Wolfgang K. Seiler
Tel. 2515

B6, B4.18

28. März 2020

6. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*
Welche der folgenden Gleichungen definieren in der projektiven Ebene über dem jeweils angegebenen Körper eine elliptische Kurve?

a) $x^3 + y^3 + z^3 = 0$ über $\mathbb{Q}$

Lösung: Das Polynom $X^3 + Y^3 + Z^3$ ist irreduzibel, denn wenn wir beispielsweise Y und Z auf den Wert eins setzen, erhalten wir das über $\mathbb{Q}$ irreduzible Polynom $X^3 + 2$. Die partiellen Ableitungen nach X, Y und Z sind $3X^2$, $3Y^2$ und $3Z^2$; sie verschwinden nur dann simultan, wenn $x = y = z = 0$ ist, und das definiert keinen Punkt der projektiven Ebenen, geschweige denn der Kurve. Somit gibt es keine singulären Punkte. Es gibt aber Punkte mit Koordinaten in $\mathbb{Q}$, beispielsweise $(1, -1, 0)$. Somit definiert diese Gleichung eine elliptische Kurve.

b) $x^3 - z^3 + xy^2 + x^2z - xz^2 - y^2z = 0$ über $\mathbb{R}$

Lösung: Diese Gleichung ist ziemlich symmetrisch in x und z; setzen wir $x = z$, heben sich je zwei der sechs Terme gegenseitig weg. Somit ist die Kurve nicht irreduzibel, sondern enthält die Gerade $x = z$. Damit ist sie keine elliptische Kurve.

c) $y^2 = x(x^2 + x + 1)$ über $\mathbb{R}$

Lösung: Das Polynom $Y^2 - X(X^2 + X + 1)$ kann keinen Faktor haben, der ein Polynom nur in X ist; falls es reduzibel ist, müssen die Faktoren also von der Form $Y -$ Polynom in X sein. Da es keinen in Y linearen Term gibt, müßte es genauer ein Produkt der Form $\big(Y + f(X)\big)\big(Y - f(X)\big) = Y^2 - f(X)^2$ sein, aber das kubische Polynom $X(X^2 + X + 1)$ ist natürlich kein Quadrat. Somit ist das Polynom irreduzibel.

Die partielle Ableitung nach Y ist $2Y$, verschwindet also nur, wenn $y = 0$ ist. Für einen Kurvenpunkt (x, y) mit $y = 0$ muß x eine Nullstelle des Polynome $X(X^2 + X + 1)$ sein. Die partielle Ableitung nach X ist bis aufs Vorzeichen gleich der Ableitung dieses Polynoms in X, und verschwindet in keiner der Nullstellen, da alle drei einfach sind. Bleiben noch die unendlichfernen Punkte, die wir trotz der in affiner Form gegebenen Gleichung natürlich trotzdem betrachten müssen. Die projektive Gleichung ist $y^2z = x(x^2 + xz + z^2)$, für $z = 0$ muß also x^3 und damit auch x verschwinden, so daß $(0 : 1 : 0)$ der einzige unendlichferne Punkt ist. Die partielle Ableitung des homogenisierten Polynoms nach Z ist Y^2, und verschwindet daher nicht in diesem Punkt. Somit sind alle Kurvenpunkte nichtsingulär.

Als Punkt mit Koordinaten in $\mathbb{R}$ haben wir zum Beispiel den unendlichfernen Punkt, aber auch $(0 : 0 : 1)$ und viele andere. Also ist die Kurve elliptisch.

d) $3x^3 + 4y^3 + 6z^3 = 0$ über $\mathbb{Q}$

Lösung: Hier gibt es keinen Punkt mit Koordinaten aus $\mathbb{Q}$: Wäre $(x : y : z)$ ein solcher Punkt, könnten wir o.B.d.A. annehmen, daß x, y, z zueinander teilerfremde ganze Zahlen sind. Da $3x^3 = -4y^3 + 6z^3$ ist, müßte $x = 2x'$ eine gerade Zahl sein. Einsetzen zeigt, daß dann $6z^3 = -24x'^3 + 4y^3$ ist, also müßte auch $z = 2z'$ gerade sein. Damit ist schließlich $4y^3 = -24x'^3 - 48z'^3$; da die rechte Seite durch acht teilbar ist, müßte also auch y gerade sein, im Widerspruch zur vorausgesetzten Teilerfremdheit. Damit definiert diese Gleichung keine elliptische Kurve.

e) $xyz + xy^2 + yz^2 = 0$ über $\mathbb{C}$

Lösung: Hier können wir y ausklammern, die Kurve enthält also die Gerade $y = 0$ und ist somit nicht irreduzibel, also auch keine elliptische Kurve.

f) $y^2z = x^3 + 2x^2 + x$ über $\mathbb{R}$

Lösung: Auf der rechten Seite können wir x ausklammern und erhalten die Gleichung

$$y^2z = x(x^2 + 2x + 1) = x(x + 1)^2 .$$

Das Polynom auf der rechten Seite hat also $x = -1$ als doppelte Nullstelle, und im Punkt $(-1 : 0 : 1)$ verschwinden alle drei partiellen Ableitungen. Also gibt es einen singulären Punkt, und die Kurve ist nicht elliptisch.

Aufgabe 2: *(6 Punkte)*

a) Finden Sie alle Punkte auf der Kurve $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2(\mathbb{F}_7)$!

Lösung: In $\mathbb{F}_7$ ist $0^3 = 0$, $1^3 = 1$, $2^3 = 1$, $3^3 = 6$, $4^3 = 1$, $5^3 = 6$ und $6^3 = 6$; dritte Potenzen sind also nur die drei Elemente $0, 1$ und 6. Die Summe von dreier dieser Zahlen verschwindet somit genau dann, wenn entweder alle gleich Null sind oder aber jeder genau einmal vorkommt. Dritte Potenz Null hat nur die Null, und es gibt keinen Punkt mit drei Koordinaten Null. In den anderen Fällen muß eine der Koordinaten Null sein, eine zweite entweder 1 oder 2 oder 4, und die dritte 3, 5 oder 6. Dies ergibt die Punkte

$$\begin{gathered}(0 : 1 : 3), (0 : 1 : 5), (0 : 1 : 6),\\ (0 : 2 : 3), (0 : 2 : 5), (0 : 2 : 6),\\ (0 : 4 : 3), (0 : 4 : 5), (0 : 4 : 6)\end{gathered}$$

und deren sämtliche Permutationen.

Wären die neun angegebenen Punkte alle verschieden, hätte die Kurve mindestens neun Schnittpunkte mit der Geraden $x = 0$, was nach Bézout nur dann möglich ist, wenn diese Gerade eine Komponente ist. Das ist natürlich nicht der Fall, denn $X^3 + Y^3 + Z^3$ ist nicht durch X teilbar. Also müssen jeweils drei dieser Punkte gleich sein, und in der Tat ist

$$\begin{gathered}(0 : 1 : 3) = (0 : 2 : 6) = (0 : 4 : 3), \quad (0 : 1 : 5) = (0 : 2 : 3) = (0 : 4 : 6)\\ \text{und} \quad (0 : 1 : 6) = (0 : 2 : 5) = (0 : 4 : 3) .\end{gathered}$$

Da es sechs Permutationen der drei Positionen gibt und nie zwei Koordinaten übereinstimmen, gibt es also achtzehn verschiedene Punkte, die wir zum Beispiel in der Form $(0 : 1 : 3)$, $(0 : 1 : 5)$ und $(0 : 1 : 6)$ und allen Permutationen davon darstellen können.

b) Finden Sie alle Punkte auf der Kurve $y^2z = x^3 + z^3$ in $\mathbb{P}^2(\mathbb{F}_5)$!

Lösung: Der einzige Punkt mit $z = 0$ ist $(0 : 1 : 0)$; für die übrigen Punkte können wir mit der affinen Gleichung $y^2 = x^3 + 1$ rechnen. Quadrate in $\mathbb{F}_5$ sind $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ und $4^2 = 1$, also $0, 1$ und 4. Für $x = 0$ ist $x^3 + 1 = 1$ ein Quadrat; dies führt auf die beiden Punkte $(0, 1)$ und $(0, 4)$. Für $x = 1$ ist $x^3 + 1 = 2$ kein Quadrat, also gibt es keine Punkte mit x-Koordinate eins. Für $x = 2$ ist $x^3 + 1 = 4$ ein Quadrat; wir erhalten die beiden Punkte $(2, 2)$ und $(2, 3)$. Für $x = 3$ ist $x^3 + 1 = 3$ kein Quadrat, für $x = 4$ ist $x^3 + 1 = 0$ ein Quadrat, und wir erhalten den Punkt $(4, 0)$. Die Kurve besteht also aus dem Punkt O sowie den affinen Punkten $(0, 1)$, $(0, 4)$, $(2, 2)$, $(2, 3)$ und $(4, 0)$. Insgesamt gibt es damit sechs Punkte.

c) Finden Sie alle Punkte auf der Kurve $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2(\mathbb{Q})$!

Lösung: Jeder Punkt in $\mathbb{P}^2(\mathbb{Q})$ kann auch durch ganzzahlige homogene Koordinaten dargestellt werden; es reicht also, nach ganzen Zahlen x, y, z zu suchen, für die $x^3+y^3+z^3$ verschwindet. Für diese ist auch $x^3+y^3 = (-z)^3$, und nach der FERMATschen Vermutung, die für Exponent drei schon lange vor WILES bewiesen wurde, hat diese Gleichung keine Lösung, für die nicht mindestens eine der drei Zahlen x, y, z verschwindet. Somit sind $(1 : -1 : 0)$, $(1 : 0 : -1)$ und $(0 : 1 : -1)$ die einzigen Punkte.

Aufgabe 3: *(5 Punkte)*
Finden Sie eine WEIERSTRASSsche Normalform für die Kurve $x^3+y^3+az^3 = 0$ mit $a \neq 0$ in $\mathbb{P}^2(\mathbb{Q})$!
Hinweis: Finden Sie zunächst einen Punkt auf der Kurve und transformieren Sie das Koordinatensystem so, daß dieser zum Punkt $(0 : 1 : 0)$ wird!

Lösung: Offensichtlich liegt für jedes $a \in \mathbb{Q}^\times$ der Punkt $(1 : -1 : 0)$ auf der Kurve. Die Transformation $(x, y, z) \mapsto \left(\frac{1}{2}(x + y), \frac{1}{2}(x - y), z\right)$ bildet $(1 : -1 : 0)$ auf $(0 : 1 : 0)$ ab; in den neuen Variablen $U = \frac{1}{2}(X + Y)$ und $V = \frac{1}{2}(X - Y)$ ist $X = U + V$ und $Y = U - V$; die neue Kurvengleichung wird also zu

$$(u + v)^3 + (u - v)^3 + az^3 = 2u^3 + 6uv^2 + az^3 = 0 \quad \text{oder} \quad 6uv^2 = -2u^3 - az^3 .$$

Wenn wir U als das neue Z nehmen, Z als das neue X und V als das neue Y, ist das schon recht nahe an einer WEIERSTRASS-Gleichung:

$$6y^2z = -ax^3 - 2z^3 \quad \text{oder} \quad \frac{-6}{a}y^2z = x^3 + \frac{2}{a}z^3 .$$

Ersetzen wir jetzt noch Z durch $Z' = -(6/a)Z$, d.h. $Z = -(a/6)Z'$, erhalten wir die WEIERSTRASS-Gleichung

$$Y^2Z' = X^3 - \frac{2}{a} \cdot \frac{a^3}{6^3}Z'^3 = X^3 - \frac{a^2}{3 \cdot 6^2}Z'^3 .$$

(Es gibt auch andere Transformationen, die auf etwas andere WEIERSTRASS-Gleichungen führen können.)

Aufgabe 4: *(3 Punkte)*

Untersuchen Sie für die folgenden rationalen Abbildungen der projektiven Ebene auf sich selbst, wo sie definiert sind und wo sie injektiv sind!

a) $(x : y : z) \mapsto (x : x : z)$

Lösung: $(x : x : z)$ ist für $x = z = 0$ kein Punkt der projektiven Ebene; daher ist die Abbildung im Punkt $(0 : 1 : 0)$ nicht definiert. Sie ist nirgends injektiv, den $(x : y : z)$ ist für jedes y aus dem Grundkörper ein Urbild von $(x : x : z)$.

b) $(x : y : z) \mapsto (x^2z : xy^2 : yz^2)$

Lösung: Falls zwei der Koordinaten verschwinden, sind alle drei Komponenten des Bildpunkts Null, d.h. in den Punkten $(0 : 0 : 1)$, $(0 : 1 : 0)$ und $(1 : 0 : 0)$ ist die Abbildung nicht definiert.

Falls keine der drei Koordinaten verschwindet, ist

$$(x^2z : xy^2 : y^2z) = \left(\frac{x^2z}{xyz} : \frac{xy^2}{xyz} : \frac{yz^2}{xyz}\right) = \left(\frac{x}{y} : \frac{y}{z} : \frac{z}{x}\right) ;$$

setzt man irgendeine der Koordinaten, zum Beispiel x willkürlich auf eins, lassen sich y und z über die Verhältnisse x/y und z/x eindeutig berechnen. Für Punkte mit $xyz \neq 0$ ist die Abbildung also injektiv.

Bleiben noch die Punkte, in denen genau eine der Koordinaten verschwindet. Im Falle $x = 0$ ist der Bildpunkt $(0 : 0 : yz^2) = (0 : 0 : 1)$, d.h. die ganze Gerade $x = 0$ wird auf den Punkt $(0 : 0 : 1)$ abgebildet. Entsprechend geht die Gerade $y = 0$ auf den Punkt $(1 : 0 : 0)$ und $z = 0$ auf $(0 : 1 : 0)$.

c) Wie sehen die beiden Abbildungen aus, wenn man sie auf die affine (x, y)-Ebene einschränkt?

Lösung: Dort können wir $z = 1$ setzen; dann wird der Bildpunkt bei der ersten Abbildung zu $(x : x : 1)$, d.h. wir haben einfach die Projektion $(x, y) \mapsto (x, x)$ in y-Richtung auf die Winkelhalbierende des ersten Quadranten.

Bei der zweiten Abbildung wird der Bildpunkt zu $(x^2 : xy^2 : y^2)$; in der affinen Ebene also zu

$$\left(\frac{x^2}{y^2}, x\right) .$$

Bei dieser Einschränkung der Bildmenge ist die Abbildung nur noch für $y \neq 0$ definiert.