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

Problem sheet 8

Due date: Wednesday, June 5

Problem 29

Let K be an imaginary quadratic number field with ring of integers $\mathcal{O}_K$. Show that there is a bijection between the set of isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}_K$, and the class group $\mathrm{Cl}(K)$ of K (i.e., the group of fractional ideals in K modulo the group of principal fractional ideals).

Problem 30

(1) Let k be a field, $\sigma\colon k \to k$ an automorphism, and let E/k be an elliptic curve. Let E^σ be the elliptic curve $E \otimes_{k,\sigma} k$, the base change of E with respect to $\mathrm{Spec}(\sigma)\colon \mathrm{Spec}(k) \to \mathrm{Spec}(k)$. Show that $j(E^\sigma) = \sigma(j(E))$ and that $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

(2) Let K be an imaginary quadratic number field with ring of integers $\mathcal{O}_K$. Let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}_K$. Show that the j-invariant $j(E)$ is algebraic over $\mathbb{Q}$.

Hint. In Part (1), start with a (Weierstraß) equation for E and write down an equation for E^σ. In order to relate it to the j-invariant, you may assume that E admits a Weierstraß equation of the form $y^2 = x^3 + ax + b$, so that $j(E)$ can be expressed as in Problem 26. For (2), use Part (1), Problem 29 and that for a transcendental number $j \in \mathbb{C}$ the set $\{\sigma(j);\ \sigma \in \mathrm{Aut}(\mathbb{C})\}$ is infinite.

Remark. This is the starting point of the *theory of complex multiplication of elliptic curves* which says, among other results, that the field $K(j(E))$ (for K and E as above) is the *Hilbert class field* of K, i.e., the maximal abelian unramified extension field of K. We have $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$. The j-invariants of all elliptic curves E with $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$ together with all roots of unity “almost” generate the maximal abelian extension of K, so that one gets an “explicit” form of class field theory of the field K.

Problem 31

Let k be a perfect field of characteristic $p > 0$ and let $f\colon C \to C'$ be a non-constant morphism of geometrically connected smooth projective curves over k.

(1) Let $q = [K(C) : K(C')]_i$ be the inseparability degree of the extension $K(C)/K(C')$ (a power of p). Show that f factors as $C \xrightarrow{F_q} C^{(q)} \to C$, where F_q is the “q-Frobenius” of C (cf. Problems 23, 25, but replace $x \mapsto x^p$ by $x \mapsto x^q$).

(2) Assume that k is algebraically closed. Show that there exists a dense open $V \subseteq C'$ such that all fibers of the restriction $f_{|f^{-1}(V)} \colon f^{-1}(V) \to V$ have cardinality $[K(C) : K(C')]_s$, the separability degree of the extension $K(C)/K(C')$.

Hint. For (1), let K_s be the separable closure of $K(C')$ in $K(C)$. Show (using that $K(C^{(q)}) = K(C)^q$ and $\deg F_q = q$ analogously to Problem 25) that $K_s = K(C^{(q)})$ as subfields of $K(C)$. For (2) use Part (1) and Problem 15 (2).

Problem 32

Let k be an algebraically closed field of characteristic $p > 0$, and let E/k be an elliptic curve. Let $E[p] = \mathrm{Ker}([p]_E) = E \times_E \mathrm{Spec}(k)$, where the fiber product is taken with respect to the multiplication by p map, $[p]_E \colon E \to E$ and the neutral element $\mathrm{Spec}(k) \to E$. Denote by $F \colon E \to E^{(p)}$ the relative Frobenius morphism of E.

Show that the following are equivalent.

(i) The group scheme $E[p]$ topologically consists of a single point,
(ii) the dual isogeny $F^\vee$ is purely inseparable (i.e., induces a purely inseparable extension $K(E)/K(E^{(p)})$),
(iii) the map $[p]_E$ is purely inseparable.

Hint. Use that $F^\vee \circ F = [p]_E$ (Problem 19), that F is purely inseparable (cf. Problem 25) and Problem 31 (2).

Remark. If E satisfies the above conditions, then we say that E is *supersingular*. The assumption that k be algebraically closed is added only for simplicity (e.g., so that Problem 31 (2) can be applied directly); the statement is true in general.