Elliptische Kurven und Kryptographie

Serie 0

zur reellen projektiven Ebene — Musterlösungen

---

0. (a) Gegeben seien die beiden projektiven Geraden

$$G_1 : X - 2Y + 3Z = 0 \qquad \text{und} \qquad G_2 : 2X - Z = 0\,.$$

Bestimme den Schnittpunkt von G_1 und G_2.

(b) Gegeben seien die beiden projektiven Punkte

$$P_1 = (1, -2, 3) \qquad \text{und} \qquad P_2 = (2, 0, -1)\,.$$

Bestimme die Gerade durch P_1 und P_2.

1. In Abhängigkeit vom reellen Parameter u definieren wir die Transformationsmatrix T_u wie folgt:

$$T_u := \begin{pmatrix} \cosh(u) & 0 & \sinh(u) \\ 0 & 1 & 0 \\ \sinh(u) & 0 & \cosh(u) \end{pmatrix}$$

(a) Bestimme das Bild K' unter T_u des Einheitskreises

$$K : X^2 + Y^2 - Z^2 = 0\,.$$

(b) Seien G_1 und G_2 die beiden Tangenten vom Punkt $(1, 0, 0)$ an K.
Bestimme die Bilder G_1' und G_2' unter T_u der Geraden G_1 und G_2, sowie deren Berührungspukte mit K'.

2. Zeige, dass unter projektiven Transformationen Doppelverhältnisse erhalten bleiben.

0. a) $G_2: 2X - Z = 0 \iff Z = 2X$, eingesetzt in $G_1: 7X - 2Y = 0 \iff 7X = 2Y$.

Wähle z.B. $X = 2$ und erhalte $P = (2, 7, 4) \hat{=} (1/2, 7/4, 1)$.

b) Dual zu (a) erhalten wir $G: 2X + 7Y + 4Z = 0$.

1. Bem.: $\forall u \in \mathbb{R}: T_u^{-1} = T_{-u}$.

a) Es gilt: $(X, Y, Z)^t$ liegt auf $K \iff$
$T_u(X, Y, Z)^t$ liegt auf K', also
$(X, Y, Z)^t$ liegt auf $K' \iff T_{-u}(X, Y, Z)^t$ liegt auf K, d.h.

$$K': (\cosh(u)X - \sinh(u)Z)^2 + Y^2 - (-\sinh(u)X + \cosh(u)Z)^2 = 0$$

was sich jedoch vereinfacht zu $X^2 + Y^2 - Z^2 = 0$.

b) Eine Gerade durch $P_1 = (1, 0, 0)$ ist von der Form
$G: vY + wZ = 0$, OE: $v = 1$, d.h. $Y = -wZ$, eingesetzt in $K: X^2 + w^2Z^2 - Z^2 = 0 \iff X^2 = (1 - w^2)Z^2$. Nun wollen wir genau einen Punkt in $G \cap K$, also $w^2 = 1$ und somit $w_1 = -1$, $w_2 = 1$, d.h. $G_1: Y - Z = 0$
$G_2: Y + Z = 0$

$G_1': \sinh(u)X + Y - \cosh(u)Z = 0$
$G_2': -\sinh(u)X + Y + \cosh(u)Z = 0$

Die Berührpunkte von G_1 und G_2 an K sind

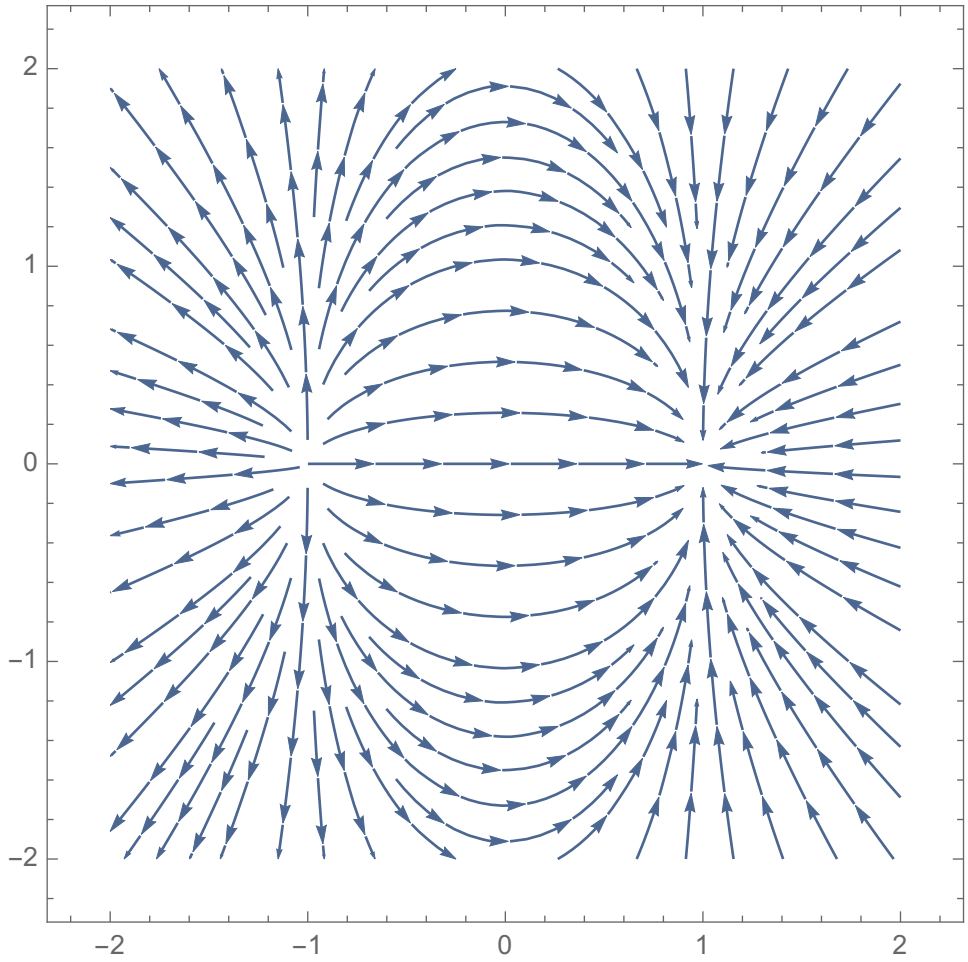
$Q_1 = (0, 1, 1)$ bzw. $Q_2 = (0, -1, 1)$

und deren Bilder sind

$Q_1' = (\sinh u, 1, \cosh u)$ bzw.
$Q_2' = (\sinh u, -1, \cosh u)$

1. Ergänzung:

   Im Folgenden ist der StreamPlot zu T_u für wachsendes u im Bereich $[-2,2]^2$ abgebildet. In $\mathbb{R}^3$ besitzt T_u die Eigenvektoren $(0,1,0)$, $(-1,0,1)$ und $(1,0,1)$. Dies sind auch gerade die Koordinaten der Fixpunkte von T_u in der projektiven Ebene.

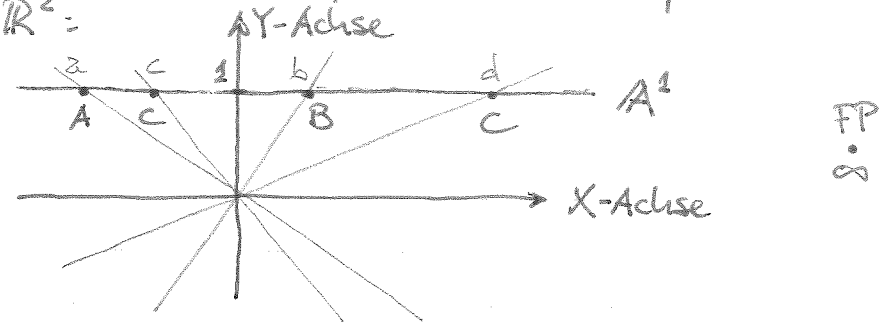


Eine zentrale Eigenschaft von proj. Transformationen ist durch folgenden Satz gegeben:

Satz 9.3. Doppelverhältnisse bleiben unter projektiven Transformationen erhalten.

Beweis: [2015: auf die letzte Vorlesung verschoben]

Seien A, B, C, D vier Punkte auf einer Geraden G. In $\mathbb{R}^3$ haben wir also 4 $\mathbb{R}^3$-Geraden a, b, c, d auf einer $\mathbb{R}^3$-Ebene E. In E wählen wir ein Koord.-System so, dass keine der 4 $\mathbb{R}^3$-Geraden mit der x-Achse zusammenfällt und identifizieren E mit $\mathbb{R}^2$:



Die Ebene E ist eine projektive Gerade welche aufgefasst werden kann als affine Gerade $\mathbb{A}^1$ zusammen mit einem Fernpunkt FP.

Auf der proj. Geraden hat A die Form $A = \begin{pmatrix} x_A \\ y_A \end{pmatrix}$; wählen wir den Repräsentanten auf $\mathbb{A}^1$ so erhalten wir

$$\begin{pmatrix} x_A/y_A \\ 1 \end{pmatrix} =: \begin{pmatrix} \alpha \\ 1 \end{pmatrix}$$

Analog definieren wir β, γ, δ.

Es gilt nun:

$$DV(ABCD) = \frac{\frac{\gamma-\alpha}{\beta-\gamma}}{\frac{\delta-\alpha}{\beta-\delta}} = \frac{(\gamma-\alpha)\cdot(\beta-\delta)}{(\delta-\alpha)\cdot(\beta-\gamma)}$$

Sei nun φ eine proj. Transformation. Dann bildet φ die Gerade G auf eine Gerade G' ab, bzw. die Ebene E auf eine Ebene E'. Identifizieren wir E' mit E, so induziert φ eine lin. Abbildung $\varepsilon: E \to E$, d.h. ε ist eine lin. Abb. $\mathbb{R}^2 \to \mathbb{R}^2$. Im gewählten Koord.-System entspricht ε einer 2×2 Matrix mit $\det(\varepsilon) = 1$;

$$\varepsilon: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{mit} \quad ad - bc = 1$$

Die Abbildung ε bildet die Punkte A, B, C, D auf A', B', C', D' ab. Es gilt z.B.

$$\varepsilon(A) = A' = \varepsilon \cdot \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} a\alpha + b \\ c\alpha + d \end{pmatrix} = \begin{pmatrix} \frac{a\alpha+b}{c\alpha+d} \\ 1 \end{pmatrix}$$

Für das Doppelverhältnis der Bildpunkte, also $DV(A'B'C'D')$ erhalten wir:

$$\frac{\left(\frac{a\gamma+b}{c\gamma+d} - \frac{a\alpha+b}{c\alpha+d}\right)\cdot\left(\frac{a\beta+b}{c\beta+d} - \frac{a\delta+b}{c\delta+d}\right)}{\left(\frac{a\delta+b}{c\delta+d} - \frac{a\alpha+b}{c\alpha+d}\right)\cdot\left(\frac{a\beta+b}{c\beta+d} - \frac{a\gamma+b}{c\gamma+d}\right)} =$$

$$= \ldots = DV(ABCD) \qquad \dashv$$

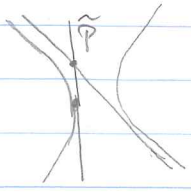
Bemerkungen:
- Wie bei proj. Trans. bleiben DV auch bei Basistransformationen erhalten.

Badeball mit Polkappen

Typen von KS:
- Kreis/Ellipse (0 ∞)
- Parabel (1 ∞)
- Hyperbel (2 ∞)

- Bei proj. Transformationen und Basiswechseln gehen Kegelschnitte (bzw. quadratische Kurven) in Kegelschnitte über. Insbesondere geht ein Kreis in einen Kegelschnitt über.

Beispiel: $K: 2X^2 - 3Y^2 + XY + XZ + 5YZ - 2Z^2 = 0$



Basiswechsel:

$$\begin{array}{ccc} \tilde{P}_1 & \tilde{P}_2 & \tilde{P}_3 \\ \begin{pmatrix} -7 & -1 & 3 \\ 7 & 1 & -2 \\ 5 & 1 & 0 \end{pmatrix} \end{array}$$

$X = (-7\tilde{X} - \tilde{Y} + 3\tilde{Z})$
$Y = (7\tilde{X} + \tilde{Y} - 2\tilde{Z})$
$Z = (5\tilde{X} + \tilde{Y})$

$\Rightarrow 4X^2 + YZ = 0$ bzw. $y = -4x^2$

Hauptnenner von Zähler und Nenner sind gleich und kürzen sich weg; wir erhalten:

Zähler: $((a\gamma+b)\cdot(c\alpha+d)-(a\alpha+b)\cdot(c\gamma+d))\cdot((a\beta+b)\cdot(c\delta+d)-(a\delta+b)\cdot(c\beta+d))$

$= (\cancel{ac\alpha\gamma}+ad\gamma+bc\alpha+\cancel{bd}-\cancel{ac\alpha\gamma}-bc\gamma-ad\alpha-\cancel{bd})\cdot(ad\beta+cb\delta-ad\delta-bc\beta)$

$= \underbrace{(ad(\gamma-\alpha)-bc(\gamma-\alpha))}_{\boxed{ad-bc=1}\ (\gamma-\alpha)}\cdot\underbrace{(ad(\beta-\delta)-bc(\beta-\delta))}_{(\beta-\delta)} = (\gamma-\alpha)\cdot(\beta-\delta)$

Nenner: $\ldots\quad(\delta-\alpha)\cdot(\beta-\gamma)$

$$\Rightarrow DV(A'B'C'D') = \frac{(\gamma-\alpha)\cdot(\beta-\delta)}{(\delta-\alpha)\cdot(\beta-\gamma)} = DV(ABCD)$$