Fachbereich Mathematik und Statistik
Dr. Michele Serra
Prof. Dr. Salma Kuhlmann
SS 2023

Universität Konstanz

Introduction to Elliptic Curves

Exercise Sheet 3
Endomorphisms of Elliptic Curves

Exercise 9 *Inseparable polynomials in positive characteristic* **(4 points)**
Let K be a field. Recall that a polynomial $f(X) \in K[X]$ is called *separable* if $f'(X)$ is not identically zero. It is called *inseparable* otherwise.
Now let $\operatorname{char} K = p > 0$. Show that a polynomial $f(X) \in K[X]$ is inseparable if and only if there exists a polynomial $h(X) \in K[X]$ such that $f(X) = h(X^p)$.

Exercise 10 **(2+2+3+1 points)**
Let E be an elliptic curve over a field K and let $\varphi \in \operatorname{End}(E)$ be a non-zero separable endomorphism In this exercise we establish that

(i) $\varphi\colon E(\bar{K}) \to E(\bar{K})$ is surjective.

(ii) For all $P \in E(\bar{K})$ we have $|\varphi^{-1}(P)| = |\ker(\varphi)|$.

(iii) $|\ker(\varphi)| = \deg(\varphi)$.

(a) Let $Q \in E(\bar{K})$ be such that $\varphi^{-1}(Q) \neq \emptyset$. Show that $|\varphi^{-1}(Q)| = |\ker(\varphi)|$. Showing (i) will then imply (ii).

(b) Let φ have degree m and be given by the rational functions

$$\varphi(X, Y) = (r_1(X), r_2(X)Y) = \left(\frac{a(X)}{c(X)}, \frac{b(X)}{d(X)}Y\right)$$

with $\gcd(a, c) = \gcd(b, d) = 1$. Consider the following sets

$$\begin{aligned}
S_1 &= \{Q = (u, v) \in E(\bar{K}) : u = 0 \text{ or } \deg(uc(X) - a(X)) < \deg(\varphi)\};\\
S_2 &= \{Q = (u, v) \in E(\bar{K}) : \exists x \in \bar{K} \text{ s.t. } u = r_1(x) \wedge r_1'(x) = 0\};\\
S_3 &= \{Q = (u, v) \in E(\bar{K}) : \exists x \in \bar{K} \text{ s.t. } u = r_1(x) \wedge r_2(x) = 0\}.
\end{aligned}$$

Show that all these three sets are finite.

(c) Let $S = S_1 \cup S_2 \cup S_3$. Show that, for all $Q = (u, v) \in E(\bar{K}) \setminus S$, we have $|\varphi^{-1}(Q)| = |\deg(\varphi)|$.

(d) Deduce (i) and (iii).

Exercise 11 **(4 points)**

Let E be an elliptic curve over a field K. Show that the map $\mathbb{Z} \to \mathrm{End}(E),\ m \mapsto [m]$ is an injective ring homomorphism.

Exercise 12 – Bonus (The Parallelogram Identity) **(6 points)**

Prove the following, which allows to show in a quick way that, for all $m \in \mathbb{Z}$, $\deg([m]) = m^2$.

Theorem Let E be an elliptic curve over a field K and let $\alpha, \beta \in \mathrm{End}(E)$. Then

$$\deg(\alpha + \beta) + \deg(\alpha - \beta) = 2(\deg(\alpha) + \deg(\beta)).$$

Hints: This can be proven in an elementary way, but it is not straightforward. A proof will be presented in the next tutorial.

- Note that the cases $\alpha = 0, \beta = 0, \alpha = \pm\beta$ follow easily from what we already know.
- The theorem follows from

$$\deg(\alpha + \beta) + \deg(\alpha - \beta) \leq 2(\deg(\alpha) + \deg(\beta)). \tag{1}$$

- Show (1) (this takes some work!).

Please hand in your solutions by ***Wednesday, 31 May 2023, 13:30h*** *in the* ***postbox by F409*** *or per e-mail to your tutor.*