Algebra I

Musterlösung 12

Elliptische Kurven in der projektiven Ebene

---

76. Gegeben sei die Ellipse $e\colon 8x^2 + 15y^2 - 6xy - 18x - 6y - 9 = 0$ in $\mathbb{R}^2$ sowie der Punkt $P = (0, 1)$ auf der Ellipse.

(a) Schreibe die Gleichung der Ellipse in homogenen Koordinaten. Welcher Punkt in der projektiven Ebene entspricht P?

(b) Bestimme den zweiten Schnittpunkt Q der Geraden $Y - Z = 0$ mit der Ellipse.

(c) Bestimme die beiden Geradengleichungen der Tangenten an die Ellipse durch die Punkte P und Q.

(d) Finde eine projektive Transformation, welche die Gerade PQ auf $X = 0$ abbildet und die beiden Tangenten auf $Y = 0$ *bzw.* $Z = 0$ abbildet.

(e) Bestimme die Gleichung der Bildkurve der Ellipse unter dieser Transformation.
Hinweis: Die Bildkurve der Ellipse unter dieser Transformation ist eine Parabel.

Lösung: (a) In homogenen Koordinaten lautet die Gleichung

$$8X^2 + 15Y^2 - 6XY - 18XZ - 6YZ - 9Z^2 = 0.$$

Der Punkt P wird dann zu $(0, 1, 1)$.

(b) In die Gleichung aus (a) setzen wir $Y = Z$ und erhalten

$$8X^2 - 24XY = X(8X - 24Y) = 0.$$

Somit ist der zweite Schnittpunkt $Q = (24, 8, 8) = (3, 1, 1)$.

(c) Wir bilden den Gradienten der Ellipsengleichung

$$(16x - 6y - 18, 30y - 6x - 6)$$

und finden durch Einsetzen von $P = (0, 1)$, dass die Tangente die Form

$$-24x + 24y = 24$$

haben muss. Durch -24 dividiert und homogenisiert lautet die Gleichung für die Tangente an P

$$0 = X - Y + Z.$$

Dasselbe mit $Q = (3, 1, 1)$ wiederholt ergibt die Gleichung

$$0 = 4X + Y - 13Z.$$

(d) Sei A die gesuchte Transformation. Für einen Punkt (a, b, c) mit $b = c$ soll gelten, dass die x-Koordinate von $A(a, b, c)$ gleich null ist. Das ist erfüllt, wenn die erste Zeile von A die

Koeffizienten der Geradengleichung $0 \cdot X + Y - Z = 0$ enthält. Also können wir die Matrix direkt aus den Geradengleichungen entnehmen, indem wir die Koeffizienten von X, Y, Z in die Zeilen schreiben. Somit ist die Transformation

$$A = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 1 \\ 4 & 1 & -13 \end{pmatrix}.$$

(e) Um die Ellipse in den neuen Koordinaten zu schreiben, müssen wir die Inverse von A berechnen. Wiederum spielt Multiplikation mit einem Skalar keine Rolle. Es gilt

$$A^{-1} = \begin{pmatrix} 12 & 3 & 0 \\ 17 & 1 & 1 \\ 5 & 1 & 1 \end{pmatrix}$$

und somit

Es gilt $A \cdot X = Y - 7Z, A \cdot Y = 8X - Y - Z, A \cdot Z = -8X + Y + 25Z$. Damit transformieren wir

$$\begin{aligned} 0 &= 8X^2 + 15Y^2 - 6XY - 18XZ - 6YZ - 9Z^2 \\ &= 8(12\tilde{X} + 3\tilde{Y})^2 + 15(17\tilde{X} + \tilde{Y} + \tilde{Z})^2 - 6(12\tilde{X} + 3\tilde{Y})(17\tilde{X} + \tilde{Y} + \tilde{Z}) \\ &\quad - 18(12\tilde{X} + 3\tilde{Y})(5\tilde{X} + \tilde{Y} + \tilde{Z}) - 6(17\tilde{X} + \tilde{Y} + \tilde{Z})(5\tilde{X} + \tilde{Y} + \tilde{Z}) - 9(5\tilde{X} + \tilde{Y} + \tilde{Z})^2 \\ &= 34\tilde{X}^2 - \tilde{Y}\tilde{Z}. \end{aligned}$$

Das ist offensichtlich eine Parabel.

77. Bestimme mit der Parabel aus Aufgabe 76 alle rationalen Punkte in $\mathbb{R}^2$ auf der Ellipse.

Lösung: Alle rationalen Punkte in $\mathbb{R}^2$ der Parabel aus der letzten Aufgabe sind

$$\left\{(a, 34a^2) : a \in \mathbb{Q}\right\}.$$

In der Projektiven Ebene werden diese Punkte als $(a, 34a^2, 1)$ geschrieben und es kommt noch der Punkt $(1, 34, 0)$ im Unendlichen hinzu. Mit der Abbildung A transformieren wir diese zu Punkten auf der Ellipse zurück, nämlich

$$\begin{aligned} A(a, 34a^2, 1) &= (34a^2 - 1, -34a^2 + a + 1, 34a^2 + a + 13) \\ &= \left(\frac{34a^2 - 1}{34a^2 + a + 13}, \frac{-34a^2 + a + 1}{34a^2 + a + 13}, 1\right) \end{aligned}$$

und $A(1, 34, 0) = (34, -33, 38) = (\frac{17}{19}, -\frac{33}{38}, 1)$. Die rationalen Punkte auf der ursprünglichen Ellipse sind daher

$$\left\{\left(\frac{34a^2 - 1}{34a^2 + a + 13}, \frac{-34a^2 + a + 1}{34a^2 + a + 13}\right) : a \in \mathbb{Q}\right\} \cup \left\{\left(\frac{17}{19}, -\frac{33}{38}, 1\right)\right\}.$$

78. Zeige: Ist $P = (x, y)$ ein rationaler Punkt auf der Kurve $C[a, b]$, so gilt

$$x = \frac{m}{e^2} \quad \text{und} \quad y = \frac{n}{e^3}$$

mit $m, n, e \in \mathbb{Z}$ und $(m, e) = 1 = (n, e)$.

Lösung: Seien $x = \frac{m}{p}$ und $y = \frac{n}{q}$ die Darstellung von x und y als gekürzte Brüche mit positivem Nenner. Einsetzen in die Kurvengleichung und Multiplikation mit p^3q^2 ergibt

$$n^2p^3 = m^3q^2 + am^2pq^2 + bmp^2q^2.$$

Wegen $\mathrm{ggT}(n, q) = 1$ gilt $q^2|p^3$. Genauso sehen wir $p|q^2$. Das wieder in obige Gleichung eingesetzt impliziert aber $p^2|m^3q^2$, also $p|q$, und dies wieder eingesetzt ergibt $p^3|q^2$. Somit stimmt die behauptete Aussage mit $e = \frac{q}{p}$.

Eine positive natürliche Zahl k heisst ***kongruente Zahl***, falls es positive rationale Zahlen a, b, c gibt, für die gilt:

$$a^2 + b^2 = c^2 \quad \text{und} \quad \tfrac{1}{2}ab = k.$$

Mit anderen Worten ist k eine kongruente Zahl, falls k der Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten ist.

Sei nun n eine positive natürliche Zahl. Dann definieren wir

$$K_n := \{(a, b, c) \in \mathbb{Q}^3 \mid a, b, c > 0,\ a^2 + b^2 = c^2,\ \tfrac{1}{2}ab = n\}.$$

Weiter sei die Kurve C_n wie folgt definiert:

$$C_n : y^2 = x^3 - n^2x$$

Es sei V_n die Menge aller rationalen Punkte auf C_n im ersten Quadranten von $\mathbb{Q}^2$:

$$V_n := C_n(\mathbb{Q}) \cap \{(x, y) \in \mathbb{Q}^2 \mid x, y > 0\}.$$

79. Zeige, dass für eine kongruente Zahl n ein Punkt $(x, y) \in V_n$ existiert, welcher

$$x = \left(\frac{p}{2q}\right)^2$$

erfüllt, das heisst, x ist das Quadrat einer rationalen Zahl mit geradem Nenner.

Hinweis: Finde eine Bijektion

$$\{x \in \mathbb{Q} : x - n, x, x + n \text{ Quadrate in } \mathbb{Q}\} \to \{(a, b, c) \in K_n : a < b < c\}.$$

Lösung: Sei x so, dass $x + n, x - n, x$ Quadrate in $\mathbb{Q}$ sind. Es gilt

$$(\sqrt{x+n} - \sqrt{x-n})^2 + (\sqrt{x+n} + \sqrt{x-n})^2 = (2\sqrt{x})^2.$$

Daraus sehen wir, dass

$$x \mapsto (\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x})$$

eine Bijektion ist mit Umkehrabbildung

$$(a, b, c) \mapsto \left(\frac{c}{2}\right)^2.$$

Es bleiben zwei Dinge zu zeigen, nämlich:

- Die Zahl $\left(\frac{c}{2}\right)^2$ ist eine mögliche x-Koordinate eines rationalen Punktes auf der Kurve C_n: $y^2 = x^3 + n^2x$.
- Sei $c = \frac{p}{q}$ die Darstellung als gekürzter Bruch, dann ist p ungerade.

Um die erste Aussage zu zeigen, bemerken wir zuerst, dass wir die Gleichung $y^2 = x^3 - n^2 x$ zu

$$\frac{y^2}{x} = x^2 - n^2$$

umschreiben können. Weiter gilt für $(a, b, c) \in K_n$

$$(a+b)^2 = c^2 + 4n$$
$$(a-b)^2 = c^2 - 4n$$

und daher

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2.$$

Also ist

$$\left(\left(\frac{c}{2}\right)^2, \left(\frac{a^2 - b^2}{c^2}\right)\right)$$

ein rationaler Punkt auf C_n. Für die zweite Aussage seien $a = \frac{p_1}{q_1}, b = \frac{p_2}{q_2}$ gekürzte Brüche. Wir zeigen zuerst, dass dann auch der Bruch $\frac{p_1^2 q_2^2 + p_2^2 q_1^2}{q_1^2 q_2^2}$ gekürzt ist. Da $\frac{1}{2}ab = \frac{p_1 p_2}{2 q_1 q_2} \in \mathbb{N}$ ist, gilt $q_1 | p_2$ und $q_2 | p_q$. Ein gemeinsamer Teiler von q_1 und q_2 müsste daher p_2 teilen. Da q_2 und p_2 teilerfremd sind, folgt $\mathrm{ggT}(q_1, q_2) = 1$ und folglich gilt auch $\mathrm{ggT}(q_1, p_1 q_2) = 1 = \mathrm{ggT}(q_2, p_2 q_1)$. Somit ist obiger Bruch gekürzt. Daraus folgt $p_1^2 q_2^2 + p_2^2 q_1^2 = p^2$. Da n quadratfrei ist, gilt $\mathrm{ggT}(p_1, p_2) \in \{1, 2\}$, aber $8 \nmid p_1 p_2$. Falls p_1 und p_2 beide gerade sind, ist $p_1^2 q_2^2 + p_2^2 q_1^2$ durch 8, aber nicht durch 16, teilbar, denn $(\frac{p_1}{2})^2 q_2^2 + (\frac{p_2}{2})^2 q_1^2$ ist als Summe der Quadrate zweier ungerader Zahlen kongruent 2 modulo 4. Somit ist auch q^2 durch 8, aber nicht durch 16 teilbar, was für ein Quadrat einer natürlichen Zahl nicht sein kann. Daher muss entweder p_1 oder p_2, aber nicht beide, ungerade sein und folglich ist auch p ungerade.

80. (a) Finde eine Bijektion $V_n \to K_n$. Folgere, dass n genau dann eine kongruente Zahl ist, wenn $V_n \neq \emptyset$ gilt.

(b) Sei n eine kongruente Zahl. Zeige: Ist $P = (x, y) \in V_n$, so tritt für $2P = (x', y')$ genau einer der folgenden Fälle ein:

$$2P \in V_n, \qquad -2P \in V_n, \qquad y' = 0$$

(c) Finde zur kongruenten Zahl 6 mindestens zwei rechtwinklige Dreiecke mit rationalen Seiten der Fläche 6.

Lösung: (a) Bezeichne die gesuchte Bijektion mit $\varphi = (\varphi_a, \varphi_b, \varphi_c) \colon V_n \to K_n$. Wir schreiben die Gleichung zu

$$n = \frac{nx(x+n)(x-n)}{y^2} = \frac{1}{2}\varphi_a(x,y)\varphi_b(x,y)$$

um. Wir raten, dass

$$\varphi_a(x,y) = \frac{(x+n)(x-n)}{y}, \varphi_b(x,y) = \frac{2nx}{y}$$

eine Bijektion liefern könnte. Es ist dann

$$\varphi_c = \frac{x^2 + n^2}{y}.$$

Um zu zeigen, dass das eine Bijektion ist, berechnen wir den Kandidaten für die Umkehrabbildung

$$(a, b, c) \mapsto (x, y) = \left(\frac{n(a+c)}{b}, \frac{2n^2(a+c)}{b^2} \right)$$

und rechnen durch Einsetzen nach, dass das auch tatsächlich die Umkehrabbildung ist. Die zweite Aussage folgt sofort.

(b) Offensichtlich schliessen sich die drei Möglichkeiten gegenseitig aus. Aus der Vorlesung kennen wir die Formel für $2P$, ihre x-Koordinate lautet

$$x' = \frac{x^4 + 2n^2x^2 + n^4}{4x^3 - 4n^2x} = \frac{(x^2 + n^2)^2}{4x(x^2 - n^2)}$$

und ist für alle rationalen Zahlen x positiv. Die y-Koordinate $y' = \sqrt[3]{x'(x'+n)(x'-n)} = 0$ ist genau dann gleich 0, wenn $x' = n$ ist. Anderenfalls ist entweder y' oder $-y'$ ebenfalls positiv.

(c) Für $n = 6$ kennen wir das pythagoräische Tripel $(3, 4, 5)$. Dieses korrespondiert nach der vorherigen Aufgabe zu einem rationalen Punkt auf der Kurve C_{36}, nämlich $(12, 36)$. Mit der obigen Formel können wir diesen nun zu einem Punkt mit x-Koordinate $\frac{25}{4}$ verdoppeln. Daraus können wir ein Pythogaräisches Tripel basteln, nämlich

$$\left(\frac{49}{16y}, \frac{75}{y}, \frac{1201}{16y} \right).$$

Die Bedingung an den Flächeninhalt ergibt $y = \frac{35}{8}$. Somit ist das Tripel

$$\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70} \right).$$