

EXERCISES ON VARIOUS COHOMOLOGY THEORIES OF ELLIPTIC CURVES

EMRE CAN SERTÖZ

Let k be a ring and set $f = y^2z - x^3 + xz^2 \in k[x, y, z]$, noting that f is the homogenization of $y^2 - x(x-1)(x+1)$. For the following exercises, E will be the scheme over k defined by f in \mathbb{P}_k^2 . Mark a point on E . If K is a k -algebra, then we will write $E(K)$ for the K -valued points of E , that is, K -valued solutions of f .

Exercise 1. Let $k = \mathbb{C}$ be the field of complex numbers and E^{an} be the complex Riemann surface underlying the elliptic curve E . It is classical that there is a biholomorphism $E^{\text{an}} \simeq \mathbb{C}/\mathbb{Z}\langle 1, \tau \rangle$ for some $\tau \in \mathbb{H} = \{z \in \mathbb{C} \mid \text{im } z > 0\}$. In the following exercises we will compute τ .

- (1) Find explicit loops $\gamma_1, \gamma_2 \subset E^{\text{an}}$ such that their homology classes form a basis in $H_1(E, \mathbb{Z})$.
- (2) In the affine chart $\mathbb{C}^2 = \{z = 1\} \subset \mathbb{P}_{\mathbb{C}}^2$ we may define the meromorphic 1-form dx/y . Show that $dx/y|_{E \cap \mathbb{C}^2}$ extends uniquely to a holomorphic form ω on E .
- (3) Compute the integrals $\int_{\gamma_1} \omega$ and $\int_{\gamma_2} \omega$. What is the corresponding value of τ ?
- (4) Using the power series expansion of the j -invariant on the upper half plane, numerically evaluate $j(\tau)$.
- (5) The j -invariant of E is a rational number which can be computed directly from the coefficients of f . Using this formulation, check your answer to (4).

The following exercise is more meaningful in light of the following two facts: the rational numbers can be completed at a prime to obtain the p -adics and completed at the “place at infinity” to obtain real numbers. Before we move on to p -adics, let us study the $\text{Gal}(\mathbb{C}/\mathbb{R})$ action on the cohomology of our elliptic curve.

Exercise 2. Continue with the setup in Exercise 1. Let $\sigma: \text{Spec } \mathbb{C} \rightarrow \text{Spec } \mathbb{C}$ be the complex conjugation. Pullback via σ induces a map on the set of complex points $E(\mathbb{C})$ allowing us to act on differential forms and homological cycles on E^{an} .

- (1) Denote by σ^* the linear map on $H_1(E^{\text{an}}, \mathbb{Z})$ obtained by acting on loops in E^{an} via complex conjugation. Using your homology basis for Exercise 1 compute the 2×2 integral basis representing σ . Evidently, the \mathbb{C} -linear extension of σ^* is *not* complex conjugation.
- (2) The integrals of ω can be viewed as the coordinates of the line $H^0(E, \Omega_{E/\mathbb{C}}^1)$ in $H^1(E, \mathbb{C})$. Observe that the action of σ^* on these coordinates is via complex conjugation.
- (3) Using the Dolbeaux decomposition $H^1(E^{\text{an}}, \mathbb{C}) = H^{1,0}(E^{\text{an}}) \oplus H^{0,1}(E^{\text{an}})$ explain why σ^* maps $H^{1,0}$ to $H^{0,1}$.
- (4) Observe that $H^{1,0}(E^{\text{an}}) \simeq H^0(E, \Omega_{E/\mathbb{C}}^1) = H^0(E, \Omega_{E/\mathbb{Q}}^1) \otimes_{\mathbb{Q}} \mathbb{C}$. Show that \mathbb{Q} -differential forms $\Omega_{E/\mathbb{Q}}$ are invariant under σ .

The following exercise is an easy warm-up for Exercise 4. The choice of the prime 5 is so that I can avoid saying “good reduction” but does not hold any greater significance.

Exercise 3. Let $k = \mathbb{F}_5$ be the field with five elements and fix an algebraic closure \bar{k} . Recalling E has a group structure, denote by $E[n]$ the set of \bar{k} -valued points of E of order n . That is $E[n] = \{x \in E(\bar{k}) \mid nx = 0\}$.

Date: 2018-11-01.

- (1) Determine explicitly the smallest field extension k'/k you need in order to define the points in $E[2]$.
- (2) By fixing a basis, make the identification $E[2] \simeq \mathbb{F}_2^2$. The Galois group of k'/k acts on $E[2]$. Determine the matrix in $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ representing the action of the Frobenius on $E[2]$.
- (3) It is not much harder to compute the minimal field extension required for $E[4]$ and $E[8]$. Choosing a basis for $E[8]$, and setting a basis for $E[4]$ and $E[2]$ as multiples of the basis for $E[8]$, compute the Frobenius action on $E[2^n]$ as a matrix M_n in $\mathrm{GL}(2, \mathbb{Z}/2^n\mathbb{Z})$ for $n = 1, 2, 3$ respectively. Write $M_3 = M_{3,0} + 2M_{3,1} + 4M_{3,2}$ where $M_{3,i} \in \{0, 1\}^{2 \times 2}$ and compare to M_1, M_2 . We are approximating a matrix in $\mathrm{GL}(2, \mathbb{Z}_2)$.
- (4) Can you determine $E[5]$?

Now we look at the elliptic curve over the p -adic integers through ℓ -adic cohomology. This will combine the two worlds of complex and finite elliptic curves. Moreover, the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_5/\mathbb{Q}_5)$ enters into the picture.

Exercise 4. Let $k = \mathbb{Z}_5$ be the ring of 5-adic integers. If $K \in \{\mathbb{Q}_5, \mathbb{F}_5\}$ we have maps $k \rightarrow K$. We will denote the fibers of E/k over these fields as E_K . Fix a prime ℓ different from 5.

- (1) Show that the Tate module $T_\ell E_{\mathbb{Q}_5}$ is non-canonically isomorphic to \mathbb{Z}_ℓ^2 .
- (2) Show that the Tate module $T_\ell E_{\mathbb{F}_5}$ is non-canonically isomorphic to \mathbb{Z}_ℓ^2 .
- (3) Show that there is a canonical isomorphism $T_\ell E_{\mathbb{Q}_5} \simeq T_\ell E_{\mathbb{F}_5}$. What happens if we allow $\ell = 5$.
- (4) Show that there is a natural map between the Galois groups $\mathrm{Gal}(\bar{\mathbb{Q}}_5/\mathbb{Q}_5) \rightarrow \mathrm{Gal}(\bar{\mathbb{F}}_5/\mathbb{F}_5)$ and that the isomorphism in (3) is equivariant with respect to corresponding Galois actions.

Note in particular that the $\mathrm{Gal}(\bar{\mathbb{Q}}_5/\mathbb{Q}_5)$ action on $H_{\mathrm{\acute{e}t}}^1(E_{\mathbb{Q}_5}, \mathbb{Q}_\ell) \simeq \mathrm{hom}(T_\ell E_{\mathbb{Q}_5}, \mathbb{Q}_5)$ factors through the much smaller group $\mathrm{Gal}(\bar{\mathbb{F}}_5/\mathbb{F}_5)$.

EMRE CAN SERTÖZ, MAX PLANCK INSTITUTE FOR MATHEMATICS IN THE SCIENCES, INSELSTR. 22, 04103 LEIPZIG, GERMANY
E-mail address: emresertoz@gmail.com