Übungen zur Vorlesung **Blatt 5**
Elliptische Kurven und Kryptographie 18.05.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 1. Juni 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

(a) Sei k ein Körper der Charakteristik 0 und $F(X,Y,Z) \in k[X,Y,Z] \setminus k$ homogen vom Grad d. Zeigen Sie, dass F die Eulersche Differentialgleichung

$$X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} + Z\frac{\partial F}{\partial Z} = dF$$

löst.

(b) Ein Punkt $P = [a:b:c]$ der projektiven Kurve $\mathcal{C}_F(k)$ ist genau dann singulär, wenn der entsprechende Punkt $P' = [a:b:1]$ von $\mathcal{C}_F(k) \cap \mathbb{A}^2(k)$ singulär ist.

Aufgabe 2:

(a) Die Bernoullische Lemniskate ist die Kurve $\mathcal{C}_f$ mit $f(x,y) = (x^2+y^2)^2 - 2(x^2-y^2)$. Bestimmen Sie alle singulären Punkte von $\mathcal{C}_{F_f} \subset \mathbb{P}^2(\mathbb{C})$.

(b) Für eine Kurve $\mathcal{C}$ sei $\operatorname{sing}\mathcal{C}$ die Menge ihrer singulären Punkte. Sei k ein algebraisch abgeschlossener Körper und $f, g \in k[x,y] \setminus k$. Zeigen Sie

$$\operatorname{sing}\mathcal{C}_{F_f G_g} = \operatorname{sing}\mathcal{C}_{F_f} \cup \operatorname{sing}\mathcal{C}_{G_g} \cup (\mathcal{C}_{F_f} \cap \mathcal{C}_{G_g}).$$

Aufgabe 3:

Ist $F \in \mathbb{C}[X_1, X_2, X_3]$ homogen vom Grad $d \geq 2$, so heißt

$$H_F := \Big(\frac{\partial^2 F}{\partial X_i \partial X_j}\Big)_{1 \leq i,j \leq 3}$$

die Hesse–Matrix von F. Definiert F eine Kurve $\mathcal{C}_F \subset \mathbb{P}^2(\mathbb{C})$ und gilt $\deg(\det H_F) \geq 1$, so heißt $H(\mathcal{C}_F) := \mathcal{C}_{\det H_F}$ die Hesse–Kurve von $\mathcal{C}_F$.
Man kann zeigen: Ein glatter Punkt $P \in \mathcal{C}_F$ ist genau dann Wendepunkt, wenn $P \in H(\mathcal{C}_F)$.

(a) Zeigen Sie $\deg(\det H_F) = 3(d-2)$, falls $\det H_F \neq 0$.
(b) Bestimmen Sie alle Wendepunkte der Fermatkubik $\mathcal{C}_F \subset \mathbb{P}^2(\mathbb{C})$ mit $F(X_1,X_2,X_3) = X_1^3 + X_2^3 + X_3^3$. (Hinweis: F ist irreduzibel. Sie dürfen Aufgabe 4, Teil (a) verwenden.)

Aufgabe 4:

Gegeben sei eine projektive Kurve $\mathcal{C}_F \subset \mathbb{P}^2(\mathbb{C})$. Zeigen Sie:

(a) Ist F irreduzibel vom Grad $d \geq 2$ und enthält $\mathcal{C}_F$ keine Gerade, so besitzt $\mathcal{C}_F$ höchstens $3d(d-2)$ Wendepunkte.
(b) Ist $\mathcal{C}_F$ nichtsingulär, so ist F irreduzibel.
(c) Ist F irreduzibel, besitzt $\mathcal{C}_F$ höchstens endlich viele singuläre Punkte.