Eigenschaften elliptische Kurven in Weierstraßscher Normalform

In dieser Vorlesung sei k ein Körper, dessen Charakteristik weder zwei noch drei ist.

Wie wir in der letzten Vorlesung gesehen haben, definiert eine WEIERSTRASS-Gleichung

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

genau dann eine elliptische Kurve, wenn das Polynom auf der rechten Seite keine mehrfache Nullstelle hat. Da dieses Polynom nicht durch Z teilbar ist, sind alle Nullstellen von der Form $(x : 1)$, wobei x eine Nullstelle des inhomogenen Polynoms $f = X^3 + aX + b$ ist. Dieses hat genau dann eine mehrfache Nullstelle, wenn es einen gemeinsamen Faktor positiven Grades mit seiner Ableitung $f' = 3X^2 + a$ hat, wenn also die Resultante

$$\operatorname{Res}_X(f, f') = \begin{vmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{vmatrix} = \begin{vmatrix} 1 & 0 & a & b \\ 0 & a & 0 & 0 \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{vmatrix} + 3 \begin{vmatrix} 0 & a & b & 0 \\ 1 & 0 & a & b \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{vmatrix}$$

$$= \begin{vmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 3 & 0 & a \end{vmatrix} + 3 \begin{vmatrix} 0 & a & b \\ a & 0 & 0 \\ 3 & 0 & a \end{vmatrix} - 3 \begin{vmatrix} a & b & 0 \\ 0 & a & 0 \\ 3 & 0 & a \end{vmatrix} + 3 \cdot 3 \begin{vmatrix} a & b & 0 \\ 0 & a & b \\ 3 & 0 & a \end{vmatrix}$$

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

verschwindet.

Falls sogar $a = b = 0$ ist, steht auf der rechten Seite nur x^3, wir haben also die Spitzenkurve oder NEILsche Parabel $y^2 = x^3$.

Andernfalls kann es keine dreifache Nullstelle geben, denn $(x - c)^3$ hat für $c \neq 0$ einen nichtverschwindenden quadratischen Term. (Hier brauchen wir natürlich die Annahme, daß $\operatorname{char} k \neq 3$ ist; über einem Körper der Charakteristik drei ist $(x-c)^3 = x^3 - c^3$.) Wenn die rechte Seite zwar eine doppelte, aber keine dreifache Nullstelle hat, ist der gemeinsame Faktor von f und f' linear und verschwindet in der doppelten Nullstelle; damit liegt diese im Körper k, und da $X^3 + aX + b$ durch das Quadrat

dieses Linearfaktors teilbar ist, liegt auch die einfache Nullstelle in k. Wenn man das TAYLOR-Polynom von $y^2 - (x^3 + ax^2 + b)$ um den Punkt zu doppelten Nullstelle berechnen, sieht man, daß die Kurve dort zwei verschiedene Tangenten hat, sie schneidet sich also selbst, wie es etwa auch bei der 8 der Fall ist.

Schneiden wir eine kubische Kurve in WEIERSTRASS-Form mit der Geraden $z = 0$, so erhalten wir die Gleichung $x^3 = 0$, d.h. $x = 0$ ist eine dreifache Lösung, und wegen $x = z = 0$ ist $(0 : 1 : 0)$ ein dreifacher Schnittpunkt. Somit liegt der Punkt $(0 : 1 : 0)$ unabhängig von a und b stets auf einer solchen Kurve, und er ist immer ein Wendepunkt.

Beim Beweis, daß jede elliptische Kurve birational äquivalent zu einer Kurve in WEIERSTRASS-Form ist, haben wir viele willkürliche Transformationen ausgeführt; daher stellt sich die Frage, wie eindeutig die WEIERSTRASS-Gleichung durch die Kurve bestimmt ist.

Angesichts der speziellen Form der WEIERSTRASS-Gleichung erscheint ziemlich klar, daß ein Koordinatenwechsel, der die Form der Kurvengleichung erhält, höchstens jede der Variablen durch ein skalares Vielfaches ersetzen kann. Dies ist auch in der Tat der Fall, wenn auch ein elementarer Beweis recht umständlich und langwierig wäre.

Betrachten wir also zwei Koordinatensysteme (X, Y, Z) und (U, V, W) derart, daß $X = \alpha U$, $Y = \beta V$ und $Z = \gamma W$ ist. Natürlich darf keine der drei Konstanten verschwinden, und da wir homogene Koordinaten haben, können wir o.B.d.A. $\gamma = 1$ annehmen. Die Gleichung

$$Y^2 Z = X^3 + aXZ^2 + bZ^3$$

wird in den neuen Koordinaten zu

$$\beta^2 V^2 W = \alpha^3 U + \alpha a U W^2 + bW^3 \,.$$

Daraus können wir genau dann eine WEIERSTRASS-Gleichung machen, wenn $\beta^2 = \alpha^3$ ist, denn dann können wir durch diesen Wert dividieren. Ist $\beta^2 = \alpha^3$ und $\lambda = \alpha/\beta$, so ist

$$\lambda^2 = \frac{\alpha^2}{\beta^2} = \frac{\alpha^2}{\alpha^3} = \frac{1}{\alpha} \qquad \text{und} \qquad \lambda^3 = \frac{\alpha^3}{\beta^3} = \frac{\beta^2}{\beta^3} = \frac{1}{\beta} \,.$$

Somit ist $\beta^{-2} = \alpha^{-3} = \lambda^6$; multiplizieren wir die Gleichung damit, erhalten wir

$$V^2W = U^3 + (\lambda^4 a)UW^2 + (\lambda^6 b)W^3 \,,$$

also eine WEIERSTRASS-Gleichung mit Koeffizienten $\lambda^4 a$ und $\lambda^6 b$.

Wenn es ein $\lambda \in k^\times$ gibt, so daß $a' = \lambda^4 a$ und $b' = \lambda^6 b$ ist, definieren also die beiden WEIERSTRASS-Gleichungen

$$y^2z = x^3 + axz^2 + bz^3 = 0 \qquad \text{und} \qquad y^2z = x^3 + a'xz^2 + b'z^3 = 0$$

zwei Kurven, die durch eine lineare Koordinatentransformation ineinander übergeführt werden können und die wir daher geometrisch nicht als verschieden betrachten wollen: Die Koordinatentransformation $(x : y : z) \mapsto (\lambda^{-2}x : \lambda^{-3}y : z)$ definiert eine Bijektion zwischen den beiden Kurven, die alle geometrischen Eigenschaften erhält.

Für eine elliptische Kurve darf $4a^3 + 27b^2$ nicht verschwinden; für die zweite Kurve ist

$$4a'^3 + 27b'^2 = 4(\lambda^4 a)^3 + 27(\lambda^6 b)^2 = \lambda^{12}(4a^3 + 27b^2) \,,$$

verschwindet also erwartungsgemäß genau dann, wenn auch $4a^3 + 27b^2$ nicht verschwindet.

Definition: $\Delta = 4a^3 + 27b^2$ heißt die *Diskriminante* der elliptischen Kurve $y^2z = x^3 + axz^2 + bx^3$, und

$$j = \frac{4 \cdot 12^3 a^3}{\Delta} = \frac{6912a^3}{4a^3 + 27b^2}$$

heißt j-Invariante.

Die Diskriminante der Kurve $y^2z = x^3 + a'xz^2 + b'z^3$ ist also $\lambda^{12}\Delta$; da aber auch $a'^3(\lambda^4 a)^3 = \lambda^{12}a^3$ ist, sind die j-Invarianten gleich – was auch den Namen erklärt.

Die j-Invariante geht zurück auf FELIX KLEIN, der sich mit der analytischen Theorie elliptischer Funktionen und Kurven beschäftigte. Bei ihm war j eine analytische Funktion, und der seltsame Vorfaktor hier sorgte dafür, daß deren FOURIER-Reihe ganzzahlige Koeffizienten hatte. In der algebraischen Theorie sorgt er dafür, daß man über

beliebigen Körpern, also auch solchen der Charakteristik zwei oder drei (auf deutlich kompliziertere Weise) eine j-Invariante definieren kann, die im Falle char $k \neq 2, 3$ mit der hier definierten übereinstimmt.

Falls der Koeffizient a der WEIERSTRASS-Gleichung verschwindet, ist $j = 0$, und umgekehrt folgt auch $j = 0$ auch, daß a verschwinden muß, denn die Diskriminante einer elliptischen Kurve verschwindet nicht, da diese keine singulären Punkte enthalten darf.

Wenn b verschwindet, ist

$$j = \frac{4 \cdot 12^3 a^3}{4a^3 + 27b^2} = \frac{4 \cdot 12^3 a^3}{4a^3} = 12^3 \,,$$

und umgekehrt folgt aus $j = 12^3$ auch $b = 0$, denn $27b^2 j = 4 \cdot 12^3 - 4a^3 j$ wird hier zu $27 \cdot 12^3 b^2 = 4 \cdot 12^3 a^3 - 4a^3 \cdot 12^3 = 0$.

Im Allgemeinen müssen zwei WEIERSTRASS-Gleichungen mit gleicher j-Invariante keine Kurven definieren, die sich durch eine Koordinatentransformation ineinander überführen lassen. Beispielsweise haben über den reellen Zahlen die beiden Kurven

$$y^2 z = x^3 + xz^2 \qquad \text{und} \qquad y^2 z = x^3 - xz^2$$

beide die gleiche j-Invariante, denn in beiden Fällen ist $b = 0$, also $j = 12^3$. Die beiden Kurven sind allerdings extrem verschieden: In der affinen Ebene haben wir die Gleichungen

$$y^2 = x^3 + x = x(x^2 + 1)$$

und

$$y^2 = x^3 - x = x(x^2 - 1) = (x + 1)x(x - 1) \,.$$

Die Funktion $p(x) = x(x^2+1)$ ist negativ für $x < 0$, verschwindet an der Stelle Null und hat positive Werte für $x > 0$. Auf der Kurve $y^2 = x^3 + x$ gibt es daher keine Punkte mit negativen Koordinaten, für $x = 0$ gibt es genau den Nullpunkt, und für $x > 0$ gibt es zwei Punkte für jede x-Koordinate. Insbesondere ist die Kurve zusammenhängend.

Die Funktion $q(x) = (x + 1)x(x - 1)$ ist negativ für $x < -1$, positiv im Intervall $(-1, 0)$, dann wieder negativ im Intervall $(0,\ 1)$ und schließlich wieder positiv für $x > 0$. Für $x = -1, 0, 1$ verschwindet sie. Die Kurve

$y^2 = x^3 - x$ hat also zwei Komponenten, eine über dem abgeschlossenen Intervall $[-1, 0]$, und eine über der Menge $x \geq 1$.

Es ist klar, daß keine Koordinatentransformation diese beiden Kurven ineinander überführen kann.

Falls der Körper k algebraisch abgeschlossen ist, können allerdings zwei elliptische Kurven mit gleicher j-Invariante stets durch eine Koordinatentransformation ineinander übergeführt werden, d.h. wenn wir die Nullstellenmengen der beiden obigen Gleichungen über den komplexen Zahlen betrachten, können sie ineinander transformiert werden. In der Tat können dort alle Kurven der Form $y^2z = x^3 + axz^2$ mit $a \neq 0$ ineinander transformiert werden, denn ist $y^2z = x^3 + a'xz^2$ eine andere, so können wir stets ein $\lambda \in k$ finden, dessen vierte Potenz gleich a'/a ist, und die Kurve $y^2z = x^3 + a'xz^2 = x^3 + \lambda^4 axz^2$ entsteht aus $y^2z = x^3 + axz^2$ durch Übergang zu den neuen Koordinaten $(\lambda^{-2}x, \lambda^{-3}y, z)$: In der Tat wir die Gleichung

$$(\lambda^{-3}y)^2 z = (\lambda^{-2}x)^3 + a(\lambda^{-2}x)z$$

durch Multiplikation mit λ^6 zu $y^2z = x^3 + \lambda^4 axz^2 = x^3 + a'xz^2$. Im obigen Beispiel bräuchten wir ein λ mit $\lambda^4 = -1$, was es in $\mathbb{R}$ natürlich nicht gibt; in $\mathbb{C}$ können für λ eine der Quadratwurzeln von i nehmen, z.B. $\lambda = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$.

Wir betrachten nun allgemein zwei elliptische Kurven

$$y^2z = x^3 + axz^2 + bz^3 \qquad \text{und} \qquad y^2z = x^3 + a'xz^2 + b'z^3$$

in WEIERSTRASSscher Normalform mit gleicher j-Invariante über einem algebraisch abgeschlossenen Körper k. Falls die j-Invariante verschwindet, müssen a und a' verschwinden, die Gleichungen werden also zu $y^2z = x^3 + bz^3$ und $y^2z = x^3 + b'z^3$, wobei b und b' wegen der Nichtsingularität der Kurven nicht verschwinden dürfen. Da k algebraisch abgeschlossen ist, gibt es (mindestens) ein $\lambda \in k$ mit $\lambda^6 = b'/b$, und die Kurve $y^2z = x^3 + b'z^3 = x^3 + \lambda^6 bz^3$ entsteht aus $y^2z = x^3 + bz^3$ durch Übergang zu den neuen Koordinaten $(\lambda^{-2}x, \lambda^{-3}y, z)$.

Ist $j = 12^3$, so müssen b und b' verschwinden; diesen Fall haben wir gerade oben behandelt.

Sei nun also $j \neq 0, 12^3$; dann sind die vier Zahlen a, b, a' und b' allesamt ungleich Null. Wegen

$$\frac{1}{j} = \frac{4a^3 + 27b^2}{4 \cdot 12^3 a^3} = \frac{1}{12^3} + \frac{27}{4 \cdot 12^3} \frac{b^2}{a^3}$$

muß dann

$$\frac{b^2}{a^3} = \frac{b'^2}{a'^3} \quad \text{und damit} \quad \frac{a'^3}{a^3} = \frac{b'^2}{b^2}$$

sein. Ist $\alpha = a'/a$ und $\beta = b'/b$, so ist also $\alpha^3 = \beta^2$, und für $\mu = \beta/\alpha$ ist

$$\mu^2 = \frac{\beta^2}{\alpha^2} = \frac{\alpha^3}{\alpha^2} = \alpha \qquad \text{und} \qquad \mu^3 = \frac{\beta^3}{\alpha^3} = \frac{\beta^3}{\beta^2} = \beta \,.$$

Wir brauchen ein $\lambda \in k$ mit $\lambda^4 = \alpha$ und $\lambda^6 = \beta$; da k algebraisch abgeschlossen ist, muß es ein λ mit $\lambda^2 = \mu$ geben, und dieses gibt uns die gewünschte Koordinatentransformation.

Damit haben wir gezeigt:

Satz: Ist der Körper k algebraisch abgeschlossen, so können die Kurven mit den WEIERSTRASS-Gleichungen

$$y^2 z = x^3 + axz^2 + bz^3 \qquad \text{und} \qquad yz^2 = x^3 + a'xz^2 + b'z^3$$

genau dann durch eine Koordinatentransformation ineinander übergeführt werden, wenn sie die gleiche j-Invariante haben.

■