Eberhard Karls Universität Tübingen Wintersemester 2018/19
Fachbereich Mathematik
PD Dr. Jörg Zintl

Elliptische Funktionen und elliptische Kurven

Übungsaufgaben zum 8. Tutorium am 11.12.2018

Aufgabe 29
Seien $(C_1, \mathcal{O}_1)$ und $(C_2, \mathcal{O}_2)$ elliptische Kurven über einem algebraisch abgeschlossenen Körper k. Sei $m \in \mathbb{Z}$ und $0 \neq \varphi \in \mathrm{End}(C)$. Zeigen Sie:

$$\begin{array}{rccc} (i) & \varphi \circ [m] & = & [m] \circ \varphi \\ (ii) & (\varphi^\vee)^\vee & = & \varphi \\ (iii) & [m]^\vee & = & [m] \\ (iv) & \deg(\varphi^\vee) & = & \deg(\varphi) \\ (v) & \deg([m]) & = & m^2. \end{array}$$

Aufgabe 30
Consider the plane projective curve $C_p := V(F_p)$ over $\mathbb{F}_p$, where

$$F_p(X, Y, Z) := Y^2Z - X^3 - XZ^2 \mod p \in \mathbb{F}_p[X, Y, Z]$$

for some prime number $p \in \mathbb{N}$. Let $\mathcal{O} = (0 : 1 : 0) \in C$.

a) Let $p = 3$. Compute the group table of the elliptic curve $(C_3, \mathcal{O})$.

b) Let $p = 7$. Show that $P = (3 : 4 : 1)$ is an element of order 8 in $(C_7, \mathcal{O})$, and compute the group order $|C_7|$.

Keine Abgabe, nur zur Vorbereitung auf das Tutorium!