WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

4. April 2020

7. Übungsblatt Elliptische Kurven

Aufgabe 1: *(8 Punkte)*

k sei ein Körper mit von von zwei und drei verschiedener Charakteristik.

a) Zeigen Sie: Zwei elliptische Kurven

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

haben genau dann die gleiche j-Invariante, wenn entweder b und b' beide verschwinden oder aber wenn gilt

$$\frac{a^3}{b^2} = \frac{a'^3}{b^2} .$$

Lösung: Wenn b verschwindet, ist

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

und wegen

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

ist für $j = 12^3$ die Diskriminante $4a^3 + 27b^2 = 4a^3$, so daß b verschwinden muß. Somit ist das Verschwinden von b äquivalent zu $j = 12^3$.

a verschwindet offensichtlich genau dann, wenn j verschwindet.

Falls a und b beide nicht verschwinden, ist

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

durch a^3/b^2 eindeutig bestimmt, und ist j weder Null noch 12^3, ist auch

$$\frac{a^3}{b^2} = \frac{27}{4} \frac{j}{12^3 - j}$$

durch j eindeutig bestimmt. Die beiden elliptische Kurven haben somit genau dann die gleiche j-Invariante, wenn entweder $b = b' = 0$ ist oder $a^3/b^2 = a'^3/b'^2$.

b) Welchen Wert hat a^3/b^2, wenn die Gleichung keine elliptische Kurve definiert?

Lösung: Dann verschwindet die Diskriminante $\Delta = 4a^3 + 27b^2$, d.h. $a^3/b^2 = -27/4$.

c) Zeigen Sie, daß es für jedes $j \in k$ eine elliptische Kurve mit diesem Wert als j-Invariante gibt! *(Hinweis: Da k nicht als algebraisch abgeschlossen vorausgesetzt ist, können Sie nicht erwarten, daß Wurzeln existieren. Versuchen Sie stattdessen, zunächst eine Kurve mit einem vorgegebenen Wert von a^3/b^2 zu finden.)*

Lösung: Wenn a^3/b^2 gleich einem vorgegebenen Wert $\lambda \in k$ sein soll, muß $a^3 = \lambda b^2$ sein. Offensichtlich ist $a = b = \lambda$ eine Möglichkeit, das zu erreichen; für $\lambda \neq 0$ können wir also die Kurve

$$y^2z = x^3 + \lambda xz^2 + \lambda z^3$$

nehmen, die für $\lambda \neq -27/4$ nach *b)* eine elliptische Kurve definiert. Nach *a)* ist die Behaptung somit für für alle $j \neq 0, 12^3$ gezeigt. Für $j = 0$ können wir für beliebiges $b \neq 0$ die Kurve $y^2z = x^3 + bz^3$ betrachten, für $j = 12^3$ die Kurve $y^2z = x^3 + axz^2$ für ein beliebiges $a \neq 0$.

d) Zeigen Sie, daß jede elliptische Kurve über $\mathbb{Q}$ eine WEIERSTRASS-Gleichung

$$y^2z = x^3 + axz^2 + bz^3$$

mit ganzen Zahlen a und b hat!

Lösung: Sie hat auf jeden Fall eine solche Gleichung mit $a, b \in \mathbb{Q}$. Ersetzen wir für eine rationale Zahl $\lambda \neq 0$ die Gleichung durch $y^2z = x^3 + \lambda^4 axz^2 + \lambda^6 bz^3$, so entsteht eine Kurve, die durch eine Koordinatentransformation in die gegebene übergeht, und natürlich können wir eine ganze Zahl λ finden mit der Eigenschaft, daß $\lambda^4 a$ und $\lambda^6 b$ beide ganzzahlig sind.

Aufgabe 2: *(6 Punkte)*

a) Welche Gleichung hat die HESSEsche Kurve zu einer elliptischen Kurve in WEIERSTRASS-Normalform?

Lösung: Für $f = Y^2Z - (X^3 + aXZ^2 + bZ^3)$ ist

$$\frac{\partial f}{\partial X} = -3X^2 - aZ^2, \qquad \frac{\partial f}{\partial Y} = 2YZ \quad \text{und} \quad \frac{\partial f}{\partial Z} = Y^2 - 2aXZ - 3bZ^2\,,$$

die zweiten partiellen Ableitungen sind also

$$\frac{\partial^2 f}{\partial X^2} = -6X\,, \quad \frac{\partial^2 f}{\partial X \partial Y} = \frac{\partial^2 f}{\partial Y \partial X} = 0\,, \quad \frac{\partial^2 f}{\partial X \partial Z} = \frac{\partial^2 f}{\partial Z \partial X} = -2aZ\,,$$
$$\frac{\partial^2 f}{\partial Y^2} = 2Z\,, \quad \frac{\partial^2 f}{\partial Y \partial Z} = \frac{\partial^2 f}{\partial Z \partial Y} = 2Y \quad \text{und} \quad \frac{\partial^2 f}{\partial Z^2} = -2aX - 6bZ\,,$$

und die HESSEsche Determinante ist

$$\begin{vmatrix} -6X & 0 & -2aZ \\ 0 & 2Z & 2Y \\ -2aZ & 2Y & -2aX - 6bZ \end{vmatrix} = -6X \cdot \begin{vmatrix} 2Z & 2Y \\ 2Y & -2aX - 6bZ \end{vmatrix} - 2aZ \cdot \begin{vmatrix} 0 & -2aZ \\ 2Z & 2Y \end{vmatrix}$$
$$= 72bXZ^2 + 24aX^2Z + 24XY^2 - 8a^2Z^3\,.$$

Die Gleichung der HESSEschen ist also $72bxz^2 + 24ax^2z + 24xy^2 - 8a^2z^3 = 0\,.$

b) Bestimmen Sie eine WEIERSTRASS-Normalform dieser Kurve!

Lösung: Falls a verschwindet, wird das Polynom zu $72bXZ^2 + 24XY^2$, ist also durch X teilbar, so daß die HESSEsche die Gerade $x = 0$ als Komponente hat. Damit ist sie nicht irreduzibel und kann keine WEIERSTRASS-Normalform haben. Wir müssen daher im folgenden annehmen, daß $a \neq 0$ ist.

Dividieren wir die Gleichung durch acht und vertauschen wir die Variablen X und Z, erhalten wir die Gleichung

$$3y^2z = a^2x^3 - 9bx^2z - 3axz^2 ,$$

die schon ein bißchen an eine WEIERSTRASS-Gleichung erinnert.

Als erstes wollen wir den x^2z-Term eliminieren durch kubische Elimination. Dazu schreiben wir die rechte Seite als

$$a^2\left(x^3 - \frac{9b}{a^2}x^2z - \frac{3}{a}xz^2\right)$$

und ersetzen X durch die neue Variable

$$U = X - \frac{3b}{a^2}$$

ein. Einsetzen von $x = u + 3b/a^2$ in die rechte Seite führt auf die neue rechte Seite

$$a^2u^3 - \left(3a + \frac{27b^2}{a^2}\right)uz^2 - \left(\frac{54b^3}{a^4} + \frac{9b}{a}\right)z^3 .$$

Dividieren wir noch alles durch drei, erhalten wir für die HESSEsche Kurve in den neuen Koordinaten die Gleichung

$$y^2z = \frac{a^2}{3}u^3 - \frac{a^3 + 9b^2}{a^2}uz^2 - \left(\frac{18b^3}{a^4} + \frac{3b}{a}\right)z^3 .$$

Hier stört nur noch der Faktor vor u^3, und den können wir mit dem gleichen Trick eliminieren wie bei der Herleitung der WEIERSTRASSschen Normalform: Wir ersetzen U und Y durch die neuen Variablen

$$V = \frac{a^2}{3}U \quad \text{und} \quad W = \frac{a^2}{3}Y;$$

Z behalten wir bei. Im neuen Koordinatensystem haben wir dann die Gleichung

$$\left(\frac{3w}{a^2}\right)^2 z = \frac{a^2}{3}\left(\frac{3v}{a^2}\right)^3 - \frac{a^3 + 9b^2}{a^2}\left(\frac{3v}{a^2}\right)z^2 - \left(\frac{18b^3}{a^4} + \frac{3b}{a}\right)z^3 .$$

Ausmultipliziert wird das zu

$$\frac{9}{a^4}w^2z = \frac{9}{a^4}v^3 - \frac{3a^3 + 27b^2}{a^4}vz^2 - \left(\frac{18b^3}{a^4} + \frac{3b}{a}\right)z^3 .$$

Nun müssen wir nur noch alles mit $a^4/9$ multiplizieren und erhalten die WEIERSTRASS-Gleichung

$$w^2z = v^3 - \frac{a^3 + 9b^2}{3}vz^2 - \left(\frac{2b^3 + ba^3}{3}\right)z^3 .$$

Aufgabe 3: *(6 Punkte)*

a) Zeigen Sie, daß die Punkte $P = (0 : -1 : 1)$, $Q = (-1 : 0 : 1)$ und $O = (1 : -1 : 0)$ Wendepunkte der Kurve $x^3 + y^3 + z^3 + \lambda xyz = 0$ sind!

Lösung: In Aufgabe drei des fünften Übungsblatts haben wir nachgerechnet, daß die HESSEsche Kurve für $\lambda \neq 0$ die Gleichung

$$x^3 + y^3 + z^3 - \frac{6^3 + \lambda^3}{6\lambda^2} xyz = 0$$

hat; für $\lambda = 0$ erhielten wir $6^3 xyz = 0$. Die Punkte P, Q und O liegen in beiden Fällen auf der HESSEschen und natürlich auch auf der Kurve selbst, sind also Wendepunkte.

b) Nehmen Sie O als Neutralelement, und bestimmen Sie die Summe $P + Q$!

Lösung: Die Gerade durch P und Q hat die Gleichung $x + y + z = 0$; da auch$O$ diese Gleichung erfüllt, ist das der dritte Schnittpunkt, und da wir O als Neutralelement gewählt haben, ist $O = -O$. Somit ist $P + Q = O$.

c) Was ist $2P$?

Lösung: Da P ein Wendepunkt ist, schneidet die Tangente an P mit Vielfachheit drei, der dritte Schnittpunkt ist also P selbst. Somit ist $2P = -P$, und da nach *b)* $P + Q = O$ ist, folgt $2P = Q$.