Aufgabe F18T2A1 (12 Punkte)

(a) Definieren Sie den Begriff *Integritätsbereich*.

(b) Formulieren Sie den *Kleinen Satz von Fermat*.

(c) Sei $a \in \mathbb{Z}$ und $f = x^3 + ax^2 - (3+a)x + 1 \in \mathbb{Q}[x]$. Zeigen Sie, dass f keine Nullstelle in $\mathbb{Q}$ hat.

(d) Seien $P_1, P_2, ..., P_5 \in \mathbb{R}^2$ mit $P_j = (x_j, y_j)$ für $j = 1, ..., 5$. Zeigen Sie, dass $P_1, ..., P_5$ auf einem (möglicherweise entarteten) Kegelschnitt liegen, d.h. es gibt $a, b, c, d, e, f \in \mathbb{R}$, nicht alle null, mit

$$ax_j^2 + bx_jy_j + cy_j^2 + dx_j + ey_j + f = 0 \qquad \text{für alle } j \in \{1, 2, 3, 4, 5\}.$$

Hinweis: Betrachten Sie ein geeignetes lineares Gleichungssystem für a, b, c, d, e, f.

Lösung:

zu (a) Ein Integritätsbereich ist ein Ring R, in dem 0 der einzige Nullteiler ist. Dabei wird ein Element $a \in R$ Nullteiler genannt, wenn ein $b \in R$ mit $b \neq 0$ und $ab = 0$ existiert.

zu (b) Der kleine Satz von Fermat besagt, dass $a^p \equiv a \bmod p$ für jede ganze Zahl a und jede Primzahl p gilt.

zu (c) Weil f ein ganzzahliges normiertes Polynom ist, ist laut Vorlesung jede rationale Nullstelle r von f ganzzahlig und ein Teiler des konstanten Terms 1. Also kommen nur ± 1 als rationale Nullstellen von f in Frage. Es gilt $f(1) = 1+a-(3+a)+1 = -1 \neq 0$ und ebenso $f(-1) = (-1)^3+a(-1)^2-(3+a)(-1)+1 = -1+a+3+a+1 = 2a+3 \neq 0$, denn aus $2a+3 = 0$ würde $a = -\frac{3}{2}$ folgen, im Widerspruch zu $a \in \mathbb{Z}$. Dies zeigt, dass f in $\mathbb{Q}$ keine Nullstellen besitzt.

zu (d) Die Punkte $P_1, ..., P_5$ liegen genau dann auf dem (möglicherweise entarteten) Kegelschnitt

$$K \quad = \quad \{(x, y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 + dx + ey + f = 0\} \quad ,$$

wenn das Tupel $(a, b, c, d, e, f) \in \mathbb{R}^6$ eine Lösung des homogenen linearen Gleichungssystems (LGS) bestehend aus den Gleichungen

$$x_j^2X_1 + x_jy_jX_2 + y_j^2X_3 + x_jX_4 + y_jX_5 + X_6 = 0 \quad , \quad 1 \leq j \leq 5$$

ist. Aus der Linearen Algebra ist bekannt, dass der Lösungsraum eines homogenen reellen LGS bestehend aus endlich vielen Gleichungen in n Unbekannten ein $(n-r)$-dimensionaler Untervektorraum von $\mathbb{R}^n$ ist, wobei r den Rang der Koeffizientenmatrix bezeichnet. Dieser Rang kann höchstens so groß sein wie die Anzahl m der Gleichungen. Hier ist $n = 6$ und $m = 5$, also $r \leq 5$. Dies zeigt, dass der Lösungsraum eine Dimension $6 - r \geq 6 - 5 = 1$ besitzt, er ist also mindestens eindimensional. Insbesondere enthält er ein Element ungleich $0_{\mathbb{R}^6}$, also ein Tupel (a, b, c, d, e, f), dessen Einträge nicht alle Null sind.