

# Elliptic Curves - Homework 3

Francesco Minnocci

December 17, 2024

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

$$\begin{aligned} C' &\rightarrow C \\ [x : y : z] &\mapsto [x : y : iz], \end{aligned}$$

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

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

whose inverse is given by the morphism

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

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

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

sends

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

as can be checked directly by the explicit formulas for  $\varphi$  and  $\varphi^{-1}$ .

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

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

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  $\ell$  (all except those dividing the order of  $E(\mathbb{F}_q)$ ), multiplication by  $\ell$  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  $\ell$ .

**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  $K^{\text{nr}}$ ; this implies that it has either good reduction over  $K^{\text{nr}}$  (and we have seen that in this case  $E$  has good reduction over  $K$ ) or multiplicative reduction over  $K^{\text{nr}}$ . 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 minimal discriminant  $\Delta$ , and 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  $K^{\text{nr}}$ , the valuation  $v_{K^{\text{nr}}}(\Delta)$  cannot be minimal (otherwise we could use the equation  $y^2 = x^3$  for its reduction and it would be additive), and so there is some coordinate change

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

sends  $\Delta$  to  $u^{-12}\Delta$ , and

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

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

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

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

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

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

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

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  $\ell^m$ , and since  $Q$  is fixed by  $I$ , it is defined over  $K^{\text{nr}}$ . By our choice of  $m$ , the order  $\ell$  subgroup generated by  $(\ell^{m-1}Q)$  must be contained in  $E(K^{\text{nr}})^{(0)}[\ell]$ , but since  $E(K^{\text{nr}})^{(1)}$  has no  $\ell$ -torsion, the reduction map  $r$  is an injection on  $E(K^{\text{nr}})^{(0)}[\ell]$ , which should send  $(\ell^{m-1}Q)$  to a point of order  $\ell$  in  $\overline{E}(\kappa)_{\text{smooth}} \simeq \kappa^+ \simeq \overline{\mathbb{F}}_p^+$ . This yields the a contradiction, as  $\overline{\mathbb{F}}_p^+$  has no points of order  $\ell$  for  $\ell \neq p$ , and so  $E$  cannot have additive reduction over  $K^{\text{nr}}$ , which concludes.  $K$ .