Wolfgang K. Seiler
Tel. 2515

B6, B4.18

16. März 2020

4. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*
Die Kurve $C \subset \mathbb{P}^2(k)$ sei gegeben durch die Gleichung

$$(x^2 + y^2)^2 - 2a^2(x^2 - y^2)z^2 = 0$$

mit einem Parameter $a \in k$, k algebraisch abgeschlossener Körper.

a) Bestimmen Sie die Schnittpunkte von C mit der Geraden $z = 0$!

Lösung: Setzen wir in der Kurvengleichung $z = 0$, so bleibt $(x^2 + y^2)^2 = 0$ übrig, also $x^2 + y^2 = (x + iy)(x - iy) = 0$, wobei $i \in k$ eine Nullstelle des Polynoms $X^2 + 1$ ist. Die beiden Schnittpunkte sind daher $(1 : i : 0)$ und $(i : 1 : 0)$.

b) In welchen Punkten hat C eine Tangente der Form $x = \lambda z$, in welchen eine der Form $y = \lambda z$?

Lösung: In der affinen Ebene $z \neq 1$ ist die Kurve gegeben durch die Gleichung

$$f(x, y) = (x^2 + y^2)^2 - 2a^2(x^2 - y^2) = 0\,,$$

und die gesuchten Tangenten haben die Gleichung $x = \lambda$ *bzw.* $y = \lambda$, sind also parallel zur y- *bzw.* x-Achse, so daß dort die partielle Ableitung von f nach y *bzw.* x verschwinden muß.

$$\frac{\partial f}{\partial x} = 4x(x^2 + y^2) - 4a^2x = 4x(x^2 + y^2 - 4a^2)$$

verschwindet, wenn entweder x verschwindet oder $x^2 + y^2 = a^2$ ist.

$$f(0, y) = y^4 + 2a^2y^2 = y^2(y^2 + 2a^2)\,;$$

die Kurvenpunkte mit x-Koordinate Null sind also $(0, 0)$ und $(0, \pm i\sqrt{2})$.
Setzen wir $x^2 + y^2 = a^2$ in die Kurvengleichung ein, erhalten wir

$$a^4 - 2a^2(x^2 - y^2) = a^4 - 2a^2(2x^2 - a^2) = a^2(a^2 - 4x^2 + 2a^2) = a^2(3a^2 - 4x^2) = 0\,;$$

es gibt also die beiden Lösungen $x = \pm\frac{\sqrt{3}}{2}a$. Wegen $x^2 + y^2 = a^2$ ist dann $y = \pm\frac{1}{2}a$, wir haben also die vier Punkte $(\pm\frac{\sqrt{3}}{2}a, \pm\frac{1}{2}a)$.
Bei der partiellen Ableitung nach y geht die Diskussion weitgehend analog: Jetzt muß entweder $y = 0$ sein, was auf die Punkte $(0, 0)$ und $(0, \pm\sqrt{2})$ führt, oder $x^2 + y^2 + a^2 = 0$. Setzen wir $x^2 + y^2 = -a^2$ in die Kurvengleichung ein, erhalten wir

$$a^4 - 2a^2(x^2 - y^2) = a^4 - 2a^2(2x^2 + a^2) = a^2(a^2 - 4x^2 - 2a^2) = -a^2(a^2 + 4x^2) = 0\,.$$

Jetzt gibt es die beiden Lösungen $x = \pm\frac{i}{2}a$. Wegen $x^2 + y^2 = a^2$ ist dann $y = \pm\frac{i\sqrt{3}}{2}a$, wir haben also die vier Punkte $(\pm\frac{i}{2}a, \pm\frac{i\sqrt{3}}{2}a)$.

c) Bestimmen Sie die Tangente(n) an C im Punkt $(0 : 0 : 1)$!

Lösung: Wir wissen bereits, daß es dort sowohl eine waagrechte als auch eine senkrechte Tangente gibt, was natürlich nur die x- und die y-Achse sein kann. Falls es noch weitere gäbe, müste der Punkt mindestens Vielfachheit drei haben; da

$$\frac{\partial^2 f}{\partial x^2} = 12x^2 + 4y^2 - 4a^2$$

dort den Wert $-4a^2 \neq 0$ hat, ist dies nicht der Fall.

Aufgabe 2: *(8 Punkte)*

a) Welche Gleichung(en) muß das Koeffizientenpaar

$$\big((a_1 : b_1 : c_1), (a_2 : b_2 : c_2)\big) \in \mathbb{P}^2(k) \times \mathbb{P}^2(k)$$

erfüllen, damit das lineare Gleichungssystem

$$a_1x + b_1y + c_1z = 0 \quad \text{und} \quad a_2x + b_2y + c_2z = 0$$

einen zweidimensionalen Lösungsraum hat?

Lösung: Der Lösungsraum ist genau dann zweidimensional, wenn die beiden Gleichungen proportional zueinander sind, d.h. wenn $a_1 : a_2 = b_1 : b_2 = c_1 : c_2$ ist. Dies läßt sich durch die drei Polynomgleichungen

$$a_1b_2 = a_2b_1, \quad a_1c_2 = a_2c_1 \quad \text{und} \quad b_1c_2 = b_2c_1\ .$$

b) Zeigen Sie, daß sich $\mathbb{P}^2(k) \times \mathbb{P}^2(k)$ einbetten läßt in $\mathbb{P}^8(k)$, indem das Punktepaar aus $(a_1 : a_2 : a_3)$ und $(b_1 : b_2 : b_3)$ abgebildet wird auf den Punkt mit Koordinaten $c_{ij} = a_ib_j$ für $i, j = 1, 2, 3$!

Lösung: Wir betrachten also die Abbildung

$$\begin{cases} \mathbb{P}^2(k) \times \mathbb{P}^2(k) \to \mathbb{P}^8(k) \\ \big((a_1 : a_2 : a_3), (b_1 : b_2 : b_3)\big) \mapsto (c_{11} : c_{12} : c_{13} : c_{21} : c_{22} : c_{23} : c_{31} : c_{32} : c_{33}) \end{cases}$$

mit $c_{ij} = a_ib_j$. Sie ist wohldefiniert, d.h. es kann nicht passieren, daß alle c_{ij} verschwinden, denn es gibt stets mindestens ein $a_i \neq 0$ und mindestens ein $b_j \neq 0$. Werden die Koordinaten von $(a_1 : a_2 : a_3)$ oder $(b_1 : b_2 : b_3)$ mit einer Konstanten multipliziert, werden auch alle c_{ij} damit multipliziert, so daß sich der Bildpunkt nicht ändert.

Als nächstes müssen wir zeigen, daß die Abbildung injektiv ist. Sei also $(c_{11} : c_{12} : c_{13} : c_{21} : c_{22} : c_{23} : c_{31} : c_{32} : c_{33})$ Bild der beiden Punktepaare $\big((a_1 : a_2 : a_3), (b_1 : b_2 : b_3)\big)$ und $\big((a'_1 : a'_2 : a'_3), (b'_1 : b'_2 : b'_3)\big)$. Wie wir uns bereits überlegt haben, muß mindestens ein c_{ij} von Null verschieden sein; für dessen Indizes i, j kann dann keine der vier Zahlen a_i, a'_i, b_j und b'_j verschwinden. Wir können daher, ohne die Punkte zu verändern, die Koordinaten so normieren, daß $a_i = a'_i = b_j = b'_j = 1$ ist; damit wird auch $c_{ij} = 1$. Für ein beliebiges $\ell \in \{1, 2, 3\}$ ist dann c_{hj} gleich $a_hb_j = a_h$, aber auch gleich $a'hb'_j = a'_h$, d.h. $a_h = a'_h$. Genauso ist $c_{ih} = b_h = b'_h$, d.h. die beiden Punktepaare stimmen überein.

c) Welche Polynome verschwinden auf dem Bild dieser Einbettung?

Lösung: Wegen der Definition $c_{ij} = a_ib_j$ ist

$$c_{ij}c_{h\ell} = a_ib_ja_hb_\ell = a_ib_\ell a_hb_j = c_{i\ell}c_{hj}\ ,$$

d.h. alle Polynome $c_{ij}c_{h\ell} - c_{i\ell}c_{hj}$ verschwinden auf dem Bild.

d) Welche weiteren Polynome verschwinden in den Bildern jener Punkte, die die Bedingung aus *a)* erfüllen?

Lösung: Umgeschrieben auf die neuen Koordinaten $(a_1 : a_2 : a_3)$ und $(b_1 : b_2 : b_3)$ erfüllen diese die drei Polynomgleichungen

$$a_1b_2 = a_2b_1, \quad a_1b_3 = a_3b_1 \quad \text{und} \quad a_2b_3 = a_3b_2\,,$$

d.h. im Bild ist $c_{12} = c_{21}$, $c_{13} = c_{31}$ und $c_{23} = c_{32}$.

Aufgabe 3: *(2 Punkte)*
Welche Gleichung(en) müssen die Koordinaten dreier Punkte aus $\mathbb{P}^2$ erfüllen, wenn die drei Punkte bezüglich Geraden nicht in allgemeiner Lage sind?

Lösung: Wenn die drei Punkte $P_i = (x_i : y_i : z_i)$ bezüglich Geraden nicht in allgemeiner Lage sind, heißt das, daß sie auf einer Geraden liegen, d.h. die drei Tripel (x_i, y_i, z_i) sind linear abhängig. Das ist genau dann der Fall, wenn die Determinante

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}$$

verschwindet.

Aufgabe 4: *(4 Punkte)*
$\mathcal{L}_d$ sei das lineare System aller Kurven vom Grad $d \geq 1$ in $\mathbb{P}^2(k)$. Zeigen Sie, daß es im projektiven Raum $\mathcal{L}_d$ endlich viele Hyperflächen (d.h. Nullstellenmengen eines homogenen Polynoms in den Koordinaten) gibt, so daß jeder Divisor $D \in \mathcal{L}_d$, der *nicht* die Form $D = C$ hat mit einer irreduziblen Kurve C vom Grad d, auf mindestens einer dieser dieser Hyperflächen liegt!

Lösung: Wir identifizieren $\mathcal{L}_d$ mit dem projektiven Raum zum Vektorraum der Koeffizientenvektoren homogener Polynome d-ten Grades in drei Veränderlichen. Falls der Divisor zu einem solchen Polynom F nicht gleich einer irreduziblen Kurve ist, ist F als Produkt zweier Polynome positiven Grades darstellbar, d.h. es gibt homogene Polynome G_1, G_2 mit Graden $d_1, d_2 \geq 1$ und $d_1 + d_2 = d$, so daß $F = G_1G_2$ ist. Die Polynommultiplikation läßt sich interpretieren als eine Abbildung $\mathcal{L}_{d_1} \times \mathcal{L}_{d_2} \to \mathcal{L}_d$; falls F keine irreduzible Kurve definiert, liegt der zugehörige Punkt von $\mathcal{L}_d$ also im Bild einer solchen Abbildung.
Wie wir wissen, hat $\mathcal{L}_d$ die Dimension

$$\binom{d+2}{2} - 1 = \frac{(d+1)(d+2)}{2} - 1 = \binom{d^2+3d}{2}\,.$$

Da $(d_1 + d_2)^2 > d_1^2 + d_2^2$ für $d_1, d_2 \geq 1$, ist die Summe der Dimensionen von $\mathcal{L}_{d_1}$ und $\mathcal{L}_{d_2}$ echt kleiner als die Dimension von $\mathcal{L}_d$; das Bild obiger Abbildung muß daher in einer Hyperfläche liegen. Wählen wir zu jedem Paar (d_1, d_2) mit $d_1, d_2 \geq 1$ und $d_1 + d_2 = d$ eine solche Hyperfläche, erhalten wir endlich viele Hyperflächen, für die die zu beweisende Behauptung gilt.