

Problem sheet 6

Due date: Wednesday, May 22

Problem 21

Let k be a field (of characteristic $\neq 2$, if you prefer), and let E/k be an elliptic curve. Show that the automorphism group of E (as a k -group scheme) is non-trivial.

Problem 22

Let k be an algebraically closed field of characteristic $\neq 2$ and let E/k be an elliptic curve.

- (1) Let $f, g: E \rightarrow \mathbb{P}_k^1$ be morphisms of degree 2 which are ramified over $0, 1, \infty, \lambda$, and such that $f(0) = \infty = g(0)$. Suppose that for each of $0, 1, \lambda$, the (unique) preimage under f and under g are the same (i.e., $f(x_1) = 1 = g(x_1)$ for some $x_1 \in E(k)$, etc.) Show that $f = g$.
- (2) Show that the order of the automorphism group $\text{Aut}(E)$ of E (as a k -group scheme) divides 12 (and in particular is finite).

Hint. Part (1) is close to what we have done in class. First show that f, g are given (as morphism from E to some projective space) by the same line bundle. What is the ambiguity in the choice of two global sections of this line bundle? For Part (2), define a morphism from $\text{Aut}(E)$ to the symmetric group S_3 and study its kernel. To do so, you may proceed as follows: As discussed in class, we may assume that E is given by an (affine) Weierstraß equation of the form $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in k \setminus \{0, 1\}$. This means that E admits a morphism $f: E \rightarrow \mathbb{P}_k^1$ ramified precisely over $0, 1, \infty, \lambda$ and with $f(0) = \infty$; then f is ramified exactly at the points of $E[2](k)$, and this set is preserved by every automorphism. Combine this with Part (1).

Remark. If the base field has characteristic 2, the order of the automorphism group of an elliptic curve divides 24, but does not necessarily divide 12.

Problem 23

Let p be a prime number.

Recall the absolute and relative Frobenius morphisms: Let R be an \mathbb{F}_p -algebra. The morphism $\text{Spec}(R) \rightarrow \text{Spec}(R)$ induced by the ring homomorphism $a \mapsto a^p$ is called the *absolute Frobenius morphism*. Let X be a characteristic p scheme (i.e., the morphism $X \rightarrow \text{Spec}(\mathbb{Z})$ factors through \mathbb{F}_p ; equivalently, $p = 0$ in all rings $\Gamma(U, \mathcal{O}_X)$, $U \subseteq X$ open). The absolute Frobenius morphisms on the affine pieces of X glue to the *absolute Frobenius morphism* F_X of X , a universal homeomorphism.

Now let S be a characteristic p scheme and let X be an S -scheme. We write $X^{(p)}$ for the fiber product $X \times_{S, F_S} S$ and call the map $F_{X/S}: X \rightarrow X^{(p)}$ given by $F_X: X \rightarrow X$ and the structure morphism $X \rightarrow S$ the *relative Frobenius* of X over S . This is by definition a morphism of S -schemes.

Let k be a field of characteristic p .

- (1) Assume that $X = X_0 \otimes_{\mathbb{F}_p} k$ for some \mathbb{F}_p -scheme X_0 . Show that there is a natural identification $X^{(p)} = X$.
- (2) Compute the relative Frobenius morphisms of \mathbb{A}_k^n and \mathbb{P}_k^n on (homogeneous) coordinates (seen as an endomorphism, in view of Part (1)).
- (3) Compute the degree of $F_{\mathbb{P}_k^1/k}$.

Problem 24

I asked ChatGPT 4 the following question: **What is the degree of the Frobenius morphism of a curve over a field of positive characteristic?**

The following is ChatGPT's answer. What do you think about it?

The degree of the Frobenius morphism for a curve over a field of positive characteristic p is p . Here's a detailed explanation:

- (1) **Background:** The Frobenius morphism is a fundamental concept in the arithmetic geometry of algebraic varieties over fields of positive characteristic. For a curve (or more generally, any algebraic variety) defined over a finite field \mathbb{F}_q where $q = p^k$ for some prime p and integer k , the Frobenius morphism acts on the coordinates of the points of the variety.
- (2) **Action on Points:** If X is a curve defined over \mathbb{F}_q , then the Frobenius morphism F acts on a point (x, y) on the curve by raising each coordinate to the p -th power. That is, $F(x, y) = (x^p, y^p)$.
- (3) **Degree Definition:** The degree of a morphism between curves is defined as the number of pre-images a generic point has under the morphism, counting multiplicities. More formally, it can be seen as the degree of the field extension that the function induces on the function fields of the curves.
- (4) **Computation:** In the case of the Frobenius morphism F , it raises the coordinates to the power of p . If we consider a function field $K(X)$ of the curve X , where K is the base field, the Frobenius morphism acts on the function field by sending any element f to f^p . This extension $K(X)$ to $K(X)^p$ (the field obtained by applying the Frobenius morphism to every element of $K(X)$) is a purely inseparable extension of degree p .
- (5) **Why Degree p :** The key point here is that every element x of $K(X)$ has exactly one p -th root in $K(X)$, and it is $x^{1/p}$. Therefore, for each point x in the curve X under F , there is exactly one point that maps to x under F , that is, $x^{1/p}$. This implies that F is a bijective map on the points of the curve, and the corresponding field extension has degree p .

Thus, the degree of the Frobenius morphism $F: X \rightarrow X$ is p , which reflects the fundamental impact of the characteristic p of the field on the geometry of the curve.