Elliptische Kurven und Kryptographie

Serie 3

Schnittpunkte von Kurven vom Grad ≤ 3 Musterlösungen

---

9. Beweise die folgende Aussage:

(a) Für jeden Punkt P der reellen projektiven Ebene existieren zwei Geraden G_1 und G_2 durch P, sodass jede Gerade G durch P in der Form

$$\alpha G_1 + \beta G_2 = 0 \qquad (\text{mit } \alpha, \beta \in \mathbb{R})$$

geschrieben werden kann.

Beweis:

Ohne Einschränkung (bzw. bis auf projektive Transformation) sei $P = (0, 0, 1)$. Eine Gerade durch P ist dann von der Form $G\colon\ aX + bY = 0$. Seien $G_1\colon\ X = 0$ und $G_2\colon\ Y = 0$, dann erhalten wir G für $\alpha = a$ und $\beta = b$.

10. Beweise die folgenden Aussagen:

(a) Sind $P_1, \ldots, P_4$ vier verschiedene Punkte der reellen projektiven Ebene, sodass keine drei Punkte auf einer Geraden liegen, so existieren zwei Kegelschnitte K_1 und K_2 durch $P_1, \ldots, P_4$, sodass jeder Kegelschnitt K durch $P_1, \ldots, P_4$ in der Form

$$\alpha K_1 + \beta K_2 = 0 \qquad (\text{mit } \alpha, \beta \in \mathbb{R})$$

geschrieben werden kann.

(b) Ist P_0 ein Punkt, der verschieden ist von $P_1, \ldots, P_4$, so existiert genau ein Kegelschnitt durch $P_0, \ldots, P_4$.

(c) Seien $P_1 = (1, 1, 1)$, $P_2 = (-1, 1, 1)$, $P_3 = (-1, -1, 1)$, $P_4 = (1, -1, 1)$.
Finde jeweils einen Kegelschnitt durch $P_1, \ldots, P_4$ sowie durch:
(i) $P_0 = (0, 2, 1)$ (ii) $P_0 = (1, 2, 1)$ (iii) $P_0 = (0, 0, 1)$ (iv) $P_0 = (1, 0, 0)$

Beweis:

(a) Ohne Einschränkung (bzw. bis auf projektive Transformation) seien $P_1, \ldots, P_4$ wie in Teil (c) und seien $K_1\colon\ x^2 - 1 = 0$ und $K_2\colon\ y^2 - 1 = 0$ zwei verschiedene Geradenpaare durch diese Punkte. Ein beliebiger Kegelschnitt K durch $P_1, \ldots, P_4$ ist a priori von der Form

$$K\colon\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_{13}x + a_{23}y + a_{33} = 0\,.$$

Setzen wir nun $P_1, \ldots, P_4$ ein, so erhalten wir das Gleichungssystem

$$\begin{aligned} a_{11} + a_{12} + a_{22} + a_{13} + a_{23} + a_{33} &= 0 \\ a_{11} - a_{12} + a_{22} - a_{13} + a_{23} + a_{33} &= 0 \\ a_{11} + a_{12} + a_{22} - a_{13} - a_{23} + a_{33} &= 0 \\ a_{11} - a_{12} + a_{22} + a_{13} - a_{23} + a_{33} &= 0 \end{aligned}$$

Daraus folgt $a_{12} = a_{13} = a_{23} = 0$ und $a_{33} = -(a_{11} + a_{22})$. Also gilt $K = a_{11}K_1 + a_{22}K_2$.

(b) Ein weiterer Punkt $P_0 = (X_0, Y_0, Z_0)$ liefert uns also die Gleichung

$$a_{11}X_0^2 + a_{22}Y_0^2 - (a_{11} + a_{22})Z_0^2 = 0\,,$$

welche sich nach a_{11} oder a_{22} auflösen lässt. Die letzte Unbekannte in der Gleichung von K lässt sich dann frei in $\mathbb{R}^*$ wählen.

(c) i. Wir erhalten die Gleichung

$$4a_{22} - (a_{11} + a_{22}) = 0\,,$$

also zum Beispiel $K\colon 3x^2 + y^2 - 4 = 0$.

ii. $K\colon x^2 - 1 = 0$.

iii. $K\colon x^2 - y^2 = 0$.

iv. $K\colon y^2 - 1 = 0$.

11. Beweise den folgenden SATZ VON CHASLES (1837):

Einer cubischen Kurve C sei ein Sechseck mit den Punkten $P_1, \ldots, P_6$ und den Seiten $S_1 = \overline{P_1P_2}$, $S_2 = \overline{P_2P_3}$, $S_3 = \overline{P_3P_4}$, $S_4 = \overline{P_4P_5}$, $S_5 = \overline{P_5P_6}$, $S_6 = \overline{P_6P_1}$ einbeschrieben.

Liegen dann die Schnittpunkte $S_1 \wedge S_4$ und $S_2 \wedge S_5$ auf C, so liegt auch $S_3 \wedge S_6$ auf C.

Beweis: Definiere die beiden kubischen Kurven $C_1 := S_1 \cdot S_3 \cdot S_5$ und $C_2 := S_2 \cdot S_4 \cdot S_6$. Diese schneiden sich genau in den 9 erwähnten Punkten (d. h. in den 6 Ecken und den 3 Seitenschnittpunkten). Nun geht jede kubische Kurve, die durch 8 dieser Punkte geht, ebenfalls durch den 9-ten, entsprechend auch unsere Kurve C.

12. Beweise den folgenden SATZ VON PASCAL (1640):

Einem nicht zerfallenden Kegelschnitt K sei ein Sechseck mit den Punkten $P_1, \ldots, P_6$ und den Seiten $S_1 = \overline{P_1P_2}$, $S_2 = \overline{P_2P_3}$, $S_3 = \overline{P_3P_4}$, $S_4 = \overline{P_4P_5}$, $S_5 = \overline{P_5P_6}$, $S_6 = \overline{P_6P_1}$ einbeschrieben.

Dann liegen die drei Schnittpunkte $S_1 \wedge S_4$, $S_2 \wedge S_5$, $S_3 \wedge S_6$ auf einer Geraden.

Hinweis: Ist K ein Kegelschnitt und G eine Gerade, dann ist $K \cdot G = 0$ eine cubische Kurve.

Beweis:

Definiere C_1 und C_2 wie oben, die Gerade G durch $S_1 \wedge S_4$ und $S_2 \wedge S_5$ sowie die kubische Kurve $C := K \cdot G$. Dann liegt der Punkt $S_3 \wedge S_6$ auf C. Er kann nicht auf K liegen, da K nicht zerfällt, liegt also wie gewünscht auf G.