Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 5

Wendepunkte

Eine projektive kubische Kurve ist von der Form

$$C = V_+(F) \subset \mathbb{P}^2_K$$

mit einem homogenen Polynom $F \in K[X,Y,Z]$ vom Grad 3. Als solches ist

$$F = \sum_{(r,s,t)\, r+s+t=3} \alpha_{(r,s,t)} X^r Y^s Z^t$$

und daher ist F durch die zehn Koeffizienten festgelegt. Die Nullstellenmenge ändert sich nicht bei Multiplikation mit einem Skalar $\neq 0$. Durch Variablentransformationen und Normierungen kann man hier die Darstellung vereinfachen. Für einen Teil der Vereinfachungen muss man die Charakteristiken $2,3$ ausschließen und voraussetzen, dass der Körper gewisse Wurzeln besitzt, was über einem algebraisch abgeschlossenen Körper stets gegeben ist. Die Vereinfachungsmöglichkeiten hängen auch davon ab, ob die Kurve glatt ist oder nicht.

Eine ebene projektive Kurve vom Grad d schneidet eine projektive Gerade, die nicht ganz auf C liegt, in d Punkten, wenn man die Multiplizitäten mitzählt. Die Schnittpunkte ergeben sich einfach dadurch, dass man die Geradengleichung nach einer Variable auflöst und diese in der Kurvengleichung ersetzt. Dabei entsteht ein homogenes Polynom vom Grad d in zwei Variablen. Über einem algebraisch abgeschlossenen Körper zerfällt dieses in homogene Linearfaktoren, und diese beschreiben die Schnittpunkte mit der Geraden. Unter der Schnittmultiplizität des Schnittpunktes versteht man den Exponenten des zugehörigen Linearfaktors. Multiplizität 1 bedeutet transversaler Schnitt. Die (projektive) Tangente an einen glatten Punkt der Kurve, die durch

$$\frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z = 0$$

gegeben ist, schneidet die Kurve in dem Punkt mit Multiplizität ≥ 2.

Unter einem *Wendepunkt* einer algebraischen Kurve versteht man einen glatten Punkt der Kurve, in dem die Schnittmultiplizität der Kurve mit ihrer Tangente in dem Punkt ≥ 3 ist. Für eine kubische Kurve bedeutet dies, dass die Tangente die Kurve in keinem weiteren Punkt schneidet.

LEMMA 5.1. *Es sei $V_+(F) \subseteq \mathbb{P}^2_K$ eine glatte projektive Kurve von Grad 3 über einem Körper K der Charakteristik $\neq 2, 3$. Es sei P ein K-Punkt der Kurve, in dem die Determinante der Hesse-Matrix von F verschwindet. Dann ist P ein Wendepunkt der Kurve.*

Beweis. Durch eine lineare Transformation können wir erreichen, dass $P = (0, 0, 1)$ ist und dass die Tangente der Kurve durch diesen Punkt durch $Y = 0$ gegeben ist. Da die Tangente durch die Gleichung

$$\frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z = 0$$

beschrieben wird, folgt

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Dies bedeutet wiederum, dass die Monome XZ^2 und Z^3 nicht in F vorkommen. Die Hesse-Matrix hat somit im gegebenen Punkt die Form

$$\begin{pmatrix} \frac{\partial}{\partial X}\frac{\partial F}{\partial X}(P) & \frac{\partial}{\partial X}\frac{\partial F}{\partial Y}(P) & 0 \\ \frac{\partial}{\partial X}\frac{\partial F}{\partial Y}(P) & \frac{\partial}{\partial Y}\frac{\partial F}{\partial Y}(P) & \frac{\partial}{\partial Y}\frac{\partial F}{\partial Z}(P) \\ 0 & \frac{\partial}{\partial Y}\frac{\partial F}{\partial Z}(P) & 0 \end{pmatrix}.$$

Diese Hesse-Matrix ist nach Voraussetzung nicht invertierbar, es sei $v \neq 0$ ein Element des Kernes. Wir betrachten zuerst den Fall, wo $v \notin \langle e_1, e_3 \rangle$ ist. Aus der dritten Zeile folgt

$$\frac{\partial}{\partial Y}\frac{\partial F}{\partial Z}(P) = 0.$$

Daher kommt YZ^2 in F nicht vor. Dies bedeutet, dass in F die Variable Z höchstens in der ersten Potenz vorkommt. Doch in diesem Fall ist die Kurve nach Aufgabe 4.23 nicht glatt.

Wir betrachten nun den Fall, wo $v \in \langle e_1, e_3 \rangle$ ist, sagen wir $v = \begin{pmatrix} \alpha \\ 0 \\ \gamma \end{pmatrix}$. Bei $\alpha = 0$ erhält man mit der zweiten Zeile wie soeben eine nichtglatte Kurve. Sei also $\alpha \neq 0$. Da v und e_1 zusammen mit e_3 die gleiche projektive Gerade definieren, können wir nach einer weiteren linearen Transformation, die die Koordinaten des Punktes und die Tangentengleichung nicht ändert, $v = e_1$ annehmen. Daraus ergibt sich

$$\frac{\partial}{\partial X}\frac{\partial F}{\partial X}(P) = \frac{\partial}{\partial X}\frac{\partial F}{\partial Y}(P) = 0,$$

was wiederum bedeutet, dass die Monome X^2Z und XYZ in F nicht vorkommen. Somit besitzt F die Form

$$aYZ^2 + bY^2Z + G(X, Y)$$

mit einem homogenen Polynom G vom Grad 3 in X und Y. Da die Kurve irreduzibel ist, muss X^3 in G vorkommen. Wenn man die so gegebene Kurve

mit der Tangente, also mit der Bedingung $Y = 0$ schneidet, so muss $X^3 = 0$ und also $X = 0$ sein, es gibt also genau einen Schnittpunkt mit der Tangente. □

KOROLLAR 5.2. *Es sei $V_+(F) \subseteq \mathbb{P}^2_K$ eine glatte projektive Kurve von Grad 3 über einem algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2, 3$. Dann besitzt die Kurve zumindest einen Wendepunkt.*

Beweis. In der Hesse-Matrix zu F kommen ausschließlich lineare Terme vor. Die Determinante davon ergibt also eine Kurvengleichung vom Grad 3. Diese Kurve schneidet nach Korollar 30.4 (Algebraische Kurven (Osnabrück 2017-2018)) die Ausgangskurve in zumindest einem Punkt. Auf einen solchen Punkt können wir Lemma 5.1 anwenden und erhalten so einen Wendepunkt. □

Da die elliptische Kurve und ebenso die Determinante der Hesse-Matrix den Grad 3 besitzen, gibt es nach dem Satz von Bezout (mit Multiplizitäten gezählt) insgesamt 9 Wendepunkte.

Wir werden nun glatte ebene projektive Kurven vom Grad 3 mit einem Wendepunkt betrachten, den es gemäß Korollar 5.2 bei einem algebraisch abgeschlossenen Körper der Charakteristik $\neq 2, 3$ stets gibt. Wir wollen die Kurvengleichung weiter vereinfachen und weitgehend affin arbeiten. Dazu führen wir eine lineare Transformation derart durch, dass der fixierte Wendepunkt zum Punkt $(0, 1, 0)$ wird und dass die unendlich ferne Gerade $V_+(Z)$ die Tangente durch diesen Punkt wird. Dies bedeutet, dass in der beschreibenden Gleichung die Monome X^2Y, XY^2, Y^3 nicht vorkommen. Die homogene Kurvengleichung kann man dann, wenn man die Variablen noch geeignet streckt, in der Form

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

schreiben.

Weierstraßform

Wir betrachten affine kubische Gleichungen in den Variablen x, y. Eine Gleichung der Form

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

nennt man eine *lange Weierstraß-Gleichung* und eine Gleichung der Form

$$y^2 = x^3 + ax + b$$

eine *kurze Weierstraß-Gleichung*. Die homogene Gestalt der langen Weierstraß-Gleichungen ist

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

und die homogene Gestalt der kurzen Weierstraß-Gleichung ist

$$Y^2Z \;=\; X^3 + aXZ^2 + bZ^3.$$

Auf die lange Form kann man eine elliptische Kurve über einem algebraisch abgeschlossenen Körper der Charakteristik $\neq 2,3$ nach Korollar 5.2 stets bringen, aber auch, wie wir jetzt sehen, auf die kurze Form. Wenn man $Z = 0$ setzt, also den Durchschnitt mit der unendlich fernen Geraden $V_+(Z)$ betrachtet, so erhält man $X^3 = 0$, also den einzigen Schnittpunkt $(0,1,0)$, den man (siehe die nächste Vorlesung) üblicherweise als Nullpunkt der Gruppenverknüpfung auf der elliptischen Kurve wählt.

LEMMA 5.3. *Es sei eine affine kubische Gleichung*

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

über einem Körper der Charakteristik $\neq 2,3$ gegeben. Dann gibt es eine lineare Variablensubstitution derart, dass in den neuen Variablen u, v die Gleichung die Form

$$v^2 \;=\; u^3 + au + b$$

besitzt.

Beweis. Wir schreiben

$$v \;=\; y + \frac{a_1}{2}x + \frac{a_3}{2}.$$

Dann ist

$$\begin{aligned} v^2 &= \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 \\ &= y^2 + a_1xy + a_3y + \frac{1}{2}a_1a_3x + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_3^2 \\ &= x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{2}a_1a_3x + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_3^2 \\ &= x^3 + b_2x^2 + b_1x + b_0, \end{aligned}$$

wobei wir für dieses kubische Polynom neue Bezeichnungen für die Koeffizienten eingeführt haben. Mit der Transformation $u = x + \frac{b_2}{3}$ können wir den quadratischen Term b_2x^2 eliminieren. □

BEISPIEL 5.4. Wir möchten die Fermat-Kubik

$$X^3 + Y^3 + Z^3 \;=\; 0$$

in Charakteristik $\neq 2,3$ auf die kurze Weierstraßform transformieren. Die Hesse-Matrix ist

$$\begin{pmatrix} 6X & 0 & 0 \\ 0 & 6Y & 0 \\ 0 & 0 & 6Z \end{pmatrix}.$$

Daher ist $(0,1,-1)$ ein Wendepunkt der Kurve, den wir nach $(0,1,0)$ transformieren wollen. Wir erreichen dies mit den neuen Variablen $X = X, Y = Y, W = Y + Z$. Die Gleichung wird zu

$$X^3 + Y^3 + (W - Y)^3 \;=\; X^3 + W^3 - 3W^2Y + 3WY^2 \;=\; 0.$$

Die (projektive) Tangente in $(0,1,0)$ wird durch $W = 0$ beschrieben. Die Dehomogenisierung bezüglich W führt auf die affine Gleichung

$$x^3 = 1 - 3y + 3y^2,$$

durch eine quadratische Ergänzung und Normierung entsteht eine Gleichung der Form

$$\tilde{y}^2 = x^3 + b$$

mit $b \neq 0$, was man wiederum über einem algebraisch abgeschlossenen Körper zu 1 normieren kann.

LEMMA 5.5. *Es seien*

$$y^2 = x^3 + ax + b$$

und

$$y'^2 = x'^3 + a'x' + b'$$

kubische Kurven in kurzer Weierstraßform über einem Körper K. Dann gibt es genau dann eine lineare Variablentransformation, die die erste Gleichung in die zweite überführt, wenn es ein $c \in K$, $c \neq 0$, mit

$$c^4 a' = a$$

und

$$c^6 b' = b$$

gibt.

Beweis. Es sei

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Wenn man für x den Term $rx' + sy'$ einsetzt, so entsteht bei $s \neq 0$ ein y'^3-Term, den man durch eine Substitution

$$y = tx' + uy'$$

nicht wegbekommt. Also muss $s = 0$ sein. Damit muss auch $t = 0$ sein, da andernfalls ein x'^2-Term entsteht. Sei also $x = rx'$ und $y = uy'$, was auf die neue Gleichung

$$u^2 y'^2 = r^3 x'^3 + arx' + b$$

führt. Damit man diese sowohl in x' als auch in y' normieren kann, muss

$$u^2 = r^3$$

sein. Dies ist nach Aufgabe 1.10 genau dann der Fall, wenn es ein $c \in K^\times$ mit $u = c^3$, $r = c^2$ gibt. Die Normierung wird dann mittels Division durch c^6 durchgeführt, was auf $a' = ac^2/c^6 = ac^{-4}$ und $b' = b/c^6 = bc^{-6}$ führt. □

Beispiel 5.6. Wir betrachten die elliptischen Kurven der Form $y^2 = x^3 - n^2x$ bzw. $y^2 = x^3 - m^2x$ mit $n, m \in \mathbb{N}_+$, die in Zusammenhang mit den kongruenten Zahlen auftreten. Nach Lemma 5.5 sind die beiden genau dann durch eine lineare Variablentransformation ineinander überführbar, wenn der Quotient $\frac{m^2}{n^2}$ eine vierte Potenz in $\mathbb{Q}$ ist, wenn also $\frac{m}{n}$ ein Quadrat (in $\mathbb{Q}$ und dann bereits) in $\mathbb{Z}$ ist. Bei elliptischen Kurven dieser Bauart kann man sich also auf quadratfreie natürliche Zahlen n beschränken. Wenn man diese Kurven als elliptische Kurven über $\mathbb{C}$ betrachtet, so sind sie alle gleich.

Definition 5.7. Es sei E eine elliptische Kurve über einem Körper K in kurzer Weierstraßform

$$y^2 = x^3 + ax + b.$$

Dann nennt man

$$\Delta = -16(4a^3 + 27b^2)$$

die *Diskriminante* von E.

Vergleiche zur Diskriminante eines kubischen Polynoms auch Satz 1.2 (Körper- und Galoistheorie (Osnabrück 2018-2019)) und Beispiel 8.13 (Körper- und Galoistheorie (Osnabrück 2018-2019)). Die Diskriminante ist genau dann $\neq 0$, wenn das kubische Polynom x^3+ax+b keine mehrfache Nullstelle besitzt, was nach Lemma 4.8 die Glattheit der Kurve bedeutet, siehe Aufgabe 5.4.

Definition 5.8. Es sei E eine elliptische Kurve über einem Körper K in kurzer Weierstraßform

$$y^2 = x^3 + ax + b.$$

Dann nennt man

$$j = \frac{-12^3(4a)^3}{\Delta},$$

wobei Δ die Diskriminante zu E bezeichnet, die *j- Invariante* von E.

Bei der in Lemma 5.5 beschriebenen Transformation ändert sich die j-Invariante der Kurve nicht, siehe Aufgabe 5.10.

Legendresche Normalform

Wir sagen, dass eine elliptische Kurve in Zerlegungsform vorliegt, wenn sie die Gestalt

$$Y^2 = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

mit Elementen $\lambda_i \in K$ besitzt. In diesem Fall kann man durch Verschiebungen und Streckungen auch die sogenannte Legendresche Normalform erreichen.

Definition 5.9. Man sagt, dass eine elliptische Kurve in *Legendrescher Normalform* vorliegt, wenn sie durch eine Gleichung der Form

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

mit $\lambda \in K \setminus \{0, 1\}$ beschrieben wird.

Es ist

$$X(X-1)(X-\lambda) = X^3-(\lambda+1)X^2+\lambda X.$$

Wenn man aus der Legendreschen Normalform die Weierstraßsche Normalform erhalten möchte, so muss man hier den quadratischen Term eliminieren. Wenn Weierstraßsche Normalform vorliegt, so muss das Polynom X^3+aX+b im Allgemeinen keine Faktorzerlegung in Linearfaktoren besitzen. Nach einer endlichen Erweiterung des Körpers und erst recht über einem algebraisch abgeschlossenen Körper ist aber eine solche Zerlegung möglich. Durch Verschieben und Strecken kann man dann erreichen, dass 0 und 1 Nullstellen sind, die dritte Nullstelle kann alles sein und man hat im Allgemeinen keine Optimierungsmöglichkeiten mehr.

LEMMA 5.10. *Es sei K ein Körper der Charakteristik $\neq 2,3$ und es liege eine elliptische Kurve E über K in Legendrescher Normalform*

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

vor. Dann gelten folgende Aussagen.

(1) *Eine kurze Weierstraßgleichung von E ist durch*

$$y^2 = x^3+ax+b$$

mit

$$a = \frac{-\lambda^2+\lambda-1}{3}$$

und

$$b = \frac{-2\lambda^3+3\lambda^2+3\lambda-2}{27}$$

gegeben.

(2) *Die Diskriminante von E ist*

$$\Delta(E) = 2^4\lambda^2(\lambda-1)^2.$$

(3) *Die j-Invariante von E ist*

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

Beweis. (1) Es ist

$$X(X-1)(X-\lambda) = X^3-(\lambda+1)X^2+\lambda X.$$

Mit dem Ansatz

$$X = W+\frac{\lambda+1}{3}$$

ist dies gleich

$$\begin{aligned} & X^3-(\lambda+1)X^2+\lambda X \\ = \ & \left(W+\frac{\lambda+1}{3}\right)^3-(\lambda+1)\left(W+\frac{\lambda+1}{3}\right)^2+\lambda\left(W+\frac{\lambda+1}{3}\right) \end{aligned}$$

$$
\begin{aligned}
&= W^3 + \frac{(\lambda+1)^2 - 2(\lambda+1)(\lambda+1) + 3\lambda}{3} W + \left(\frac{\lambda+1}{3}\right)^3 - (\lambda+1) \\
&\quad \left(\frac{\lambda+1}{3}\right)^2 + \lambda\left(\frac{\lambda+1}{3}\right) \\
&= W^3 + \frac{-(\lambda+1)^2 + 3\lambda}{3} W - 2\frac{(\lambda+1)^3}{27} + \frac{\lambda(\lambda+1)}{3} \\
&= W^3 + \frac{-\lambda^2 + \lambda - 1}{3} W + \frac{-2(\lambda+1)^3 + 9\lambda(\lambda+1)}{27} \\
&= W^3 + \frac{-\lambda^2 + \lambda - 1}{3} W + \frac{-2\lambda^3 + 3\lambda^2 + 3\lambda - 2}{27}.
\end{aligned}
$$

(2) Eine längere Rechnung (siehe Aufgabe 5.13 und Aufgabe 5.14) zeigt

$$
\begin{aligned}
4a^3 + 27b^2 &= \frac{4(-\lambda^2+\lambda-1)^3 + (-2\lambda^3+3\lambda^2+3\lambda-2)^2}{27} \\
&= \frac{-27\lambda^4 + 54\lambda^3 - 27\lambda^2}{27} \\
&= -\lambda^2(\lambda-1)^2.
\end{aligned}
$$

(3) Es ist

$$
\begin{aligned}
j(E) &= -\frac{12^3(4a)^3}{\Delta} \\
&= -\frac{4^3 \cdot 4^3(-\lambda^2+\lambda-1)^3}{2^4\lambda^2(\lambda-1)^2} \\
&= -2^8\frac{(-\lambda^2+\lambda-1)^3}{\lambda^2(\lambda-1)^2} \\
&= 2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.
\end{aligned}
$$

□

Die dritte Nullstelle, also das λ in der Legendreschen Normalform, ist durch die elliptische Kurve nicht eindeutig bestimmt. Stattdessen kann man auch

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

nehmen.

Abbildungsverzeichnis