a := K[t]/(P_a).$$

Das folgende Lemma zeigt, dass alle separablen quadratischen Erweiterungen von dieser Form sind:

Lemma 1.0.1. a) *K_a/K ist eine separable Erweiterung*

b) *Sei* $\mathrm{char}(K) \neq 2$. *Für jede separable quadratische Erweiterung F/K gilt $F \cong_K K_a$ für ein $a \in D_4(K)$*

c) *Äquivalent sind*

(i) $K_a \cong_K K_{a'}$

(ii) *Es existiert ein $d \in D_2(K)$ mit* $a' = \dfrac{a - d + d^2}{(1-2d)^2}$

Beweis. a) Es reicht zu zeigen, dass P_a separabel ist. Die Diskriminante von P_a ist $\Delta(P_a) = 1 - 4a$. Dieser Wert ist nach Voraussetzung für den Parameter a ungleich 0, also ist P_a separabel.

b) Da jede quadratische Erweiterung eine einfache Erweiterung ist, existiert ein $\gamma \in F$ mit $F = K[\gamma]$. Sei $Q(t) := t^2 + \alpha t + \beta$ das Minimalpolynom von γ über K. Dann folgt $K[\gamma] = K[t]/\big(Q(t)\big)$ und es gilt $\Delta(Q) = \alpha^2 - 4\beta \neq 0$, da Q separabel ist. Dann ist

$$K[t]/\big(Q(t)\big) \to K_{\frac{1-\alpha^2+4\beta}{4}}$$
$$t \mapsto t - \frac{1+\alpha}{2}$$

der gewünschte Isomorphismus. Die Wohldefiniertheit folgt aus

$$\left(t - \frac{1+\alpha}{2}\right)^2 + \alpha\left(t - \frac{1+\alpha}{2}\right) + \beta = t^2 - t + \frac{1-\alpha^2+4\beta}{4} = 0$$

und

$$1 - 4\left(\frac{1-\alpha^2+4\beta}{4}\right) = \alpha^2 - 4\beta = \Delta(Q) \neq 0.$$

Es gilt also $\frac{1-\alpha^2+4\beta}{4} \in D_4(K)$. Die Wohldefiniertheit der Umkehrabbildung folgt aus

$$\begin{aligned}&\left(t+\frac{1+\alpha}{2}\right)^2-\left(t+\frac{1+\alpha}{2}\right)+\frac{1-\alpha^2+4\beta}{4}\\&=t^2+\alpha t+\beta=0.\end{aligned}$$

c) (i)⇒(ii) Jeder Isomorphismus $\phi\colon K_a \xrightarrow{\sim} K_{a'}$ ist eindeutig durch das Bild von t bestimmt. Sei $\phi(t)=ct+d$, wobei $c,d\in K$, $c\neq 0$. Aufgrund der Wohldefiniertheit von ϕ gilt

$$\begin{aligned}\phi(P_a)&=c^2t^2+c(2d-1)t+a-d+d^2=0\\&\Leftrightarrow t^2+\frac{c(2d-1)}{c^2}t+\frac{a-d+d^2}{c^2}=t^2-t+a'\end{aligned}$$

Durch Koeffizientenvergleich folgt $c=1-2d$ und

$$a'=\frac{a-d+d^2}{c^2}=\frac{a-d+d^2}{(1-2d)^2}$$

(ii)⇒(i) Sei $a'=\frac{a-d+d^2}{(1-2d)^2}$, $d\in D_2(K)$. Dann ist

$$\begin{aligned}\phi\colon K_a &\to K_{a'}\\ t&\mapsto (1-2d)t+d\end{aligned}$$

ein Isomorphismus. Die Wohldefiniertheit folgt aus

$$\begin{aligned}\phi(P_a)=&(1-2d)^2t^2-t\left(1-4d+4d^2\right)+a-d+d^2\\=&(1-2d)^2\left(t^2-t+a'\right)=0\end{aligned}$$

Die Umkehrabbildung

$$\begin{aligned}\phi^{-1}\colon K_{a'} &\to K_a\\ t&\mapsto \frac{t-d}{1-2d}\end{aligned}$$

ist wegen

$$\left(\frac{t-d}{1-2d}\right)^2-\frac{t-d}{1-2d}+a'=\left(\frac{1}{1-2d}\right)^2\left(t^2-t+a\right)=0$$

ebenfalls wohldefiniert.

□

2. Kubische Gleichungen und Polynome

2.1. **Das assoziierte Dreieck.** Unter einem kubischen Polynom *in allgemeiner Normalform* über einem gegebenen Körper K verstehen wir ein Polynom

$$P(t) = t^3 + a_2t^2 + a_1t + a_0$$

mit $a_i \in K$ für $i = 1, 2, 3$. Über einem algebraischen Abschluss $\bar{K}$ von K sei das Polynom von der Form

$$P(t) = (t - r_1)(t - r_2)(t - r_3).$$

Im Folgenden bezeichnen wir das Tupel $\mathcal{D} := (r_1, r_2, r_3)$ aufgrund der Anschauung für $K = \mathbb{C}$ als *das zu $P(t)$ assoziierte Dreieck.*

Definition 1. Ein kubisches Polynom in allgemeiner Normalform sowie das assoziierte Dreieck heißen *speziell*, falls paarweise verschiedene $i, j, k \in \{1, 2, 3\}$ existieren, sodass mindestens eine der folgenden Eigenschaften erfüllt ist:

a) $r_i = r_j$
b) $r_i + r_j = 2r_k$
c) $r_i + r_j\zeta + r_k\zeta^2 = 0$, wobei $\zeta \in K$ die Gleichung $1 + \zeta + \zeta^2 = 0$ erfüllt, .

Für $\mathrm{char}(K) \neq 3$ sei $G(\mathcal{D}) = \frac{1}{3}(r_1 + r_2 + r_3)$ *der Schwerpunkt von $\mathcal{D}$.*

Satz 2.1.1. *Ein Polynom $P \in K[X]$ ist genau dann speziell, wenn es inseparabel ist oder eine nicht-triviale Symmetrie bezüglich des assoziierten Dreiecks $\mathcal{D}$ existiert, das heißt, eine affine Transformation*

$$\varphi \in \mathrm{Aff}(1) := \{f \colon K \to K, t \mapsto at + b,\ a, b \in K\},\ \varphi \neq id,$$

die sich auf ein Element der Symmetriegruppe von $\mathcal{D}$ einschränkt, also auf eine Permutation der Elemente von $\mathcal{D}$.

Beweis. "⇒" Die verschiedenen Fälle sind

a) P ist nicht separabel. Dann ist P nach Definition speziell.
b) Es gilt $3r_k = r_i + r_j + r_k$, also $r_k = G(\mathcal{D})$ für $\mathrm{char}(K) \neq 3$. Es existiert die Symmetrie

$$t \mapsto r_i + r_j - t,$$

die r_i und r_j vertauscht.
c) Es gilt

$$r_i - r_j = \zeta^2(r_j - r_k) = \zeta(r_k - r_i).$$

Damit existiert die zyklische Symmetrie

$$t \mapsto r_j + \zeta(t - r_i)$$

mit Ordnung 3.

"⇐" Der inseparable Fall ist offensichtlich richtig. Sei also $\mathcal{D}$ nun separabel. Dann besteht die Symmetriegruppe von $\mathcal{D}$, die symmetrische Gruppe $\mathcal{S}_3$, neben der Identität aus Spiegelungen der Ordnung 2 und Drehungen der Ordnung 3. Sei das nach Voraussetzung existierende $\varphi \in \mathrm{Aff}(1)$ zunächst eine Spiegelung, das heißt, ohne Einschränkung gilt

$$\begin{aligned}\varphi(r_1) =& ar_1 + b = r_2\\ \varphi(r_2) =& ar_2 + b = r_1\\ \varphi(r_3) =& ar_3 + b = r_3\end{aligned}$$

Nun gibt es folgende Fälle

(i) $a = 1$: Es folgt sofort $b = 0$ und damit ein Widerspruch zu $\varphi \neq id$.

(ii) $a \neq 0$: Es folgt $r_3 = \dfrac{b}{1-a}$ und $r_1(1-a)(1+a) = b(a+1)$. Es gibt nun die Fälle

  (1) $a \neq -1$: Es folgt $r_1 = r_2 = r_3 = \dfrac{b}{1-a}$, im Widerspruch zur Separabilität von P.

  (2) $a = -1$: Es folgt $r_1 + r_2 - 2r_3 = 0$.

Sei φ nun eine Drehung, also ohne Einschränkung

$$\begin{aligned}\varphi(r_1) =& ar_1 + b = r_2\\ \varphi(r_2) =& ar_2 + b = r_3\\ \varphi(r_3) =& ar_3 + b = r_1.\end{aligned}$$

Es folgt

$$r_1\left(1 - a^3\right) = b\left(a^2 + a + 1\right).$$

Wir betrachten die folgenden Fälle

(i) $a^3 \neq 1$: Es ergibt sich wiederum $r_1 = r_2 = r_3 = \dfrac{b}{1-a}$ im Widerspruch zur Separabilität von P.

(ii) $a = 1$: Für $\mathrm{char}(K) \neq 3$ folgt $b = 0$ im Widerspruch zu $\varphi \neq id$. Für $\mathrm{char}(K) = 3$ ergibt sich $r_1 + r_2 + r_3 = 0 = 3r_3$, also $r_1 + r_2 = 2r_3$.

(iii) $a = \zeta$ ist primitive dritte Einheitswurzel: Es ergibt sich jeweils $r_1 + \zeta r_2 + \zeta^2 r_3 = 0$.

Falls also eine affine Transformation existiert, die sich auf ein nichttriviales Element der Symmetriegruppe von $\mathcal{D}$ einschränkt, so ist $\mathcal{D}$ speziell. □

Bemerkung. Für $K = \mathbb{C}$ ist ein Dreieck $\mathcal{D} = \{r_1, r_2, r_3\}$ genau dann speziell, wenn es eine der folgenden Bedingungen erfüllt:

(i) $\mathcal{D}$ ist inseparabel

(ii) Für den Schwerpunkt $G(\mathcal{D}) = \dfrac{r_1 + r_2 + r_3}{3}$ gilt $G(\mathcal{D}) \in \mathcal{D}$.

(iii) $\mathcal{D}$ ist gleichseitig.

2.2. **Die Normalform einer kubischen Gleichung.** Dieses Kapitel stellt im Wesentlichen eine Ausarbeitung von [Rost] dar, das Ziel ist der Beweis des folgenden Satzes:

Satz 2.2.1. *Sei P ein nicht-spezielles kubisches Polynom in allgemeiner Normalform über einem Körper K. Dann existieren $\phi \in Aff(1)$, $\lambda \in K \setminus \{0\}$ und ein eindeutig bestimmter Parameter $t \in D_4(K)$ mit $(4t-1)(27t-7)^2 \neq 0$, sodass*

$$\lambda P \circ \phi = r^3 - r^2 + (9t-2)r - (4t-1).$$

Bemerkung. Der Parameter t bestimmt eine kubische Gleichung eindeutig bis auf affine Transformationen.

Vor dem Beweis des Satzes folgen zuerst noch ein paar Vorbemerkungen, die uns die Beweisführung erleichtern sollen. Es sei also $P(x) \in K[x]$ ein kubisches Polynom in allgemeiner Normalform. Dann ist $F := K[x]/(P(x))$ eine freie K-Algebra und in F gilt $P(x) = 0$. *Das charakteristische Polynom von x* sei das charakteristische Polynom der Multiplikation mit x, also der linearen Abbildung

$$\begin{aligned} m_x \colon F &\to F \\ a &\mapsto xa. \end{aligned}$$

Bezüglich der K-Basis $\{1, x, x^2\}$ von F hat die Darstellungsmatrix von m_x für $P(x) = x^3 + a_2x^2 + a_1x + a_0$ die Form

$$\begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$$

Das heißt, für das charakteristische Polynom von x gilt $\chi_x(r) = P(r)$. Es folgt

$$\begin{aligned} P(r) &= \chi_x(r) \\ &= r^3 + a_2r^2 + a_1r + a_0 \\ &=: r^3 - T(x)r^2 + Q(x)r - N(x), \end{aligned}$$

wobei $T(x)$ die Spur von x und $N(x)$ die Norm von x bezüglich der Erweiterung F/K ist. Falls x invertierbar ist, gilt für das charakteristische Polynom von x^{-1}

$$x^{-3} - T\left(x^{-1}\right)x^{-2} + Q\left(x^{-1}\right)x^{-1} - N\left(x^{-1}\right) = 0.$$

Dies führt durch Multiplikation mit $\dfrac{x^3}{N\left(x^{-1}\right)}$ zu

$$x^3 - \frac{Q\left(x^{-1}\right)}{N\left(x^{-1}\right)}x^2 + \frac{T\left(x^{-1}\right)}{N\left(x^{-1}\right)}x - \frac{1}{N\left(x^{-1}\right)} = 0.$$

Da nach Konstruktion das charakteristische Polynom von x auch das Minimalpolynom ist, folgt wegen der Multiplikativität der Normfunktion

$$Q(x) = \frac{T\left(x^{-1}\right)}{N\left(x^{-1}\right)} = T\left(x^{-1}\right) N(x).$$

Bemerkung. Sei F eine Erweiterung eines Körpers K vom Grad n, $x \in F$, und $\chi_x(r)$ das charakteristische Polynom von x. Dann gilt

$$\chi_{ax+b}(r) = 0 \Leftrightarrow \chi_x\left(\frac{r-b}{a}\right) = 0,\ b \in K, a \in K^*.$$

Beweis. Sei M_x die Darstellungsmatrix der Abbildung m_x. Dann gilt

$$\begin{aligned}
&\det(r\mathbb{1} - M_{ax+b}) \\
=&\det(r\mathbb{1} - (aM_x + b\mathbb{1})) \\
=&\det((r-b)\mathbb{1} - aM_x)) \\
=&a^n \det\left(\frac{r-b}{a}\mathbb{1} - M_x\right).
\end{aligned}$$

Es gilt also

$$\begin{aligned}
&\det(r\mathbb{1} - M_{ax+b}) = 0 \\
\Leftrightarrow &\det\left(\frac{r-b}{a}\mathbb{1} - M_x\right) = 0,
\end{aligned}$$

da nach Voraussetzung $a \in K^*$. □

Um kubische Polynome über einem gegebenen Körper K bis auf affine Transformationen zu bestimmen, reicht es also aus, charakteristische Polynome $P_x(r)$ von Elementen x aus kubischen Erweiterungen und affine Transformationen des Parameters x über K zu betrachten.

Definition 2. Sei V ein Vektorraum über einem Körper K. Eine Menge A heißt *affiner Raum bezüglich* V, falls eine Abbildung

$$\begin{aligned}
A \times V &\to A \\
(a, v) &\mapsto a + v
\end{aligned}$$

mit den folgenden Eigenschaften existiert:

a) $a + 0 = a$, für $0 \in V$ und für alle $a \in A$
b) Für je zwei $a, b \in A$ existiert genau ein $v \in V$ mit $a + v = b$
c) $a + (v + w) = (a + v) + w$ für alle $a \in A, v, w \in V$

Die *Dimension von* A ist definiert als die Dimension von

$$A - a_0 := \{a - a_0 \mid a \in A\}$$

als Untervektorraum von V für ein beliebiges $a_0 \in A$.

Um zu zeigen, dass ein nicht-spezielles kubisches Polynom P in die gewünschte Normalform transformiert werden kann, werden wir im Folgenden eine zu P und damit zu x assoziierte affine Gerade

$$l_x = \{f(x) + sg(x) \mid s \in K\}, f(x), g(x) \in K$$

konstruieren. Diese Gerade wird durch die Parameter $T(x), Q(x), N(x)$ der kubischen Gleichung bestimmt sein und die Eigenschaft

$$l_{ax+b} = al_x + b,\ a \in K^*, b \in K$$

besitzen. Jede affine Tansformation von x impliziert also die selbe Transformation jedes Punktes auf der assoziierten Geraden. Aus diesem Grund werden wir uns im Folgenden auf die Transformationen der Gerade beschränken und diese in eine Normalform bringen, die dann die gewünschte Normalform der kubischen Gleichung impliziert. Doch zuerst zur Konstruktion der affinen Gerade. Gesucht sind Funktionen $f, g\colon F \to K$ mit den Eigenschaften

$$\begin{aligned} f(ax+b) =& af(x) + b \\ g(ax+b) =& ag(x). \end{aligned}$$

Die Funktion f definiert also in Abhängigkeit von x einen Punkt auf der affinen Gerade, die Funktion g einen "Richtungsvektor", also ein Element des zugrunde liegenden Vektorraums, das invariant unter Translationen ist. Damit folgt wie gewünscht

$$l_{ax+b}(s) = f(ax+b) + sg(ax+b) = af(x) + b + sag(x) = al_x(s) + b.$$

Um die Parameter f und g definieren zu können, sind zunächst einige Rechnungen nötig. Zuerst bestimmen wir die Diskriminante von P in Abhängigkeit von x. Da x eine Nullstelle von P ist, erreichen wir mit der Transformation $r \mapsto r + x$, dass 0 eine der Nullstellen ist. Das Polynom hat nun die Form

$$\begin{aligned} P(r) &= r^3 + (3x - T(x))\, r^2 + (3x^2 - 2T(x)x + Q(x))r \\ &=: r^3 + \varphi(x)r^2 + \delta(x)r \end{aligned}$$

Dabei ist $\delta(x)$ gerade die Ableitung von $P(r)$ an der Stelle x. Für die Diskriminante des quadratischen Polynoms

$$r^2 + \varphi(x)r + \delta(x)$$

erhalten wir $(r_2 - r_3)^2 = \varphi(x)^2 - 4\delta(x)$. Wegen der Invarianz unter Translationen folgt für die Diskriminante des ursprünglichen Polynoms

$$\begin{aligned} \Delta(x) =& (x - r_2)^2 (x - r_3)^2 (r_2 - r_3)^2 \\ =& N\left((r_2 - r_3)^2\right) \\ =& N\left(\varphi(x)^2 - 4\delta(x)\right). \end{aligned}$$

Es zeigt sich, dass $\varphi(x)$ invariant unter Translationen ist:

$$\begin{aligned}\varphi(ax+b) &= 3(ax+b) - T(ax+b)\\ &= 3ax + 3b - aT(x) - 3b\\ &= a(3x - T(x))\\ &= a\varphi(x),\ a, b \in K,\ a \neq 0\end{aligned}$$

Damit folgt mit

$$A(x) := N(\phi(x)),$$

dass gilt $A(ax+b) = a^3 A(x)$. Da $\delta(x)$ über die Ableitung von P definiert ist, ist auch dieser Parameter invariant unter Translationen. Außerdem folgt wegen $\delta(x) = (x - r_2)(x - r_3)$, dass

$$\delta(ax) = (ax - ar_2)(ax - ar_3) = a^2\delta(x)$$

und mit $D(x) := T(\delta(x))$ auch $D(ax+b) = a^2 D(x)$. Man berechnet

$$\begin{aligned}D(x) &= T(\delta(x))\\ &= T\left(3x^2 - 2T(x)x + Q(x)\right)\\ &= 3T(x)^2 - 6Q(x) - 2T(x)^2 + 3Q(x)\\ &= T(x)^2 - 3Q(x)\end{aligned}$$

und

$$\begin{aligned}A(x) &= N(\phi(x))\\ &= 2T(x)^3 + 27N(x) - 9T(x)Q(x)\\ &= -3(T(x)Q(x) - 9N(x)) + 2T(x)\left(T(x)^2 - 3Q(x)\right).\end{aligned}$$

Mit $M(x) = T(x)Q(x) - 9N(x)$ folgt

$$A(x) = -3M(x) + 2T(x)D(x).$$

Bemerkung. Seien $r_1, r_2, r_3 \in \bar{K}$ die Nullstellen von $P(r) = P_x(r)$. Dann ist $P(r)$ genau dann speziell, wenn eine der folgenden Bedingungen erfüllt ist

a) $P(r)$ ist inseparabel
b) $D(x) = 0$
c) $A(x) = 0$.

Beweis. Es gilt

$$\begin{aligned}D(x) &= T(x)^2 - 3Q(x)\\ &= (r_1 + r_2 + r_3)^2 - 3(r_1r_2 + r_1r_3 + r_2r_3)\\ &= r_1^2 + r_2^2 + r_3^2 - r_1r_2 - r_1r_3 - r_2r_3\\ &= \left(r_1 + \zeta r_2 + \zeta^2 r_3\right)\left(r_1 + \zeta^2 r_2 + \zeta r_3\right),\end{aligned}$$

wobei ζ der Gleichung $\zeta^2+\zeta+1=0$ genügt. $D(x)=0$ gilt also genau dann, wenn das zu x assoziierte Dreieck gleichseitig ist. Außerdem gilt

$$\begin{aligned} A(x) &= -3M(x)+2T(x)D(x) \\ &= -3Q(x)T(x)+27N(x)+2T(x)D(x) \\ &= (2r_1-r_2-r_3)(2r_2-r_1-r_3)(2r_3-r_1-r_2). \end{aligned}$$

Es gilt also genau dann $A(x)=0$, wenn ein Punkt des zu x assoziierten Dreiecks der Schwerpunkt ist. Mit Satz 2.1.1 folgt die Behauptung. □

Da $P_x(r)$ nicht-speziell ist, können wir den ersten Parameter der gesuchten charakteristischen Gerade definieren:

$$g(x) = -\frac{A(x)}{D(x)}.$$

Es gilt wie gewünscht

$$g(ax+b) = -\frac{a^3A(x)}{a^2D(x)} = ag(x).$$

Für den Parameter $M(x)$ gilt

$$\begin{aligned} M(ax+b) =& a^3(T(x)Q(x)-9N(x))+2a^2b\left(T(x)^2-3Q(x)\right) \\ =& a^3M(x)+2a^2bD(x). \end{aligned}$$

Also folgt $\frac{M}{D}(ax+b) = a\frac{M}{D}(x)+2b$. Da für die Spur aber $T(ax+b) = aT(x)+3b$ gilt, ergibt sich

$$f(x) := T(x) - \frac{M(x)}{D(x)}$$

mit der gewünschten Eigenschaft $f(ax+b)=af(x)+b$.

Definition 3. Sei $x\in F,\ D(x)\neq 0$. Dann heißt

$$l_x(s) = f(x)+sg(x),\ s\in K$$

die *Basic Line* von x.

Bemerkung. Für $A(x)\neq 0$ ist die Basic Line eine wohldefinierte, zu dem Polynom P assoziierte affine Gerade.

Bemerkung. a) $3f(x)+g(x)=T(x)$

b) $2f(x)+g(x)=\frac{M(x)}{D(x)}$

Beweis. a)
$$\begin{aligned} 3f(x)+g(x) &= 3T(x)-3\frac{M(x)}{D(x)}-\frac{A(x)}{D(x)} \\ &= 3T(x)+\frac{A(x)}{D(x)}-2T(x)-\frac{A(x)}{D(x)} \\ &= T(x) \end{aligned}$$

b) $$2f(x) + g(x) = T(x) - \frac{T(x)D(x) - M(x)}{D(x)}$$
$$= \frac{M(x)}{D(x)}$$

□

Nun zum Beweis des Satzes.

Beweis. Sei $P(r) \in K[r]$ also ein nicht-spezielles kubisches Polynom, $F := K[r]/(P)$ und $x \in F$ mit $P(x) = 0$. Nach einer früheren Bemerkung ist P das charakteristische Polynom von x, also von der Form $\chi_x(r) = r^3 - T(x)r^2 + Q(x)r - N(x)$. Durch die affine Transformation $\phi(x) = \dfrac{x - f(x)}{g(x)}$ gelangt die Basic Line in die Form

$$f(\phi(x)) = 0,\ g(\phi(x)) = 1$$

Dies ergibt folgende Normalisierung der zu P assoziierten Parameter

$$T = 1,\ 9N - 4Q + 1 = 0$$

Mit der Wahl von $t := \dfrac{N+1}{4} \in K$ folgt

$$(T, Q, N) = (1, 9t - 2, 4t - 1),$$

das heißt, das Polynom P hat mit $\lambda := \dfrac{1}{g(x)^3}$ nun die Form

$$\lambda P(r) = r^3 - r^2 + (9t - 2)r - (4t - 1).$$

□

2.3. **Klassifikation.**

Satz 2.3.1 (Rost)**.** *Sei $P(r) \in K[r]$ ein nicht-spezielles kubisches Polynom mit dem assoziierten Dreieck $\mathcal{D} = \{x, r_2, r_3\}$. Dann ist die t-Invariante der Gleichung $P(r) = 0$ gegeben durch*

$$t = \frac{A(x)^2 - \Delta(x)}{4A(x)^2},\ \textit{falls}\ \operatorname{char}(K) \neq 2$$

und

$$t = 1 + \frac{D(x)^3}{A(x)^2},\ \textit{falls}\ \operatorname{char}(K) = 2$$

Beweis. Nach dem obigen Satz gelangt eine nicht-spezielle kubische Gleichung durch die affine Transformation

$$x \mapsto \frac{x - f(x)}{g(x)}$$

in die gewünschte Normalform. Für $\mathrm{char}(K) \neq 2$ gilt

$$\begin{aligned}
N\left(\frac{x-f(x)}{g(x)}\right) &= N\left(\frac{D(x)}{A(x)}\left(r_2+r_3-\frac{M(x)}{D(x)}\right)\right)\\
&= \frac{1}{A(x)^3}N(D(x)(r_2+r_3)-M(x)),\ \text{da } T = x+r_2+r_3\\
&= \frac{1}{A(x)^3}N\left(r_2^3+r_3^3-2xr_2^2-2xr_3^2-r_2r_3^2-r_2^2r_3+4xr_2r_3\right)\\
&= -\frac{1}{A(x)^3}N\left((2x-r_2-r_3)(r_2-r_3)^2\right)\\
&= -\frac{1}{A(x)^3}N(\varphi(x))N\left((r_2-r_3)^2\right)\\
&= -\frac{\Delta(x)}{A(x)^2}
\end{aligned}$$

Mit Koeffizientenvergleich folgt

$$N\left(\frac{x-f(x)}{g(x)}\right) = 4t-1$$

und damit

$$t = \frac{-\dfrac{\Delta(x)}{A(x)^2}+1}{4} = \frac{A(x)^2-\Delta(x)}{4A(x)^2}.$$

Für $\mathrm{char}(K) = 2$ gilt

$$\begin{aligned}
Q\left(\frac{x-f(x)}{g(x)}\right) &= \frac{D(x)^2}{A(x)^2}Q(x-f)\\
&= \frac{D(x)^2}{A(x)^2}\left(Q(x)+f(x)^2\right)\\
&= \frac{D(x)^3+M(x)^2}{A(x)^2}\\
&= 1+\frac{D(x)^3}{A(x)^2},
\end{aligned}$$

da mit $A(x) = -3M(x)+2T(x)D(x)$ auch $A(x) = M(x)$ gilt. Mit Koeffizientenvergleich folgt

$$Q\left(\frac{x-f(x)}{g(x)}\right) = 9t-2 = t.$$

□

Sei nun $\mathrm{char}(K) \neq 2,3$. Dann gelangt die kubische Gleichung mit der Transformation $r \mapsto 3r-1$ in die Form

$$r^3-3(7-27t)r+7-27t = 0.$$

Diese Gleichung hat die Diskriminante $3^6(7-27t)^2(1-4t)$, folglich hat eine kubische Gleichung in Normalform die Diskriminante

$$\Delta = (7-27t)^2(1-4t).$$

Mit Hilfe der Cardanischen Formel lassen sich nun die Nullstellen durch Radikale ausdrücken. Für $y = u + v$ ergibt sich $y^3 = 3uvy + u^3 + v^3$. Vergleicht man die Koeffizienten mit denen der ursprünglichen Gleichung, erhält man mit $D := 7 - 27t$ die Gleichungen $uv = D$ und damit $u^3v^3 = D^3$ und $u^3 + v^3 = -D$. Nach dem Satz von Vieta sind u^3 und v^3 die Nullstellen der quadratischen Gleichung

$$z^2 + Dz - D^3 = 0.$$

Man erhält die Lösungen

$$u^3 = D\left(\frac{-1+\sqrt{1-4D}}{2}\right) =: D\omega$$

und

$$v^3 = D\left(\frac{-1-\sqrt{1-4D}}{2}\right) =: D\bar{\omega}.$$

Wegen $D = \omega\bar{\omega}$ folgt $u = \sqrt[3]{\omega^2\bar{\omega}} =: \alpha$ und $v = \sqrt[3]{\omega\bar{\omega}^2} =: \bar{\alpha}$. Es gilt also $y = \alpha + \bar{\alpha}$ und damit

$$\begin{aligned} x =& \frac{1+\alpha+\bar{\alpha}}{3} \\ =& \frac{1}{6}\left(2 - \sqrt[3]{(1-E)\left(1+\sqrt{E}\right)} - \sqrt[3]{(1-E)\left(1-\sqrt{E}\right)}\right), \end{aligned}$$

wobei $E = 1 - 4D = 27(4t-1)$.

Korollar 2.3.2. *Sei $P(r) \in K[r]$ ein kubisches Polynom und $x \in K[r]/(P(r))$ mit $P(x) = 0$ und $D(x), A(x) \neq 0$. Dann lässt sich die Gleichung $P(r) = 0$ durch eine affine Transformation über K in eine der folgenden Normalformen bringen:*

a) $(4t-1)(27t-7) \neq 0$, *falls $r_i \neq r_j$ für $i \neq j$*

b) $t = \frac{1}{4}$, *falls P eine doppelte Nullstelle besitzt und* $\mathrm{char}(K) \neq 2$

c) $t = \frac{7}{27}$, *falls P eine dreifache Nullstelle besitzt und* $\mathrm{char}(K) \neq 3$

Beweis. a) Dies zeigt Satz 2.2.1.

b) Wir betrachten eine Gleichung der Form

$$P(r) = (r-r_1)^2(r-r_2) = 0,\ r_1 \neq r_2.$$

Wegen $A(r_1) = 2(r_2-r_1)^3 \in K$ und $D(r_1) = (r_2-r_1)^2 \in K$ folgt auch $r_2 - r_1 \in K$ und mit $T(r_1) = 2r_1 + r_2 \in K$ auch $r_1, r_2 \in K$. Damit kann die Gleichung durch die Transformation

$$r \mapsto 2(r_1 - r_2)r + r_2$$

in die Form

$$r\left(r-\frac{1}{2}\right)^2 = r^3 - r^2 + \frac{1}{4}r = 0$$

gebracht werden. Für $\mathrm{char}(K) = 2$ gilt mit der Existenz einer doppelten Nullstelle auch $A = 0$.

c) Wir betrachten eine Gleichung der Form

$$P(r) = (r - r_1)^3 = 0.$$

Wegen $\mathrm{char}(K) \neq 3$ folgt mit $T(r_1) = 3r_1 \in K$ auch $r_1 \in K$. Damit kann die Gleichung durch die Transformation

$$r \mapsto 3r_1 r$$

in die Form

$$\left(r-\frac{1}{3}\right)^3 = r^3 - r^2 + \frac{1}{3}r - \frac{1}{27} = 0$$

gebracht werden. Für $\mathrm{char}(K) = 3$ gilt mit der Existenz einer dreifachen Nullstelle auch $D = 0$.

□

Beispiel. Gegeben sei die reelle kubische Gleichung

$$P(r) = \chi_x(r) = r^3 - (-1)r^2 + (-2)r = r(r-1)(r+2) = 0.$$

Man berechnet $f = -\frac{9}{7}$ und $g = \frac{20}{7}$ (siehe Grafik 1). Nun wählt man die Koordinaten $f = 0$ und $g = 1$ (siehe Grafik 2) mit Hilfe der Transformation

$$\phi\colon x \mapsto \frac{x-f}{g} = \frac{7}{20}x + \frac{9}{20}.$$

Man erhält

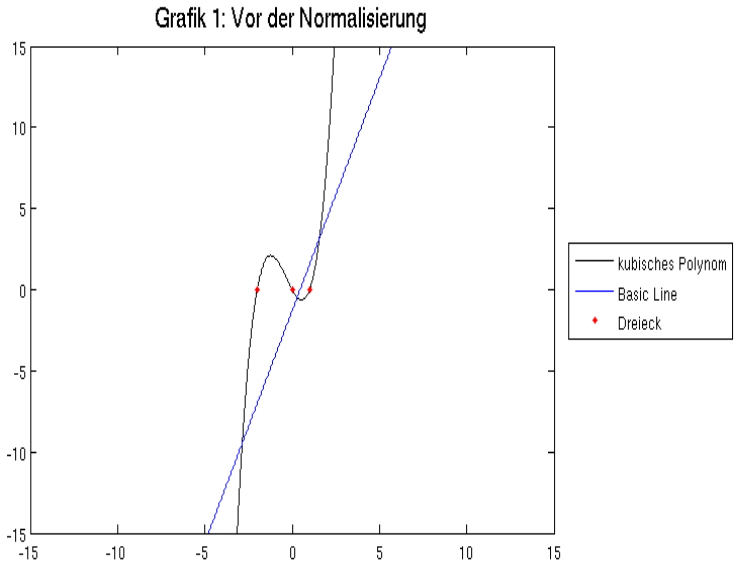
$$\begin{aligned} &\chi_{\phi(x)}(r) = 0 \\ \Leftrightarrow\ &\chi_x\left(\phi^{-1}(r)\right) = 0 \\ \Leftrightarrow\ &r^3 - r^2 + \frac{19}{400}r + \frac{9}{100} = 0 \end{aligned}$$

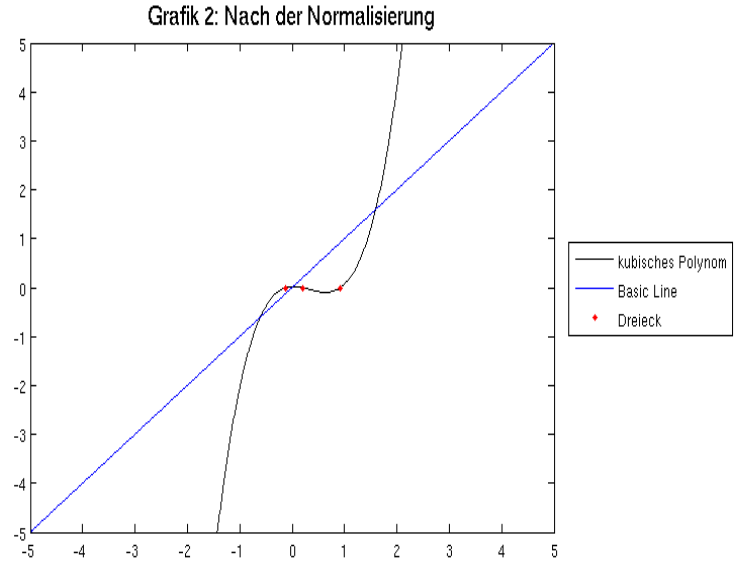
das heißt, für die charakteristische Invariante t gilt

$$t = \frac{\frac{9}{100}+1}{4} = \frac{91}{400}$$

oder mit $A(x) = -20$ und $\Delta(x) = -12$ auch

$$t = \frac{A(x)^2 - \Delta(x)}{4A^2} = \frac{91}{400}.$$





2.4. **Charakteristische Fixpunkte.** Im Folgenden soll noch eine weitere Möglichkeit diskutiert werden, um kubische Gleichungen zu normieren. Anstelle der rechnerisch motivierten Parameter f und g werden wir im Fall $\mathrm{char}(K) \neq 2, 3$ eine kubische Gleichung mit Hilfe charakteristischer Fixpunkte normieren.

Bemerkung. Für eine nicht-spezielle kubische Gleichung

$$P(r) = (r - r_1)(r - r_2)(r - r_3) = 0$$

mit dem assoziierten Dreieck $\mathcal{D} = (r_1, r_2, r_3)$ und der Basic Line l_x existiert der Schwerpunkt $G(\mathcal{D}) = \frac{1}{3}(r_1 + r_2 + r_3)$. Dieser liegt wegen

$$G(\mathcal{D}) = \frac{T(x)}{3} = f(x) + \frac{1}{3}g(x)$$

auf der assoziierten Basic Line.

Um einen weiteren charakteristischen Punkt auf der Basic Line zu bestimmen, brauchen wir zuerst eine Aussage aus der rationalen Geometrie:

Definition 4. Sei A eine affine Gerade über einem Körper K. Für zwei Punkte $u, v \in A,\ u \neq v$, definieren wir die Abbildung

$$r_{u,v} \colon A \setminus \{u\} \to A \setminus \{u\}$$
$$t \mapsto u + \frac{(v-u)^2}{t-u}$$

Wir bezeichnen $r_{u,v}$ als *Spiegelung an v mit Pol u.*

Die Abbildung ist wohldefiniert, da die Differenzen $v-u, t-u$, nach der Definition einer affinen Geraden, in K liegen und damit auch der Quotient $\frac{(v-u)^2}{t-u}$. Die Fixpunkte dieser Abbildung sind v und $2u-v$. Es ist leicht nachzurechnen, dass $r_{u,v} = r_{u,2u-v}$ gilt. Der gesuchte zweite charakteristische Punkt einer kubischen Gleichung ergibt sich aus dem folgenden Lemma. Dazu definieren wir analog zu dem assoziierten Dreieck einer kubischen Gleichung für ein Dreieck $\mathcal{D} = \{r_1, r_2, r_3\}$ auf einer beliebigen affinen Geraden die Parameter

$$\begin{aligned} T(\mathcal{D}) :=& r_1 + r_2 + r_3 \\ Q(\mathcal{D}) :=& r_1r_2 + r_1r_3 + r_2r_3 \\ N(\mathcal{D}) :=& r_1r_2r_3. \end{aligned}$$

Lemma 2.4.1. *Sei A eine affine Gerade über einem Körper K, mit* $\mathrm{char}(K) \neq 2, 3$. *Außerdem sei $\mathcal{D} = \{t_1, t_2, t_3\}$ ein nicht-spezielles Dreieck in A und $G(\mathcal{D})$ der Schwerpunkt von $\mathcal{D}$. Dann existiert ein eindeutiger Punkt $R(\mathcal{D}) \in A$ mit $R(\mathcal{D}) \neq G(\mathcal{D})$ und $R(\mathcal{D}) \notin \mathcal{D}$ mit*

$$G(r_{R(\mathcal{D}),G(\mathcal{D})}(\mathcal{D})) = G(\mathcal{D}).$$

Das heißt, wenn wir das Dreieck $\mathcal{D}$ an seinen Schwerpunkt mit Pol $R := R(\mathcal{D})$ spiegeln, dann ist der Schwerpunkt des resultierenden Dreiecks der Schwerpunkt von $\mathcal{D}$. Wir nennen R den *Spiegelungspol von $\mathcal{D}$.*

Beweis. Mit einer geeigneten Koordinatenwahl auf der affinen Geraden kann ohne Einschränkung angenommen werden, dass $G(\mathcal{D}) = 0$ gilt.

Da 3 invertierbar ist, ist dies äquivalent zu $T(\mathcal{D}) = r_1 + r_2 + r_3 = 0$. Der gesuchte Punkt R muss also die folgende Gleichung erfüllen:

$$\begin{aligned}
&\sum_{i=1}^{3} R + \frac{R^2}{r_i - R} = 3R + R^2 \sum_{i=1}^{3} \frac{1}{r_i - R} = 0 \\
\Leftrightarrow\ & 3R(r_1 - R)(r_2 - R)(r_3 - R) + R^2 \left(Q(\mathcal{D}) + 3R^2\right) \\
=\ & 3RN(\mathcal{D}) - 2R^2 Q(\mathcal{D}) = 0
\end{aligned}$$

Es ergeben sich nun die folgenden Fälle:

a) $N(\mathcal{D}) = 0$: Mit $N(\mathcal{D}) = r_1 r_2 r_3$ ergibt sich ein Widerspruch zur Separabilität von $\mathcal{D}$.
b) $Q(\mathcal{D}) = 0$: Da nach Koordinatenwahl $T(\mathcal{D}) = 0$ gilt, folgt ebenfalls
$$D(\mathcal{D}) = T(\mathcal{D})^2 - Q(\mathcal{D}) = 0,$$
im Widerspruch dazu, dass $\mathcal{D}$ nicht speziell ist.
c) $N(\mathcal{D}) \neq 0, Q(\mathcal{D}) \neq 0$: Wegen $R \neq G(\mathcal{D}) = 0$ folgt
$$R = \frac{3N(\mathcal{D})}{2Q(\mathcal{D})}.$$

Damit folgt die Eindeutigkeit des gesuchten Punktes. Für die Existenz bleibt nur noch zu prüfen, dass $R \notin \mathcal{D}$. Nehmen wir also an, es gilt $R = r_1$. Dann folgt nach der obigen Rechnung

$$\begin{aligned}
0 =& 3R^2 + Q(\mathcal{D}) \\
=& 2r_1^2 - r_1 r_3 - r_3^2, \text{ da } r_1 + r_2 + r_3 = 0 \\
=& (r_1 - r_3)(2r_1 + r_3) \\
=& (r_1 - r_3)(r_1 - r_2),
\end{aligned}$$

im Widerspruch zur Separabilität von $\mathcal{D}$. Damit ist auch die Existenz des gesuchten Punktes $R(\mathcal{D})$ gezeigt. □

Korollar 2.4.2. *Sei K ein Körper, $\bar{K}$ ein algebraischer Abschluss und $P(r) \in K[r]$ ein nicht-spezielles kubisches Polynom mit*

$$P(r) = r^3 - T(x)r^2 + Q(x)r - N(x) = (r - r_1)(r - r_2)(r - r_3) \in \bar{K}[r],$$

also mit dem assoziiertem Dreieck $\mathcal{D} = (r_1, r_2, r_3)$. Außerdem seien $l_x^{\bar{K}}(s)$ und $l_x^K(s)$ die assoziierten Basic Lines über dem jeweiligen Körper. Dann gilt für den Spiegelungspol des Dreiecks

$$R(\mathcal{D}) = \frac{M(x)}{2D(x)} \in l_x^K.$$

Beweis. Das Dreieck $\mathcal{D}$ liegt auf der Basic Line $l_x^{\bar{K}}$. Also existiert nach Lemma 2.4.1 der Spiegelungspol $R(x) := R(\mathcal{D})$, der sich ebenfalls auf

$l_x^{\bar{K}}$ befindet. Durch die Transformation $x \mapsto x - \frac{T(x)}{3}$ folgt für den Schwerpunkt $G(\mathcal{D}) = 0$. Nach dem Beweis von Lemma 2.4.1. folgt

$$\begin{aligned} R\left(x - \frac{T(x)}{3}\right) =& \frac{3N(x)}{2Q(x)} \\ =& \frac{3N(\varphi(x))}{3T(x)^2 + 9Q(x)} \\ =& \frac{-A(x)}{6D(x)} \end{aligned}$$

Da $R\left(x - \frac{T(x)}{3}\right)$ auf der Basic Line $l_x^{\bar{K}}$ liegt, erhalten wir

$$\begin{aligned} R(x) =& R\left(x - \frac{T(x)}{3}\right) + \frac{T(x)}{3} \\ =& \frac{T(x)}{3} - \frac{A(x)}{2D(x)} \\ =& \frac{M(x)}{2D(x)}. \end{aligned}$$

Mit

$$\frac{M(x)}{2D(x)} = f(x) + \frac{1}{2}g(x)$$

folgt auch $R(\mathcal{D}) \in l_x^K$. □

Nun ist für $\mathrm{char}(K) = 2, 3$ jeweils einer der beiden Fixpunkte $G(\mathcal{D})$ und $R(\mathcal{D})$ nicht definiert. Eine Charakteristik-unabhängige Darstellung der Basic Line erhalten wir durch die Transformation $\psi(x) = 2x - T(\mathcal{D})$. Es gilt

$$\begin{aligned} \psi(R(\mathcal{D})) =& f(x) \\ \psi(G(\mathcal{D})) =& G(\mathcal{D}). \end{aligned}$$

Mit $f(x) - G(\mathcal{D}) = \frac{1}{3}g(x)$ erhalten wir wieder die erste, charakteristikfreie Darstellung der Basic Line als

$$l_x(s) = f(x) + sg(x),\ s \in K.$$

Wir erhalten außerdem, wie schon im Beweis von Korollar 4.2.2. erwähnt, die Relationen

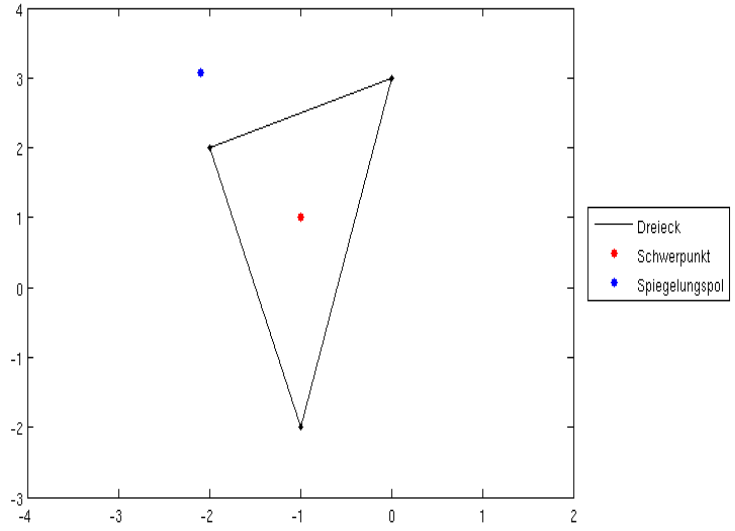
$$R = f + \frac{1}{2}g$$

und

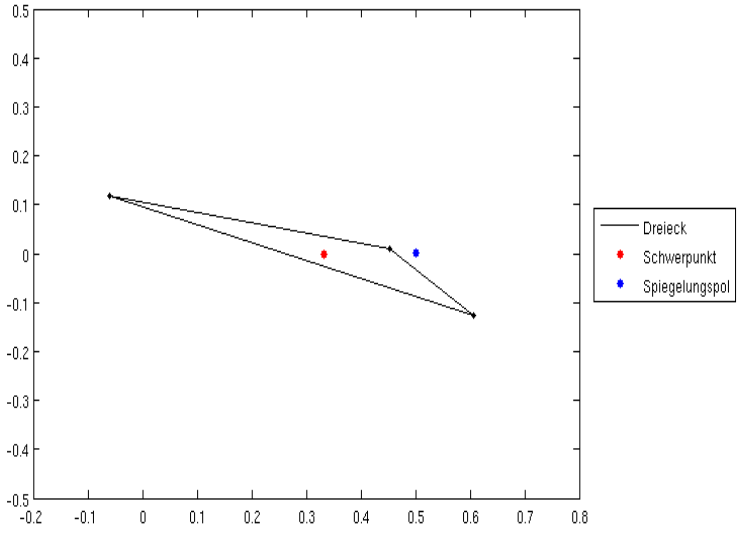
$$G = f + \frac{1}{3}g.$$

Die für die Normalform einer kubischen Gleichung verwendeten Normalisierungen $f = 0$ und $g = 1$ sind für $\mathrm{char}(K) \neq 2, 3$ also äquivalent zu der Koordinatenwahl $R = \frac{1}{2}$ und $G = \frac{1}{3}$ der Fixpunkte.

Grafik 3: Vor der Normalisierung



Grafik 4: Nach der Normalisierung



Beispiel. Sei $K = \mathbb{C}$ und $\mathcal{D} = (2+3i, -4+2i, -1-2i)$ ein Dreieck. Die assoziierte kubische Gleichung ist

$$r^3 - (-3+3i)r^2 + (-2-9i)r - (-2+36i) = 0.$$

Für die Fixpunkte erhalten wir $G = -1+i$ und $R = -2.0946+3.0676i$ (siehe Grafik 4). Mit den Koordinatenwahlen $G = \frac{1}{3}$ und $R = \frac{1}{2}$ gelangt die Gleichung in Normalform mit $t = 0,2474 + 0,0088i$ (siehe Grafik 4).

Im folgenden Kapitel werden wir die Normalisierung einer elliptischen Kurve auf die Normalisierung einer assoziierten kubischen Gleichung zurückführen. Die gesuchte Normalform folgt dann aus einer geschickten Koordinatenwahl der Basic Line, also durch Fixieren der charakteristischen Punkte R und G.

3. Elliptische Kurven

3.1. **Grundlagen.** Die folgenden Grundlagen orientieren sich in Inhalt und Notation an [Sil1986].

Definition 5. ([Sil1986])

a) Eine *elliptische Kurve* ist ein Paar $(E, \mathcal{O})$, wobei E eine Kurve, also eine glatte projektive Varietät der Dimension 1 vom Geschlecht 1 ist und $\mathcal{O} \in E$. Eine elliptische Kurve heißt über einem Körper K definiert, falls sie als Varietät über K definiert ist (wir schreiben im Folgenden E/K).

b) Eine Kurve heißt *Weierstraß-Kurve*, wenn sie Nullstellenmenge eines homogenen Polynoms der Form

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

in $K\mathbb{P}^2$ ist.

c) Für eine projektive Kurve C, definiert über einem Körper K, sei $I(C)$ das Ideal, das von der Menge

$$\{f \in K[X],\ f \text{ ist homogen und } f(P) = 0 \text{ für alle } P \in C\}$$

erzeugt wird. Der Quotient $K[C] := K[X]/I(C)$ heißt der *affine Koordinatenring von* C, der Quotientenkörper $K(C)$ heißt *Funktionenkörper von* C.

Im Folgenden werden wir für eine Weierstraß-Kurve auch die nichthomogene Notation

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

verwenden. Wir nennen eine Weierstraß-Kurve C *glatt*, falls sie keinen singulären Punkt besitzt, das heißt, es existiert kein Punkt $P \in C$ mit

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = 0.$$

Um die Definition einer elliptischen Kurve mit der einer Weierstraß-Kurve zu verbinden, werden wir zeigen, dass zu jeder elliptischen Kurve eine (allerdings nicht notwendigerweise eindeutige) Weierstraß-Kurve gefunden werden kann. Umgekehrt ist jede glatte Weierstraß-Kurve eine elliptische Kurve.

Satz 3.1.1. ([Sil1986] S.63ff) *Sei E eine elliptische Kurve über einem gegebenen Körper K. Dann gilt*

a) *Es gibt Funktionen $x, y \in K(E)$, sodass die Abbildung*

$$\phi\colon E \to \mathbb{P}^2$$
$$P \mapsto [x(P), y(P), 1]$$

einen Isomorphismus von E auf eine Weierstraß-Kurve C induziert. Insbesondere gilt $\phi(\mathcal{O}) = [0,1,0]$.

b) *Je zwei Weierstraß-Kurven C_1, C_2 zu E wie in a) lassen sich durch eine affine Transformation*

$$x \mapsto u^2x + r$$
$$y \mapsto u^3y + su^2x + t$$

mit $u, r, s, t \in K, u \neq 0$, ineinander überführen.

c) *Jede glatte Weierstraß-Kurve ist eine elliptische Kurve mit dem ausgezeichneten Punkt $\mathcal{O} = [0, 1, 0]$.*

Beweis. a) Sei

$$V_n := \{f \in K(E)^* \mid \mathrm{ord}_{\mathcal{O}}(f) \geq -n,\ \mathrm{ord}_x(f) \geq 0, \text{für alle } x \in E \setminus \mathcal{O}\},$$

$n \in \mathbb{N} \cup \{0\}$, der $\bar{K}$-Vektorraum der Funktionen auf E, die außer bei $\mathcal{O}$ regulär sind und bei $\mathcal{O}$ einen Pol von maximal Ordnung n haben. Aus dem Riemann-Roch-Theorem folgt, dass $dim_{\bar{K}}V_n = n$ für $n \geq 1$ und $dim_{\bar{K}}V_0 = 1$. Da V_0 und V_1 eindimensional sind und V_0 die konstanten Funktionen enthält, folgt, dass es auf E keine Funktionen gibt, die an $\mathcal{O}$ einen Pol mit Ordnung 1 besitzen. Wähle ein $x \in V_2$ mit $\mathrm{ord}_{\mathcal{O}}x = -2$ und ein $y \in V_3$ mit $\mathrm{ord}_{\mathcal{O}}y = -3$, sodass $\{1, x\}$ und $\{1, x, y\}$ Basen von V_2 beziehungsweise V_3 sind. In V_6 sind also die sieben Funktionen $1, x, y, x^2, xy, y^2, x^3$ enthalten. Wegen $dim_{\bar{K}}V_6 = 6$ existert also eine nicht-triviale Linearkombination

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

mit $A_i \in K,\ i = 1, ..., 7$. Es gilt $A_6A_7 \neq 0$ da sonst alle Terme der Linearkombination eine verschiedene Polordnung an $\mathcal{O}$ hätten und somit $A_1 = ... = A_7 = 0$ gelten müsste. Durch die Transformation $(x, y) \mapsto (-A_6A_7x, A_6A_7^2y)$ und Teilen der Gleichung durch $A_6^3A_7^4$ ergibt sich eine Weierstraß-Kurve C. Die gewünschte Abbildung ist also

$$\phi\colon E \to \mathbb{P}^2$$
$$P \mapsto [x(P), y(P), 1]$$

$\phi\colon E \to C$ ist surjektiv und ein Morphismus ([Sil1986] S.23f). Es gilt

$$\phi(\mathcal{O}) = [x(\mathcal{O}), y(\mathcal{O}), 1] = \left[\frac{x}{y}(\mathcal{O}), \frac{y}{y}(\mathcal{O}), \frac{1}{y}(\mathcal{O})\right] = ([0, 1, 0]).$$

Zu zeigen bleibt, dass C glatt ist und ϕ tatsächlich einen Isomorphismus von E auf C liefert. Diese Punkte sollen hier nicht mehr ausgeführt werden.

b) Seien $\{x, y\}$ und $\{x', y'\}$ zwei Paare von Weierstraß-Koordinatenfunktionen für E. Wegen $\mathcal{O} = [0, 1, 0]$ muss gelten $\mathrm{ord}_{\mathcal{O}}y < 0$ und $\mathrm{ord}_{\mathcal{O}}y < \mathrm{ord}_{\mathcal{O}}x$. Wie der Ordnungsbetrachtung aus a) folgt nun $\mathrm{ord}_{\mathcal{O}}y^2 = \mathrm{ord}_{\mathcal{O}}x^3$. Also besitzen x, y an $\mathcal{O}$ die Ordnungen -2

beziehungsweise -3. Damit sind $\{1, x\}$ und $\{1, x'\}$ Basen für V_2 und ebenso $\{1, x, y\}$ und $\{1, x', y'\}$ Basen für V_3. Es existieren also Linearkombinationen der Form

$$x = u_1 x' + r \text{ und } y = u_2 y + s_2 x' + t,$$

mit $u_1, u_2, r, s_2, t \in K$, mit $u_1 u_2 \neq 0$. Da die Koeffizienten von X^3 und Y^2 in Weierstraß-Gleichungen jeweils 1 sind, folgt $u_1^3 = u_2^2$. Mit $u = \frac{u_2}{u_1}$ und $s = \frac{s_2}{u^2}$ folgt die Behauptung.

c) Dies soll hier nicht bewiesen werden.

□

Im Folgenden soll nun die j-Invariante eingeführt werden, die eine elliptische Kurve E bis auf Isomorphie (über einem algebraischen abgeschlossenen Körper) eindeutig charakterisiert. Dazu betrachten wir zunächst den Fall $\text{char}(K) \neq 2, 3$ und orientieren uns wieder an [Sil1986] S.46f. Eine Weierstraß-Kurve kann hier durch die Transformation $y \mapsto \frac{y - a_1 x - a_3}{2}$ in die Form

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

gebracht werden, wobei

$$\begin{aligned} b_2 &= a_1 + 4a_2 \\ b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

Mit der zweiten Transformation $(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ erhält man die Form

$$E : y^2 = x^3 - 27c_4 - 54c_6$$

mit den Parametern

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6. \end{aligned}$$

Nun können wir mit $b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$ die Diskriminante und die j-Invariante einer elliptischen Kurve einführen:

$$\begin{aligned} \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\ j &= \frac{c_4^3}{\Delta} \end{aligned}$$

Für $\text{char}(K) = 2$ erhalten wir die Parameter

$$\begin{aligned} \Delta &= a_6 \\ j &= \frac{1}{a_6} \end{aligned}$$

und für $\mathrm{char}(K) = 3$

$$\Delta = -a_2^3 a_6$$
$$j = \frac{-a_2^3}{a_6}.$$

Proposition 3.1.2. ([Sil1986] S.50ff)

a) Eine Weierstraß-Kurve C ist genau dann glatt, wenn $\Delta(C) \neq 0$.
b) Zwei elliptische Kurven E_1, E_2 über einem Körper K sind genau dann isomorph über $\bar{K}$, wenn gilt $j(E_1) = j(E_2)$.
c) Sei $j_0 \in \bar{K}$. Dann existiert eine elliptische Kurve E über $K(j_0)$ mit $j(E) = j_0$.

Beweis. Es soll an dieser Stelle nur Teil c) bewiesen werden.

c) Sei $j_0 \neq 0, 1728$. Dann erfüllt

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

die Bedingungen $j(E) = j_0$ und $\Delta(E) = \dfrac{j_0^2}{(j_0 - 1728)^3} \neq 0$. Für die beiden Ausnahmefälle finden sich die Kurven

$$E_1\colon y^2 + y = x^3, \Delta(E) = -27,\ j(E) = 0,$$
$$E_2\colon y^2 = x^3 + x, \Delta(E) = -64,\ j = 1728.$$

In Charakteristik 2 oder 3 gilt $1728 = 2^6 3^3 = 0$, deshalb ist in beiden Fällen enweder E_1 oder E_2 die gesuchte Kurve. □

3.2. **Die Normalform einer elliptischen Kurve.**

Definition 6. Die Weierstraß-Kurve zu der Gleichung

$$F(j, a) = \frac{Y^2Z - XYZ - aX^2Z}{4a + 1} - X^3 + \frac{36X + Z}{j - 1728}Z^2,$$

mit $a \in D_4(K), j \in K \setminus \{0, 1728\}$ heißt die *Normalform* $E(j, a)$ der zugehörigen elliptischen Kurve E mit $j = j(E)$.

Lemma 3.2.1. *Sei E eine elliptische Kurve über einem Körper K, $j(E) \neq 0, 1728$. Dann existieren ein homogenes Polynom*

$$f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

$a_i \in K$, sodass $f(X, Y, Z) = 0$ eine Weierstraß-Kurve zu E ist, eine affine Transformation $\phi \in Gl(3, K)$ und $\lambda \in K$, mit

$$\lambda f \circ \phi = Y^2Z - XYZ - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

Beweis. Nach Satz 3.1.1.a) existiert eine Funktion

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

$a_i \in K$ derart, dass $f(X,Y,Z) = 0$ eine Weierstraß-Kurve zu E ist. Die gewünschte Gleichung $a_1 = -1$ wird für $a_1 \neq 0$ durch die Transformation $X \mapsto \frac{X}{a_1}$ und für $a_1 = 0$ und $\mathrm{char}(K) \neq 2$ durch $Y \mapsto Y - \frac{X}{2}$ erreicht. Für $\mathrm{char}(K) = 2$ gilt $j = \frac{a_1^{12}}{\Delta(E)}$. Da nach Voraussetzung $j \neq 0$ ist, gilt also auch $a_1 \neq 0$. Die zweite Gleichung $a_3 = 0$ kann nun mit der Verschiebung $X \mapsto X - a_3Z$ erreicht werden. □

Satz 3.2.2. *Sei E eine elliptische Kurve über einem Körper K, $j(E) \neq 0, 1728$. Dann existieren ein homogenes Polynom*

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

$a_i \in K$, sodass $f(X,Y,Z) = 0$ eine Weierstraß-Kurve zu E ist, eine affine Transformation $\phi \in Gl(3,K), a \in D_4(K), \lambda \in K$, mit

$$\lambda f \circ \phi = F(j,a).$$

Beweis. Nach Satz 3.1.1.a) existiert eine Funktion

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

$a_i \in K$ derart, dass $f(X,Y,Z) = 0$ eine Weierstraß-Kurve zu E ist. Nach Lemma 3.2.1. kann f so gewählt werden, dass gilt $a_1 = -1$ und $a_3 = 0$. Die Ableitung von f nach Y ist

$$f_Y = 2YZ - XZ = Z(2Y - X) =: Zg(X,Y).$$

Die Gleichung $g = 0$ definiert also eine Gerade L. Nach dem Gruppengesetz für eine elliptische Kurve E ist der zu einem gegebenen Punkt $P_0 = (x_0, y_0)$ inverse Punkt von der Form $-P_0 = (x_0, -y_0 + x_0)$. Die 2-Torsionspunkte erfüllen also die Gleichung $2y_0 = x_0$, das heißt, sie liegen gerade auf der Geraden L. Wir betrachten nun die Einschränkungen der Ableitungen von f nach X und Z auf L:

$$\begin{aligned}
f_X &= -YZ - 3X^2 - 2a_2XZ - a_4Z^2 \\
&= -YZ - 12Y^2 - 4a_2YZ - a_4Z^2 \\
&= -12Y^2 - (1 + 4a_2)YZ - a_4Z^2 \\
f_Z &= Y^2 - XY - a_2X^2 - 2a_4XZ - 3a_6Z^2 \\
&= -Y^2 - 4a_2Y^2 - 4a_4YZ - 3a_6Z^2 \\
&= -(1 + 4a_2)Y^2 - 4a_4YZ - 3a_6Z^2
\end{aligned}$$

Betrachtet man nun eine Linearkombination h von f_X und f_Z, die linear in Y ist, so definiert $h = 0$ einen eindeutigen Punkt $C(E)$, der

unabhängig ist von der Wahl von h.

$$\begin{aligned} h =& -12f_Z + (1+4a_2)f_X \\ =& -48a_4YZ - 36a_6Z^2 + (4a_2+1)^2YZ + (4a_2+1)a_4Z^2 \\ =& YZ\left((4a_2+1)^2 - 48a_4\right) + a_4(4a_2+1) - 36a_6Z^2 = 0 \end{aligned}$$

Für $\mathrm{char}(K) \neq 2,3$ gilt $(4a_2+1)^2 - 48a_4 = c_4 \neq 0$, da nach Voraussetzung $j(E) = \dfrac{c_4^3}{\Delta} \neq 0$. Ebenso folgt für $\mathrm{char}(K) = 3$, dass $(4a_2+1)^2 - 48a_4 = 4a_2 + 1 = b_2 \neq 0$, da $j(E) = \frac{b_2^2}{\Delta}$ und im Fall $\mathrm{char}(K) = 2$ gilt $(4a_2+1)^2 - 48a_4 = 1 \neq 0$. Also folgt in jeder Charakteristik

$$C = C(E) = \left[2\frac{-a_4(4a_2+1) + 36a_6}{(4a_2+1)^2 - 48a_4}, \frac{-a_4(4a_2+1) + 36a_6}{(4a_2+1)^2 - 48a_4}, 1\right].$$

Nun erreicht man durch die Transformation

$$X \mapsto X - X(C),\ Y \mapsto Y - Y(C),$$

dass $X(C) = Y(C) = 0$. Wir bezeichnen die daraus resultierende elliptische Kurve wieder mit

$$E : Y^2Z - XYZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Die Parameter der Kurvengleichung erfüllen nach der Verschiebung von $C(E)$ die Gleichung $a_4(4a_2+1) = 36a_6$. Es gilt $(4a_2+1) \neq 0$, da sonst auch $a_6 = 0$ und damit $j = 1728$ gelten würde. Also folgt

$$E : Y^2Z - XYZ = X^3 + a_2X^2Z + \frac{36a_6}{4a_2+1}XZ^2 + a_6Z^3.$$

Die Transformation $(X,Y) \mapsto \left(\dfrac{1}{4a_2+1}X, \dfrac{1}{4a_2+1}Y\right)$ führt mit der Normalisierung $E \mapsto \dfrac{1}{(4a_2+1)^3}E$ zu der Form

$$E : \frac{Y^2Z - XYZ - a_2X^2Z}{4a_2+1} = X^3 + \frac{(36X+1)a_6}{(4a_2+1)^3}Z^3$$

Mit $j(E) - 1728 = \dfrac{c_4^3}{\Delta} - 1728 = -\dfrac{b_2^3}{a_6} = -\dfrac{(4a_2+1)^3}{a_6}$ für $char(K) \neq 2$ und $j(E) = \dfrac{1}{a_6}$ für $\mathrm{char}(K) = 2$ folgt mit einer geeigneten Normalisierung der Gleichung jeweils die gewünschte Normalform

$$E : \frac{Y^2Z - XYZ - a_2X^2Z}{4a_2+1} = X^3 - \frac{36X+1}{j-1728}Z^3.$$

□

Definition 7. Sei E/K eine elliptische Kurve mit $j(E) \neq 0, 1728$. Dann heißt der im Beweis von Satz 3.2.2. definierte Punkt $C(E)$ *das Zentrum von* E. Falls E gegeben ist durch eine Gleichung der Form

$$E : Y^2Z - XYZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

so hat das Zentrum die Koordinaten

$$C(E) = \left[2\frac{-a_4(4a_2+1)+36a_6}{(4a_2+1)^2-48a_4}, \frac{-a_4(4a_2+1)+36a_6}{(4a_2+1)^2-48a_4}, 1\right].$$

Bemerkung. Für eine elliptische Kurve E in Normalform $E(j, a)$ gilt $C(E) = [0, 0, 1]$.

Beispiel.

$$E : y^2 - xy = x^3 + 12x^2 - 22x - 222$$

Das heißt, E wird durch die Gleichung $F(X, Y, Z) = 0$ für

$$F(X, Y, Z) = Y^2Z - XYZ - X^3 - 12X^2Z + 22XZ^2 + 222Z^3 \in \mathbb{Q}[X, Y, Z]$$

beschrieben. Für die Ableitung von F nach y gilt

$$F_Y(X, Y, Z) = 2YZ - XZ = Z(2Y - X) = 0$$

Nun berechnet man die Ableitungen nach X und Z und schränkt sie auf die Gerade $L : 2Y - X = 0$ ein:

$$F_X(X, Y, Z)|_L = -12Y^2 - 49YZ + 22Z^2$$

$$F_z(X, Y, Z)|_L = -49Y^2 + 88YZ + 666Z^2$$

Nun wählt man eine beliebige Linearkombination von F_X und F_Z, die den Y^2-Term eliminiert und setzt sie gleich 0, zum Beispiel

$$49F_X - 12F_Z = -3457YZ - 6914Z^2 = 0$$

Es folgt

$$C(E) = [-4, -2, 1].$$

Die Transformation $C(E) \mapsto [0, 0, 1]$ bringt die elliptische Kurve in die Normalform

$$E : y^2 - xy = x^3 - 72x - 2.$$

Für die j-Invariante findet sich demnach

$$j(E) = \frac{3457}{2}.$$

3.3. **Klassifikation.**

Korollar 3.3.1. *Seien $E = E(j,a)$ und $E' = E'(j',a')$ elliptische Kurven in der obigen Normalform. Dann sind folgende Bedingungen äquivalent:*

a) $E \cong_K E'$
b) *Es existieren affine Transformationen $\varphi \in GL(3,K)$ von E nach E'. Jede solche Transformation ist von der Form*
$$\varphi : (X,Y) \mapsto (X, (1-2c)Y + cX)$$
für ein $c \in D_2(K) = \{a \in K \mid 1-2a \in K^*\}$.
c) $j = j'$ *und* $K_a \cong K_{a'}$

Beweis. *b)* $\Rightarrow$ *a)* ist offensichtlich.

a) $\Rightarrow$ *b)* Es gilt $C(E) = C(E') = [0,0,1]$, also hat jeder Isomorphismus die Form
$$\varphi : (X,Y) \mapsto (uX, vY + wX),\ u,v \in K^*, w \in K.$$
Wir betrachten die Kurven
$$\varphi(E) : \frac{v^2y^2 + (2vw - uv)xy + (w^2 - uw + au^2)\,x^2}{4a+1} = u^3x^3 - \frac{36ux+1}{j-1728}$$
$$E' : \frac{y^2 - xy + a'x^2}{4a'+1} = x^3 - \frac{36x+1}{j'-1728}.$$
Wegen $E \cong_{\bar{K}} E'$ gilt $j = j'$. Aus der Gleichheit der konstanten Terme folgt auch die Gleichheit der anderen Koeffizienten. Mit
$$\frac{1}{4a'+1} = \frac{v^2}{4a+1} = \frac{uv - 2vw}{4a+1}$$
folgt $v = u - 2w$. Damit bleibt nur noch $u = 1$ zu zeigen. Wir unterscheiden nun zwei Fälle:

(i) $\mathrm{char}(K) \neq 2$: Durch Koeffizientenvergleich ergeben sich die beiden Gleichungen
$$\frac{w^2 - uw + au^2}{4a+1} = \frac{a'}{4a'+1}$$
$$\frac{(u-2w)^2}{4a+1} = \frac{1}{4a'+1}.$$
Subtrahieren wir das Vierfache der ersten von der zweiten Gleichung, so folgt $u^2 = 1$. Es gilt jedoch durch Vergleichen der x^3-Koeffizienten auch $u^3 = 1$ und damit $u = 1$.

(ii) $\mathrm{char}(K) = 2$: Durch Koeffizientenvergleich erhalten wir nun $v^2 = 1$ und $v = u - 2w = u$. Also folgt auch $u^2 = 1$ und wie zuvor $u = 1$.

b) $\Rightarrow$ *c)* Wegen $E \cong_{\bar{K}} E'$ gilt $j = j'$. Gegeben sei
$$\varphi : (X,Y) \mapsto (X, (1-2c)Y + cX)$$

für ein $c \in D_2(K)$. Wir vergleichen nun die Koeffizienten der Kurven

$$\varphi(E) : \frac{(1-2c)^2y^2 + (c-4c^2)\,xy + (c^2-c+a)\,x^2}{4a+1} = x^3 - \frac{36x+1}{j-1728}$$
$$E' : \frac{y^2 - xy + a'x^2}{4a'+1} = x^3 - \frac{36x+1}{j'-1728}.$$

Wegen $E \cong_{\bar{K}} E'$ gilt $j = j'$. Aus der Gleichheit der konstanten Terme folgt auch die Gleichheit der anderen Koeffizienten. Mit

$$\frac{(1-2c)^2}{4a+1} = \frac{1}{4a'+1}$$

und

$$\frac{c^2-c+a}{4a+1} = \frac{a'}{4a'+1}$$

folgt nun

$$a' = \frac{a-c+c^2}{(1-2c)^2}.$$

Mit Lemma 1.0.1. folgt $K_a \cong K'_a$.

c) $\Rightarrow$ *b)* Nach Voraussetzung existiert mit Lemma 1.0.1. ein $c \in D_2(K)$ mit

$$a' = \frac{a-c+c^2}{(1-2c)^2}.$$

Die Transformation $(X, Y) \mapsto (X, (1-2c)Y + cX)$ liefert den gesuchten Isomorphismus. □

Korollar 3.3.2. *Sei E eine elliptische Kurve mit $j(E) \neq 0, 1728$. Dann ist die zu der Normalform $E(j, a)$ assoziierte Koordinatenfunktion $x \in K(E)$ kanonisch. Sie definiert einen kanonischen Isomorphismus*

$$E/\{e \mapsto -e\} \to \mathbb{P}^1$$
$$e \mapsto x(e).$$

3.4. **Die assoziierte kubische Gleichung.** Im Folgenden soll die Normalisierung einer elliptischen Kurve für $\mathrm{char}(K) \neq 2, 3$ auf die Normalisierung einer kubischen Gleichung beziehungsweise des zugehörigen Dreiecks zurückgeführt werden. Um einer elliptischen Kurve ein solches charakteristisches Dreieck zuordnen zu können, betrachten wir die Abbildung

$$\pi \colon E \setminus \{\mathcal{O}\} \to \{E \setminus \{\mathcal{O}\}\} / \{e \mapsto -e\}$$

Nach dem Gruppengesetz für eine elliptische Kurve

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

ergibt sich für einen Punkt $P_0 = (x_0, y_0) \in E$ das additive Inverse

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Die Verzweigungspunkte von π, das heißt, alle Punkte $P = (x, y) \in E \setminus \{\mathcal{O}\}$ mit $P = -P$, liegen wegen $y = -y - a_1x - a_3$ auf einer Geraden und sind damit Nullstellen der kubischen Gleichung

$$x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6 = 0.$$

Definition 8. Sei $E\colon y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ eine elliptische Kurve über einem gegeben Körper K. Dann heißen die Nullstellen der Gleichung

$$x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6 = 0$$

in $\bar{K}$ *das Verzweigungsdreieck* $\mathcal{D}(E)$ *von* E.

Bemerkung. Wie schon zuvor lässt sich E nach Lemma 3.2.1. durch geeignete affine Transformationen in die Form

$$E\colon y^2 - xy = x^3 + a_2x^2 + a_4x + a_6$$

bringen. Dies impliziert, dass die Verzweigungspunkte von π auf der Geraden $2y = x$ liegen und die zugehörige kubische Gleichung in die Form

$$x^3 - \left(-a_2 + \frac{1}{4}\right)x^2 + a_4 - (-a_6) = 0$$

gelangt. Diese können wir für $\mathrm{char}(K) \neq 2, 3$ über die assoziierte Basic Line mit Hilfe der Fixpunkte $R = R(x)$ und $G = G(x)$ normalisieren. Dazu wählen wir die Koordinaten $R = 0$ und $G = \frac{1}{12}$.

$$G = \frac{1}{12} \Leftrightarrow T = \frac{1}{4} \Leftrightarrow -a_2 + \frac{1}{4} = \frac{1}{4} \Leftrightarrow a_2 = 0$$

$$R = 0 \Leftrightarrow M = 0 \Leftrightarrow QT = 9N \Leftrightarrow Q = -36N \Leftrightarrow a_4 = 36a_6$$

Es folgt

$$E\colon y^2 - xy = x^3 + k(36x + 1), \text{ für ein } k \in K.$$

Nach Satz 3.2.2. zur Normalisierung von elliptischen Kurven folgt

$$k = -\frac{1}{j(E) - 1728}.$$

Der Zentrumspunkt ist also gerade der Spiegelungspol R der zu der elliptischen Kurve assoziierten kubischen Gleichung.

Da sich eine affine Transformation einer elliptischen Kurve zu einer affinen Transformation der assoziierten kubischen Gleichung fortsetzt, können wir die j-Invariante einer elliptischen Kurve über die t-Invariante der assoziierten kubischen Gleichung bestimmen:

Satz 3.4.1. *Sei* $\mathrm{char}(K) \neq 2$. *Betrachte die Abbildungen*

$$\phi\colon \{\textit{nicht-spezielle Dreiecke über } K\} \to \{\textit{Elliptische Kurven } E/K\}$$

$$\mathcal{D} = \{r_1, r_2, r_3\} \mapsto y^2 = P(\mathcal{D}) := (x - r_1)(x - r_2)(x - r_3)$$

und

$$\psi\colon \{\textit{Elliptischen Kurven } E/K, j(E) \neq 0, 1728\} \to \{\textit{Dreiecke über } K\}$$
$$\psi\colon E \mapsto \mathcal{D}(E).$$

Diese induzieren inverse Bijektionen zwischen

(i) *Äquivalenzklassen von nicht-speziellen kubischen Gleichungen, definiert über K, bis auf affine Transformationen über K*
(ii) *$\bar{K}$-Isomorphieklassen von glatten elliptischen Kurven E/K mit $j(E) \neq 0, 1728$.*

Diese sind auf den Mengen der Invarianten gegeben durch

$$\left\{K \setminus \left\{\frac{1}{4}, \frac{7}{27}\right\}\right\} \overset{1:1}{\longleftrightarrow} \{K \setminus \{0, 1728\}\}$$
$$t \mapsto \frac{256 D(\mathcal{D})^3}{A(\mathcal{D})^2(1-4t)}$$
$$\frac{1}{4} - \frac{16}{j - 1728} \leftarrow j$$

Für die Fälle, in denen die zu E assoziierte Weierstraß-Gleichung singulär ist oder $j(E) \in \{0, 1728\}$ beziehungsweise $\mathcal{D}$ speziell ist, gilt

a) $j(E) = 0 \Leftrightarrow D(\mathcal{D}) = 0$
b) $j = 1728 \Leftrightarrow A(\mathcal{D}) = 0$
c) $\Delta(E) = 0 \Leftrightarrow P(\mathcal{D})$ *hat eine mehrfache Nullstelle*

Beweis. Sei

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

eine beliebige glatte elliptische Kurve über K. Für $\mathrm{char}(K) \neq 2$ erfüllt das assoziierte Dreieck $\psi(E) = \mathcal{D}(E)$ die kubische Gleichung

$$0 = x^3 + \frac{1}{4}b_2x + \frac{1}{2}b_4x + \frac{1}{4}b_6.$$

Es ist leicht nachzurechnen, dass gilt $16\Delta(\mathcal{D}) = \Delta(E)$. Mit $j(E) = 1728 + \dfrac{c_6^2}{\Delta}$ und $A(\mathcal{D}) = \dfrac{c_6}{32}$ folgt

$$t = \frac{A(\mathcal{D})^2 - \Delta(\mathcal{D})}{4A(\mathcal{D})^2} = \frac{1}{4} - \frac{\Delta(E)}{64A(\mathcal{D})^2} = \frac{1}{4} - \frac{16}{j - 1728}.$$

Damit ist die auf den Isomorphieklassen induzierte Abbildung offensichtlich wohldefiniert, da E beliebig gewählt war und die t-Invariante der assoziierten kubischen Gleichung nur von $j(E)$ abhängt. Sei nun

$$P(\mathcal{D}) = x^3 - Tx^2 + Qx - N = 0$$

eine beliebige nicht-spezielle kubische Gleichung. Nach Definition folgt

$$\phi(\mathcal{D}) = E : y^2 = x^3 - Tx^2 + Qx - N.$$

Es gilt

$$j(E) = \frac{c_4^3}{\Delta(E)} = \frac{\left(b_2^2 - 48a_4\right)^3}{16\Delta(\mathcal{D})} = \frac{256D(\mathcal{D})^3}{A(\mathcal{D})^2(1-4t)}.$$

Da der Quotient $\dfrac{D(\mathcal{D})^3}{A(\mathcal{D})^2}$ invariant unter affinen Transformationen ist, ist auch hier die auf den Isomorphieklassen induzierte Abbildung wohldefiniert. Zu zeigen bleibt, dass ϕ und ψ zueinander invers sind. Sei zunächst $E = \phi(\mathcal{D})$. Dann ist die Einschränkung von E auf die Verzweigungsgerade $y = 0$ offensichtlich wieder $P(\mathcal{D})$. Sei nun eine elliptische Kurve E gegeben. Dann gelten für die assoziierte kubische Gleichung $\psi(E) = P(\mathcal{D}) = 0$ die Relationen $A(\mathcal{D}) = \dfrac{c_6}{32}$ und $D(\mathcal{D}) = \dfrac{c_4}{16}$. Für $E' = \phi \circ \psi(E)$ folgt nun

$$\begin{aligned} j\left(E'\right) =& \frac{256D(\mathcal{D})^3}{A(\mathcal{D})^2\left(\frac{1}{4} - \frac{16}{j(E)-1728}\right)} \\ =& \frac{4D(\mathcal{D})^3(j(E)-1728)}{A(\mathcal{D})^2} \\ =& \frac{c_4^3(j(E)-1728)}{c_6^2} \\ =& j(E). \end{aligned}$$

a) Folgt aus $D(\mathcal{D}) = \dfrac{c_4}{16}$.
b) Folgt aus $A(\mathcal{D}) = \dfrac{c_6}{32}$.
c) Folgt aus $16\Delta(\mathcal{D}) = \Delta(E)$.

□

Beispiel. Wir betrachten wieder die Kurve

$$E : y^2 - xy = x^3 + 12x^2 - 22x - 222.$$

Wie zuvor schon berechnet, gilt $j(E) = \dfrac{3457}{2}$. Das zu E assoziierte Dreieck $\mathcal{D}$ genügt der Gleichung

$$x^3 + \frac{49}{4}x^2 - 22x - 222 = 0.$$

Daraus errechnen sich die Parameter

$$\begin{aligned} D(\mathcal{D}) =& \frac{3457}{16} \\ A(\mathcal{D}) =& -\frac{3457}{32} \end{aligned}$$

und damit die Invariante $t(\mathcal{D}) = \dfrac{-127}{4}$. Es gilt wie gewünscht

$$j = \frac{256D(\mathcal{D})^3}{A(\mathcal{D})^2(1-4t)} = \frac{3457}{2}.$$

4. Das Zentrum einer elliptischen Kurve

4.1. **Lage des Zentrums.**

Lemma 4.1.1. *Sei E/K eine elliptische Kurve, $C(E)$ das Zentrum von E und $\mathcal{D}(E)$ das Verzweigungsdreieck von E.*

a) *Für $j(E) \neq 0, 1728$ liegt $C(E)$ im affinen Bereich des $\mathbb{P}^2$ und $C(E) \notin E$.*
b) *Für $j(E) = 1728$ und $\mathrm{char}(K) \neq 2, 3$ liegt $C(E)$ im affinen Bereich des $\mathbb{P}^2$ und es gilt $C(E) \in E$. Insbesondere gilt $C(E) \in \mathcal{D}(E)$ und $C(E) = G(\mathcal{D}(E))$.*
c) *Für $j(E) = 0$ ist $C(E)$ der Punkt im Unendlichen auf der Gerade der 2-Torsionspunkte von E.*

Beweis. a) Nach Satz 3.2.2. kann E durch affine Transformation über K in die Normalform

$$\frac{Y^2Z - XYZ - aX^2Z}{4a+1} = X^3 - \frac{36X + Z}{j - 1728}Z^2$$

gebracht werden. Aus dem Beweis von Satz 3.2.2. und Korollar 3.3.1. folgt, dass das Zentrum nun die Koordinaten $C(E) = [0, 0, 1]$ besitzt. Dieser Punkt liegt jedoch nicht auf E.

b) Für $j(E) = 1728$ zeigt sich

$$C(E) = \left[\frac{1}{12}(4a_2 + 1), \frac{1}{24}(4a_2 + 1), 1\right],$$

das heißt, das Zentrum befindet sich im affinen Bereich. Mit der Verschiebung $C(E) = [0, 0, 1]$ gelangt die elliptische Kurve in die Form

$$E : y^2 - xy = x^3 - \frac{1}{4}x^2 + a_4x.$$

Der Zentrumspunkt liegt also auf der elliptischen Kurve. Das assoziierte Verzweigungsdreick besteht aus den Nullstellen der kubischen Gleichung

$$x^3 + a_4x = 0$$

und nach Satz 3.4.1. gilt für den Schwerpunkt $G(\mathcal{D}(E)) \in \mathcal{D}(E)$. Es gilt jedoch offensichtlich $G(\mathcal{D}(E)) = 0 = C(E)$.

c) Dies folgt für $\mathrm{char}(K) \neq 2$ sofort aus der Konstruktion des Zentrums im Beweis zur Normalform einer elliptischen Kurve. Für $\mathrm{char}(K) = 2$ gilt in der Weierstraß-Gleichung $a_1 = 0$ und für die Verzweigungsgerade erhalten wir $Z = 0$. Das Zentrum ist in diesem Fall wie auch für $\mathrm{char}(K) \neq 2$ gerade $C(E) = [0, 1, 0] = [2, 1, 0]$.

□

Bemerkung. Für eine elliptische Kurve in Normalform $E(j, a)$ bestehen die Fixpunkte unter den Automorphismen, die das Zentrum $C(E)$ invariant lassen, gerade aus der Verzweigungsgeraden $2y = x$.

Beweis. Diese Automorphismen sind, wie schon gesehen, von der Form $(x, y) \mapsto (x, (1-2c)y + cx),\ c \in D_2(K)$. Für die Fixpunkte gilt also $y = (1-2c)y + cx$ und damit auch $2y = x$. □

4.2. **Fahnen.** Eine elliptische Kurve E lässt sich als kubische Kurve in $\mathbb{P}(V_3^*)$ auffassen:

Bemerkung. Sei W ein endlich-dimensionaler K-Vektorraum mit Basis $B = \{w_1, ..., w_n\}$ und $B^* = \{x_1, ..., x_n\}$ die assoziierte Basis des Dualraums W^*. Jedem Element $g \in S^\bullet(W^*)$, der symmetrischen Algebra über W^*, entspricht genau einem Element des Polynomrings $K[x_1, ..., x_n]$, via dem Isomorphismus

$$\begin{aligned} S^\bullet(W^*) &\to K[x_1, ..., x_n] \\ \bigotimes_i x_i^{\otimes e_i} &\mapsto \prod_i x_i^{e_i},\ e_i \in \mathbb{N} \end{aligned}$$

Für ein homogenes Element $g \in S(W^*)$ definiert die Gleichung $g = 0$ also eine Teilmenge $X \subset \mathbb{P}(W)$.

Sei also wie zuvor $\{1, x, y\},\ \mathrm{ord}_{\mathcal{O}}(x) = -2,\ \mathrm{ord}_{\mathcal{O}}(y) = -3$, eine Basis des Vektorraums V_3, wobei x und y keine weiteren Polstellen besitzen. Nach der obigen Bemerkung definiert eine assoziierte Weierstraß-Gleichung $f = 0$, wobei f als homogenes Element der symmetrischen Algebra über V_3 aufgefasst wird, die elliptische Kurve E als Teilmenge von $\mathbb{P}(V_3^*)$. Die Gerade im Unendlichen ist gegeben durch

$$\begin{aligned} \mathbb{P}((V_3/K)^*) =& \{f \in V_3^* \mid f(1) = 0\} \\ =& \{[f(x), f(y), 0] \mid f \in V_3^*,\ f(1) = 0\}. \end{aligned}$$

Das heißt, wir bekommen im affinen Bereich die Einbettung

$$\begin{aligned} \iota \colon E \setminus \mathcal{O} &\to \mathbb{P}(V_3^*) \\ P &\mapsto [f \mapsto f(P)]. \end{aligned}$$

Diese ist wohldefiniert, da $\mathcal{O}$ die einzige Polstelle von x und y ist. Um die Einbettung auf ganz E fortzusetzen, überdecken wir E durch Zariski-offene Mengen der Form

$$U_g = \{P \in E \mid g(P) \neq 0\},\ g \in V_3, \mathrm{ord}_{\mathcal{O}}\, g = -3.$$

Auf einer solchen Menge U_g lässt sich die Einbettung in Übereinstimmung mit ι definieren als

$$\begin{aligned} \iota_g \colon U_g &\to \mathbb{P}(V_3^*) \\ P &\mapsto \left[f \mapsto \frac{f}{g}(P) \right]. \end{aligned}$$

Auf den Schnittmengen $U_g \cap U_{g'}$ stimmen die Einbettungen ebenfalls überein, da

$$\left[\frac{f}{g}(P) \right] = \left[\frac{f}{g'}(P) \right],\ \text{für } g(P), g'(P) \neq 0.$$

Die Einbettung ι lässt sich also fortsetzen zu

$$\iota\colon E \to \mathbb{P}(V_3^*)$$
$$P \mapsto \left[f \mapsto \frac{f}{g}(P) \right],$$

für g beliebig mit $P \in U_g$.

Definition 9. Eine *Fahne* in einem K-Vektorraum V ist eine Folge $(V_0, ..., V_n)$ von Untervektorräumen mit den Eigenschaften $V_0 = \{0\}, V_n = V$ und $V_i \subset V_{i+1},\ 0 \leq i \leq n-1$. Eine Fahne heißt *vollständig*, falls $dim\ V_i = i$, für $0 \leq i \leq n$.

Satz 4.2.1. *Das Zentrum $C(E)$ einer elliptischen Kurve E mit $j(E) \neq 0, 1728$ definiert eine charakteristische vollständige Fahne in*

$$V_3 := \{f \in K(E)^* \mid ord_{\mathcal{O}}(f) \geq -3,\ ord_x(f) \geq 0, \textit{für alle } x \in E \setminus \mathcal{O}\}.$$

Beweis. Analog zu den vorigen Berechnungen erhält man das Zentrum von E als Element $\bar{\gamma} \in \mathbb{P}(V_3^*)$. Dieses befindet sich für $j(E) \neq 0$ im affinen Bereich, also gerade in

$$\begin{aligned}\mathbb{P}(V_3^*) \setminus \mathbb{P}((V_3/K)^*) =& \{f \in V_3^* \mid f(1) \neq 0\}/K^* \\ =& \{f \in V_3^* \mid f(1) = 1\}.\end{aligned}$$

Wählt man nun, wie zuvor, eine neue Basis $\{1, \tilde{x}, \tilde{y}\}$ von V_3 mit

$$\bar{\gamma}(\tilde{x}) = \bar{\gamma}(\tilde{y}) = 0,$$

so besitzt das Zentrum nun die Koordinaten $[0, 0, 1]$. Wir betrachten nun die Dualität

$$\begin{gathered}\{U \subset V_3^* \mid dim(U) = 1\} \overset{1:1}{\longleftrightarrow} \{W \subset V_3 \mid dim(W) = 2\} \\ \langle\gamma\rangle \mapsto ker(\gamma) \\ (V_3/W)^* \leftarrow W\end{gathered}$$

Für ein zu $C(E)$, also zu $\bar{\gamma}$ assoziiertes $\gamma \in V_3^*$, ein Urbild unter der kanonischen Projektion

$$\begin{gathered}V_3^* \setminus \{0\} \to \mathbb{P}(V_3^*) \\ (x_0, x_1, x_2) \mapsto [x_0, x_1, x_2],\end{gathered}$$

gilt mit $W_2 := ker(\gamma) = V_3/K$ also $dim\ ker(W_2) = dim\ \langle\tilde{x}, \tilde{y}\rangle = 2$ und mit $W_1 := W_2 \cap V_2$ auch $dim\ W_1 = 1$, da V_2 alle Funktionen mit $\mathcal{O}$-Ordnung -2 enthält. Das Zentrum $C(E)$ einer elliptischen Kurve E mit $j(E) \neq 0$ definiert also eine charakteristische vollständige Fahne in V_3:

$$\{0\} \hookrightarrow W_1 \hookrightarrow W_2 \hookrightarrow V_3$$

□

Umgekehrt erhalten wir eine Fahne in V_3^*, und für die Projektivierung gilt

$$\begin{array}{ccccc} \mathcal{O} = \mathbb{P}((V_3/V_2)^*) & \hookrightarrow & \mathbb{P}((V_3/V_1)^*) & \hookrightarrow & \mathbb{P}(V_3^*) \\ & \searrow & & & \uparrow \\ C(E) = \mathbb{P}((V_3/W)^*) & \hookrightarrow & \mathbb{P}((V_3/W_1)^*) & & E \end{array}$$

4.3. **Die Involution.** Im Folgenden soll neben dieser algebraischen Charakterisierung des Zentrums auch noch eine geometrische Konstruktion angegeben werden. Dazu benötigen wir einige Begriffe aus der projektiven Geometrie:

Definition 10. Sei $f(x, y, z)$ ein homogenes Polynom vom Grad n und eine Kurve C definiert durch $f(x, y, z) = 0$. Für einen Punkt P auf C ist die *Tangente an* P definiert durch

$$T_P(x, y, z) = x\frac{\partial f}{\partial x}(P) + y\frac{\partial f}{\partial y}(P) + z\frac{\partial f}{\partial z}(P) = 0.$$

Für einen beliebigen Punkt $Q = [a, b, c] \in \mathbb{P}^2$ definiert die Gleichung

$$a\frac{\partial f}{\partial x} + b\frac{\partial f}{\partial y} + c\frac{\partial f}{\partial z} = 0$$

eine Kurve C_Q vom Grad $n - 1$. Sie heißt die *Polare von C bezüglich Q*. Der Punkt Q heißt der *Pol* von C_Q.

Bemerkung. Für zwei Punkte $P \in C$ und $Q = [a, b, c] \in \mathbb{P}^2$ gilt

Q liegt auf der Tangente an P

$\Leftrightarrow$ P ist ein Schnittpunkt von C und der Polaren bezüglich Q

Beweis.

$$\begin{aligned} & T_P([a, b, c]) = 0 \\ \Leftrightarrow\ & a\frac{\partial f}{\partial x}(P) + b\frac{\partial f}{\partial y}(P) + c\frac{\partial f}{\partial z}(P) = 0 \\ \Leftrightarrow\ & C_Q(P) = 0 \end{aligned}$$

□

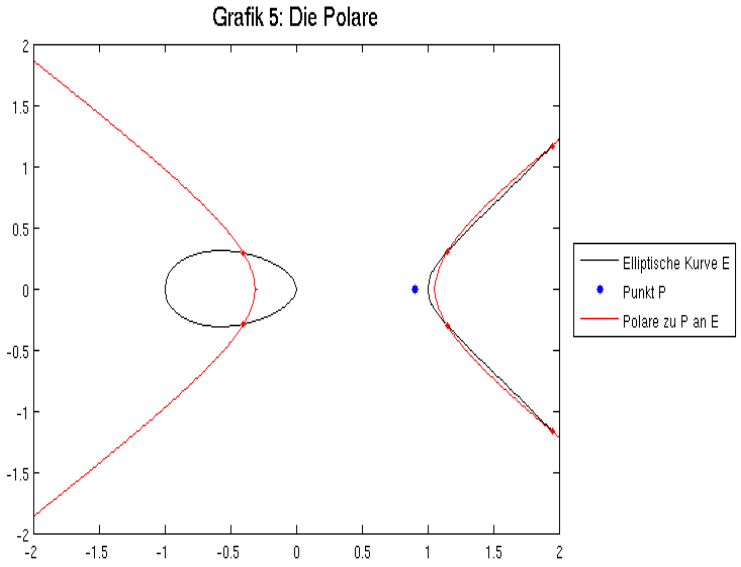
Beispiel. Sei $P = \left[\frac{9}{10}, 0, 1\right] \in \mathbb{RP}^2$ und

$$E : y^2z = \frac{1}{4}x^3 - \frac{1}{4}xz^2$$

eine elliptische Kurve über $\mathbb{R}$. Dann ist die Polare gegeben durch die Gleichung

$$C_P : y^2 = \frac{27}{40}x^2 - \frac{1}{2}xz - \frac{9}{40}z^2$$

(siehe Grafik 5).



Definition 11. Für eine Funktion $f(x_1, ..., x_n)$ heißt die Matrix

$$H(f) = \left(\left(\frac{\partial^2 f}{\partial x_i \partial x_j} \right)_{i,j} \right)$$

die Hesse-Matrix von f. Ist f homogen vom Grad n, so definiert die Gleichung $det(H(f)) = 0$ die *Hesse'sche Kurve* vom Grad $3(n-2)$.

Bemerkung. Für ein homogenes Polynom $g \in K[x, y, z]$ liegt ein Punkt $Q = [a, b, c]$ genau dann auf der Hesse'schen Kurve bezüglich der Kurve $g = 0$, wenn die Kurve

$$C_g : \sum_{w \in \{x,y,z\}} \frac{\partial^2 f(Q)}{\partial^2 w} + \sum_{\substack{v,w \in \{x,y,z\} \\ v \neq w}} \frac{\partial^2 f(Q)}{\partial v \partial w} = 0$$

degeneriert ist. Falls g homogen vom Grad 3 ist, ist C_g gerade die Polare von Q bezüglich der Kurve $g = 0$. Folglich besteht die Hesse'sche Kurve in diesem Fall aus genau den Punkten, deren assoziierte Polare degeneriert ist, das heißt, aus ein oder zwei Geraden besteht. Insbesondere gilt dies also für elliptische Kurven. Für eine genauere Erläuterung siehe [Sal1897], S.49ff.

Nun lässt sich die bisher nur algebraische Konstruktion des Zentrumspunktes einer elliptischen Kurve geometrisch beschreiben.

Lemma 4.3.1. *Sei E/K eine elliptische Kurve mit $j(E) \neq 0, 1728$ und L die Verzweigungsgerade von E. Dann existiert für jeden Punkt $P \in L$ ein Punkt $Q \in L$ mit der assoziierten Polare E_Q, sodass $P \in E_Q$.*

Beweis. Sei $f(x, y, z)$ ein homogenes Polynom mit $E : f = 0$. Nach Lemma 3.2.1. gelte ohne Einschränkung

$$f = y^2z - xyz - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

Es ist leicht nachzurechnen, dass der Nullpunkt der elliptischen Kurve $\mathcal{O} = [0, 1, 0]$ auf der assoziierten Hesse'schen Kurve liegt. Die zugehörige Polare ist also degeneriert. Sie wird durch die Ableitung nach y beschrieben:

$$E_{\mathcal{O}} : \frac{\partial f}{\partial y} = z(2y - x) = 0$$

Die Polare besteht also einerseits aus der Geraden im Unendlichen, das heißt, der Tangenten an $\mathcal{O}$ bezüglich der elliptischen Kurve und andererseits aus der Geraden

$$L : 2y = x.$$

Auf L definiert jeder Punkt P wieder eine Polare E_P bezüglich der elliptischen Kurve E. Für zwei beliebige Punkte $P_1 = [a_1, b_1, c_1], P_2 = [a_2, b_2, c_2] \in L$ mit $P_1 \neq P_2$ lässt sich ein beliebiger Punkt $P = [a, b, c] \in L$ schreiben als

$$P = P_1 + t(P_2 - P_1).$$

Daraus folgt mit $E_P : f_P = 0$ für die zu P assoziierte Polare

$$\begin{aligned} f_P &= a\frac{\partial f}{\partial x} + b\frac{\partial f}{\partial y} + c\frac{\partial f}{\partial z} \\ &= (a_1 + t(a_2 - a_1))\frac{\partial f}{\partial x} + (b_1 + t(b_2 - b_1))\frac{\partial f}{\partial y} + (c_1 + t(c_2 - c_1))\frac{\partial f}{\partial z} \\ &= f_{P_1} + t(f_{P_2} - f_{P_1}) \end{aligned}$$

Es gilt also

$$E_{P_1+t(P_2-P_1)} : f_{P_1} + t(f_{P_2} - f_{P_1}) = 0.$$

Jede dieser Polaren schneidet die Gerade L für einen algebraisch abgeschlossenen Körper in maximal 2 Punkten. Umgekehrt liegt jeder Punkt $P \in L$ auf genau einer dieser Polaren. Dazu betrachte man die Gleichung

$$f_{P_1}(P) + t(f_{P_2}(P) - f_{P_1}(P)) = 0.$$

Dies definiert einen eindeutigen Skalar $t_P \in K$. Damit ist die gesuchte Polare für $f_{P_2}(P) - f_{P_1}(P) \neq 0$ gerade

$$f_{P_1} - \frac{f_{P_1}(P)}{f_{P_2}(P) - f_{P_1}(P)}(f_{P_2} - f_{P_1}) = 0.$$

Der Ausnahmefall tritt auf L nur bei $\mathrm{char}(K) \notin \{2, 3\}$ für die beiden Punkte

$$\{Q_1, Q_2\} = \left\{ -\frac{1}{12}\left(1 \pm \sqrt{\frac{2j(E)}{j(E) - 1728}}\right) \right\}$$

mit $f_{P_2}(Q_i) - f_{P_1}(Q_i) = 0$ ein. Dies sind gerade die Nullstellen auf L der zum Punkt im Unendlichen auf L assoziierten Polaren

$$f_{P^*} = 2\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y}, \text{ mit } P^* = [2, 1, 0].$$

□

Satz 4.3.2. *Sei E/K eine elliptische Kurve mit $j(E) \neq 0, 1728$ und L die Verzweigungsgerade von E. Dann induzieren die Polaren der Punkte auf L eine kanonische Abbildung ϕ_L auf L: Nach Lemma 4.3.1. existiert für alle $P \in L$ ein eindeutiger Punkt $Q \in L$ mit $P \in E_Q$. Sei P' der zweite Schnittpunkt von E_Q mit L. Definiere*

$$\phi_L(P) = P'.$$

Es zeigt sich, dass ϕ_L für $\mathrm{char}(K) \neq 3$ eine Involution ist. Das Zentrum $C(E)$ korrespondiert zu dem Punkt im Unendlichen auf L.

Beweis. Sei $f(x, y, z)$ ein homogenes Polynom mit $E : f = 0$. Nach Lemma 3.2.1. gelte ohne Einschränkung

$$f = y^2z - xyz - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

Damit hat die Verzweigungsgerade die Form

$$L : 2y = x.$$

Für zwei gegebene Punkte $P, Q \in L$ mit $P \in E_Q$ kann nun leicht der zweite Schnittpunkt von E_Q mit L ausgerechnet werden. Wir erhalten

$$\phi_L \colon P = [2Y, Y, Z] \mapsto [2\varphi(Y, Z), \varphi(Y, Z), 1]$$

mit

$$\varphi(Y, Z) = \frac{Z\left(-a_6b_2 + 4a_4^2\right) - Y(36a_6 - a_4b_2)}{-Yc_4 + Z(36a_6 - a_4b_2)}.$$

Es gilt

$$\varphi(1, 0) = \frac{36a_6 - a_4b_2}{c_4}$$

und damit

$$\phi_L([2, 1, 0]) = C(E).$$

Umgekehrt ist $\left(\frac{36a_6 - a_4b_2}{c_4}, 1\right)$ eine Polstelle von ϕ_L, also gilt

$$\phi_L(C(E)) = [2, 1, 0].$$

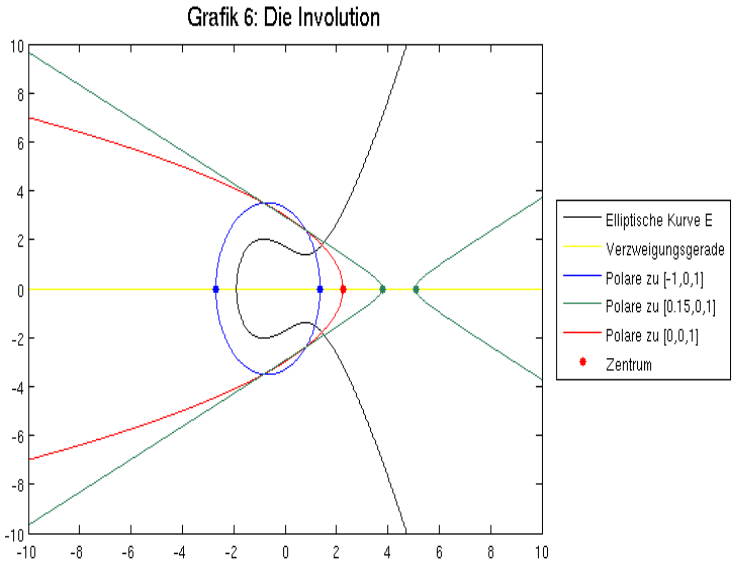
Ist die elliptische Kurve E in der Normalform

$$E \colon \frac{Y^2Z - XYZ - aX^2Z}{4a + 1} = X^3 - \frac{36X + Z}{j - 1728}z^2, \ a \in D_4(K),$$

also insbesondere $C(E) = 0$, so hat die Abbildung die Form

$$\varphi(Y, Z) = \frac{-3Z}{(j - 1728)Y}.$$

Für $\mathrm{char}(K) \neq 3$ ist ϕ_L also eine Involution. □



Beispiel. Gegeben sei die reelle elliptische Kurve $E : y^2 = x^3 - 2x + 3$. Dann ist die Verzweigungsgerade gegeben durch die Gleichung $y = 0$ und das Zentrum hat die Koordinaten $C(E) = \left[\frac{9}{4}, 0, 1\right]$ (s. Grafik 6).

4.4. **Schnittpunkte von Polaren.** Nun zu einer weiteren geometrischen Konstruktion des Zentrumspunktes einer elliptischen Kurve E mit $j(E) \neq 0, 1728$. Dazu betrachten wir mit Lemma 3.2.1. wieder die assoziierte Weierstraß-Kurve $f = 0$ mit

$$f = Y^2Z - XYZ - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

Bemerkung. Die Tangente an der Hesse'schen Kurve $H(f)$ im Nullpunkt $\mathcal{O} = [0, 1, 0]$ hat die Form

$$\begin{aligned} T_{\mathcal{O}} : x\frac{\partial H}{\partial x}(\mathcal{O}) + y\frac{\partial H}{\partial y}(\mathcal{O}) + z\frac{\partial H}{\partial z}(\mathcal{O}) &= 0 \\ \Leftrightarrow 24x + 2z(1 + 4a_2) &= 0 \\ \Leftrightarrow z = \frac{-12x}{1 + 4a_2} & \end{aligned}$$

Es gilt $1 + 4a_2 \neq 0$, da sonst nach der ersten Konstruktion des Zentrumspunktes für die Koordinaten $C(E) = [0, 0, 1]$ auch $a_6 = 0$ folgt. Damit liegt das Zentrum aber auf der elliptischen Kurve, es gilt also $j(E) = 1728$.

Jedem Punkt auf $T_{\mathcal{O}}$ lässt sich wie zuvor eine Polare bezüglich der elliptischen Kurve E zuordnen. Wir wollen nun die Schnittpunkte dieser Polaren berechnen. Dazu genügt es, die Schnittpunkte zweier beliebiger Polaren zu bestimmen:

Bemerkung. Falls ein Punkt $P \in \mathbb{P}^2$ die Gleichungen

$$x_1\frac{\partial f}{\partial x}(P) + y_1\frac{\partial f}{\partial y}(P) + z_1\frac{\partial f}{\partial z}(P) = 0$$
$$x_2\frac{\partial f}{\partial x}(P) + y_2\frac{\partial f}{\partial y}(P) + z_2\frac{\partial f}{\partial z}(P) = 0$$

für zwei Punkte $[x_1, y_1, z_1] \neq [x_2, y_2, z_2] \in T_{\mathcal{O}}$ erfüllt, so auch für einen beliebigen anderen Punkt auf

$$T_{\mathcal{O}} : [x_1, y_1, z_1] + k[x_2 - x_1, y_2 - y_1, z_2 - z_1],\ k \in K.$$

Satz 4.4.1. *Sei E/K eine elliptische Kurve mit $j(E) \neq 0, 1728$, $T_{\mathcal{O}}$ die Tangente am ausgezeichneten Punkt $\mathcal{O}$ von E und $P \in T_{\mathcal{O}}$. Dann schneiden sich die Polaren*

$$\{E_P \mid P \in T_{\mathcal{O}}\}$$

in genau einem affinen Punkt. Dieser Punkt ist das Zentrum von E.

Beweis. Ohne Einschränkung sei E nach Lemma 3.2.1. wieder von der Form $f = 0$ mit

$$f = y^2z - xyz - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

Nach den obigen Bemerkungen reicht es aus, die Schnittpunkte der Polaren von $P_1 = \left[1, 0, \frac{-12}{1+4a_2}\right]$ und $P_2 = \left[1, 1, \frac{-12}{1+4a_2}\right]$ zu betrachten, das heißt, die gemeinsamen Lösungen der Gleichungen

$$E_{P_1} : \frac{\partial f}{\partial x} + \frac{-12}{1+4a_2}\frac{\partial f}{\partial z} = 0$$
$$E_{P_2} : \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} + \frac{-12}{1+4a_2}\frac{\partial f}{\partial z} = 0$$

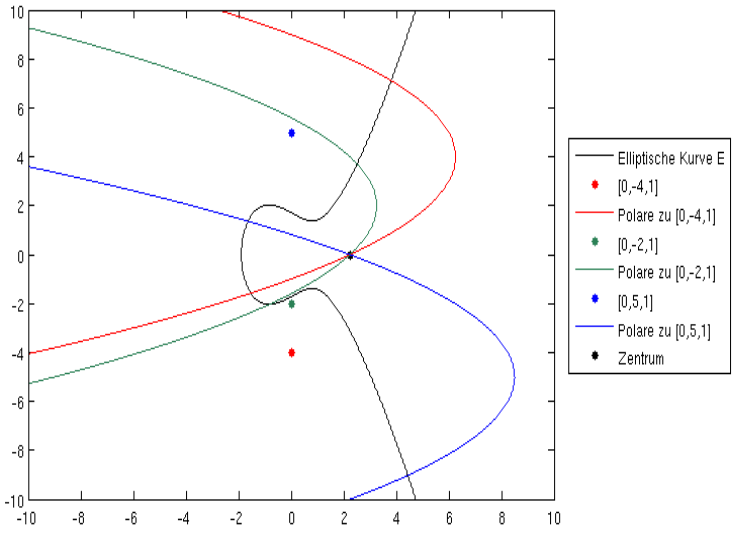
Es folgt sofort

$$\frac{\partial f}{\partial y} = z(2y - x) = 0.$$

Die Schnittpunkte der Polaren liegen also entweder auf der Gerade im Unendlichen oder auf der Geraden durch die Verzweigungspunkte der elliptischen Kurve, also der Punkte mit Ordnung 2. Betrachten wir zunächst die Punkte im Unendlichen, also die Einschränkung der Polaren E_{P_1} auf $z = 0$. Es ergibt sich

$$\begin{aligned} &-3x^2 + \frac{-12}{1+4a_2}\left(y^2 - xy - a_2x^2\right) = 0 \\ \Leftrightarrow\ &x^2 + 4\left(y^2 - xy\right) = 0 \\ \Leftrightarrow\ &(x - 2y)^2 = 0 \\ \Leftrightarrow\ &x - 2y = 0 \end{aligned}$$

Grafik 7: Das Zentrum



Alle Schnittpunkte der Polaren liegen also auf der Geraden der Verzweigungspunkte der elliptischen Kurve. Der erste Schnittpunkt ist demnach der Schnittpunkt dieser Geraden, also der gemeinsame Punkt mit der Geraden im Unendlichen, $S_1 = [2, 1, 0]$. Die weiteren Schnittpunkte ergeben sich durch die Einschränkung der Polaren E_{P_1} auf die Verzweigungsgerade $2y = x$. Man erhält

$$\begin{aligned} & -yz - 12y^2 - 4a_2yz - a_4z^2 \\ & - \frac{12}{1+4a_2}\left(y^2 - 2y^2 - 4a_2y^2 - 4a_4yz - 3a_6z^2\right) = 0 \\ \Leftrightarrow\ & z\left(y\left(48a_4 - (1+4a_2)^2\right) - z(a_4(1+4a_2) - 36a_6)\right) = 0 \end{aligned}$$

Es ergeben sich also zwei Schnittpunkte. Einerseits der schon bekannte Punkt S_1 im Unendlichen und andererseits ein affiner Punkt

$$S_2 = \left[2\frac{a_4(1+4a_2) - 36a_6}{48a_4 - (1+4a_2)^2}, \frac{a_4(1+4a_2) - 36a_6}{48a_4 - (1+4a_2)^2}, 1\right] = C(E).$$

□

Beispiel. Gegeben sei wieder die reelle elliptische Kurve $E : y^2 = x^3 - 2x + 3$. Dann ist die Tangente an der Hesse'schen Kurve gegeben durch die Gleichung $x = 0$ und das Zentrum hat die Koordinaten $C(E) = \left[\frac{9}{4}, 0, 1\right]$ (s. Grafik 7).

Literatur

[1] [Sil1986] Joseph H. Silverman, The Arithmetik of Elliptic Curves, 1986

[2] [Sal1897] George Salmon, Higher Plane Curves, 1897

[3] [Rost] Markus Rost, Notes on cubic equations,
http://www.math.uni-bielefeld.de/ rost/data/cubic-normal.pdf