Algebraic Geometry IV Prof. Dr. Ulrich Görtz
SS 2024 Dr. Yingying Wang

Problem sheet 10

Due date: Wednesday, June 19

Problem 37

Let S be a connected scheme. For an isogeny $f\colon E \to E'$ of relative elliptic curves over S we denote by $\deg(f)$ the rank of the locally free $\mathscr{O}_S$-module corresponding to the finite locally free S-scheme $\mathrm{Ker}(f)$. We also set $\deg(0) = 0$.

(1) Explain that this defines $\deg(f) \in \mathbb{Z}$ for all homomorphisms $E \to E'$ of elliptic curves over S. What happens if S is not assumed to be connected?
(2) Let $f\colon E \to E$ be an endomorphism of an elliptic curve E over S. Show that $f + f^\vee$ is an integer. We denote this integer by $\mathrm{tr}(f)$ and call it the *trace* of f.

Hint. For Part (2), compute the degree of $[1] + f$.

Problem 38

Let S be a connected scheme and let E/S be an elliptic curve. Let $f\colon E \to E$ be an endomorphism of the elliptic curve E.

(1) Show that f is a zero of the polynomial $X^2 - \mathrm{tr}(f)X + \deg(f)$.
(2) Show that for $n, m \in \mathbb{Z}$ we have $n^2 - \mathrm{tr}(f)mn + \deg(f)m^2 = \deg(n - mf) \geqslant 0$.
(3) Show that $x^2 - \mathrm{tr}(f)x + \deg(f) \geqslant 0$ for all $x \in \mathbb{R}$ and conclude that

$$\mathrm{tr}(f)^2 \leqslant 4\deg(f).$$

Problem 39

Let S be a connected scheme and let E be a relative elliptic curve over S such that the endomorphism ring $\mathrm{End}_S(E)$ is commutative.

(1) Prove that $\mathrm{End}_S(E)$ is an integral domain.
(2) Prove that $\mathrm{Frac}(\mathrm{End}_S(E)) = \mathrm{End}_S(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.
(3) Prove that $\mathrm{Frac}(\mathrm{End}_S(E))$ is equal to $\mathbb{Q}$, or is an imaginary quadratic number field.

Remark. We proved in AG3 Problem 22 that whenever S is the spectrum of a field of characteristic 0, then the endomorphism ring of every elliptic curve over S is commutative. By the results on the constancy locus of a morphism, this holds whenever S is connected and contains a point with residue field of characteristic 0.

Problem 40

Let q be a prime power, let $\mathbb{F}_q$ be the finite field with q elements and let E be an elliptic curve over $\mathbb{F}_q$. Denote by $F \in \mathrm{End}(E)$ the q-Frobenius isogeny of E.

(1) Show that $[1] - F$ is étale.
(2) Show that $\#E(\mathbb{F}_q) = 1 + q - \mathrm{tr}(F)$.
(3) Prove the *Hasse bound*

$$|\#E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Remark. One can show (this is part of the *Weil conjectures* for curves over finite fields) that every smooth projective curve E of genus 1 over the finite field $\mathbb{F}_q$ satisfies the estimate in Part (2). In particular, it follows that $E(\mathbb{F}_q) \neq \varnothing$ for every such E, so E can be equipped with the structure of an elliptic curve.