Elliptic Curves - Homework 3

Francesco Minnocci

December 16, 2024

8. To find an isomorphism between $C : x^2 + y^2 + z^2 = 0$ and $\mathbb{P}^1_{\overline{\mathbb{Q}}}$, we first observe that C is isomorphic to $C' : x^2 + +y^2 = z^2$ via

$$\begin{gathered} C' \to C \\ [x : y : z] \mapsto [x : y : iz], \end{gathered}$$

with inverse $[x : y : z] \mapsto [x : y : -iz]$. Furthermore, C' is isomorphic to $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ via the map constructed in the first homework,and we can compose the two isomorphisms to get

$$\begin{aligned} \varphi : \mathbb{P}^1_{\overline{\mathbb{Q}}} &\to C \\ [x : y] &\mapsto [y^2 - x^2 : 2xy : i(x^2 + y^2)], \end{aligned}$$

whose inverse is given by the morphism

$$\begin{aligned} \varphi^{-1} : C &\longrightarrow \mathbb{P}^1_{\overline{\mathbb{Q}}} \\ [x : y : z] &\longmapsto \begin{cases} [y : x - iz] \text{ if } y(x - iz) \neq 0 \\ [-x - iz : y] \text{ if } y(-x - iz) \neq 0 \end{cases} \end{aligned}$$

We have thus found an isomorphism between C and $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$, which shows that C is a twisted form of $\mathbb{P}^1_{\mathbb{Q}}$. To find a corresponding cocycle, notice that φ is already defined over $\mathbb{Q}(i)$. This means that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group $\mathrm{Aut}(\mathbb{P}^1_{\overline{\mathbb{Q}}})$ factors through $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, and so for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have that

$$\varphi^{-1} \circ \sigma(\varphi) = \varphi^{-1} \circ (\sigma \circ \varphi \circ \sigma^{-1}) : \mathbb{P}^1_{\overline{\mathbb{Q}}} \longrightarrow \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

sends

$$[x : y] \longmapsto \begin{cases} [x : y] & \text{if } \sigma(i) = i \\ [-y : x] & \text{if } \sigma(i) = -i, \end{cases}$$

which can be checked directly by the explicit formulas for φ and φ^{-1}.

9. In the following, we denote by $\overline{E}$ the $\overline{\mathbb{F}}_q$-points of the elliptic curve E.
Taking the exact sequence

$$0 \to \overline{E}[\ell] \to \overline{E} \to \overline{E} \to 0$$

yields a following exact sequence in cohomology:

$$\cdots \longrightarrow E(\mathbb{F}_q) \xrightarrow{\ell} E(\mathbb{F}_q) \longrightarrow H^1(\mathbb{F}_q, \overline{E}[\ell]) \longrightarrow \cancel{H^1(\mathbb{F}_q, \overline{E})} \longrightarrow \cdots$$

where the last term is zero by Lemma 12.12 in the notes. In others words, the group $H^1(\mathbb{F}_q, \overline{E}[\ell])$ is a quotient of the finite abelian group $E(\mathbb{F}_q)$, hence finite itself.

Finally, for all but finitely many ℓ (all except those dividing the order of $E(\mathbb{F}_q)$), multiplication by ℓ is an automorphism of the group $E(\mathbb{F}_q)$, which in particular has trivial cokernel $H^1(\mathbb{F}_q, \overline{E}[\ell])$. This shows that the group $H^1(\mathbb{F}_q, \overline{E}[\ell])$ is trivial for all but finitely many ℓ.

10. (in collaboration with Marco Sanna) Let $\overline{K}$ be a fixed algebraic closure of K. By the Néron-Ogg-Shafarevich criterion, the curve E has good reduction if and only the whole Tate module is fixed by the inertia subgroup I.

In the case of bad reduction, we will show that E cannot have additive reduction over K^{nr}; this implies that it has either good reduction over K^{nr} (and we have seen that in this case E has good reduction over K) or multiplicative reduction over K^{nr}. In this last case, E must also have multiplicative reduction over K (which is our goal); indeed, if the E has equation $y^2 = x^3 + Ax + B$ over K with discriminant Δ, assume by contradiction that E has additive reduction over K (that is, up to translation $\overline{A} = \overline{B} = 0$). Then, since E has multiplicative reduction over K^{nr}, the valuation $v_{K^{\mathrm{nr}}}(\Delta)$ cannot be minimal, and so there is some coordinate change

$$x = u^2 x', \quad y = u^3 y'$$

sends Δ to $u^{-12}\Delta$, and

$$v_{K^{\mathrm{nr}}}(u^{-12}\Delta) < v_{K^{\mathrm{nr}}}(\Delta) = v_K(\Delta).$$

Now, after fixing a uniformizer π of $\mathcal{O}_K$ (which is also a uniformizer of $\mathcal{O}_{K^{\mathrm{nr}}}$), we can write u as $w \cdot \pi^r$ for some $w \in \mathcal{O}_{K^{\mathrm{nr}}}$ and $r \in \mathbb{Z}$. Then, we have we can write u as $w \cdot \pi^r$, and the coordinate change

$$x \to \pi^{2r} x, \quad y \to \pi^{3r} y$$

sends Δ to $\pi^{-12r}\Delta$, which contradicts the minimality of $v_K(\Delta)$:

$$v_K(\pi^{-12r}\Delta) = v_{K^{\mathrm{nr}}}(u^{-12}\Delta) < v_K(\Delta).$$

Suppose now that E has additive reduction over K^{nr}, and let κ be the residue field of K^{nr}. As in the proof of Theorem 13.4, we first choose m large enough such that

$$l^m > |E(K^{\mathrm{nr}})/E(K^{\mathrm{nr}})^{(0)}|.$$

By assumption, there is some non-trivial element (P_i) of $T_\ell(E)$ which is fixed by I. Setting

$$\overline{n} := \min\{n : \pi_n((P_i)) \neq O\},$$

by definition of $T_\ell(E)$ this means that

$$Q := \pi_{\overline{n}+m-1}((P_i))$$

has order ℓ^m, and since Q is fixed by I, it is defined over K^{nr}. By our choice of m, the order ℓ subgroup generated by $(l^{m-1}Q)$ must be contained in $E(K^{\mathrm{nr}})^{(0)}[l]$, but since $E(K^{\mathrm{nr}})^{(1)}$ has no ℓ-torsion, the reduction map r is an injection on $E(K^{\mathrm{nr}})^{(0)}[l]$, which should send $(l^{m-1}Q)$ to a point of order ℓ in $\overline{E}(\kappa)_{\mathrm{smooth}} \simeq \kappa^+ \simeq \overline{\mathbb{F}}_p^+$; this yields a contradiction, since $\overline{\mathbb{F}}_p^+$ has no points of order ℓ for $\ell \neq p$.