

Spectra of Field Automorphisms Acting on Elliptic Curves

Bo-Hae Im and Michael Larsen

Main Theorem

Let E be an elliptic curve over a number field K and σ an element of $\text{Gal}(\bar{K}/K)$. We write $\Sigma(E, \sigma)$ for the spectrum of σ acting on $E(\bar{K}) \otimes \mathbf{C}$.

Theorem. *Let ζ be any root of unity. Then there exists a non-empty open subset of $S \subset \text{Gal}(\bar{K}/K)$ such that ζ appears with infinite multiplicity in $\Sigma(E, \gamma)$ for all $\gamma \in S$.*

What are Elliptic Curves?

Definition. An elliptic curve is a non-singular projective curve which is also a group.

Variant Definition. An elliptic curve is a compact Riemann surface which is also a group.

Basic Example. Let $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ be a lattice in \mathbf{C} . Then \mathbf{C}/Λ is an elliptic curve.

Projective Embeddings of Elliptic Curves

An ordered pair of elliptic functions (f, g) gives a map from E to \mathbf{CP}^2 :

$$z \mapsto (f(z), g(z)).$$

Example. Weierstrass embedding:

$$f(z) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

$$g(z) = \frac{-\wp'(z)}{2} = \sum_{\lambda \in \Lambda} \frac{1}{(z - \lambda)^3}.$$

$$g(z)^2 = f(z)^3 + af(z) + b$$

Example. Jacobi embedding:

$$f(z) = \operatorname{sn} z$$

$$g(z) = \operatorname{cn} z \operatorname{dn} z$$

$$g(z)^2 = (1 - f(z)^2)(1 - k^2 f(z)^2).$$

Isomorphic Double Covers

Theorem. *Two double covers of \mathbf{P}^1 give isomorphic Riemann surfaces if they are ramified over projectively equivalent sets of points.*

Example. Substituting

$$x = \frac{du - b}{-cu + a}, \quad y = \frac{v\sqrt{(c\lambda_1 + d)(c\lambda_2 + d)(c\lambda_3 + d)(c\lambda_4 + d)}}{(a - cu)^2}$$

in

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)(x - \lambda_4)$$

gives

$$v^2 = \left(u - \frac{a\lambda_1 + b}{c\lambda_1 + d}\right) \left(u - \frac{a\lambda_2 + b}{c\lambda_2 + d}\right) \cdot \left(u - \frac{a\lambda_3 + b}{c\lambda_3 + d}\right) \left(u - \frac{a\lambda_4 + b}{c\lambda_4 + d}\right).$$

Addition Formula

Theorem. If E is an elliptic curve in Weierstrass form and P , Q , and R are points on E , then $P + Q + R = 0$ if and only if P , Q , and R are collinear.

Mordell-Weil Theorem

Theorem. If E is an elliptic curve defined over a number field K , then $E(K)$ is a finitely generated abelian group.

The Group over $\bar{\mathbf{Q}}$

Theorem. If E is an elliptic curve defined over a number field K , then

$$E(\bar{\mathbf{Q}}) \cong \mathbf{Q}^\omega \times (\mathbf{Q}/\mathbf{Z})^2.$$

Idea. The group of points is *divisible* thanks to the elliptic function analogue of the $(1/n)$ -angle formulas in trig. The points of finite order are the same as the points of finite order in $E(\mathbf{C}) \cong (\mathbf{R}/\mathbf{Z})^2$.

What is $\text{Gal}(\bar{K}/K)$?

Definition. The Galois group $\text{Gal}(\bar{K}/K)$ is the set of field automorphisms σ of the field of algebraic numbers such that $\sigma(a) = a$ for all $a \in K$.

If $P(x)$ has coefficients in K , then σ permutes the roots of P .

Example. If $a \in K$, then $\sigma(\sqrt{a}) = \epsilon_a \sqrt{a}$, where $\epsilon_a = \pm 1$ satisfies the compatibility condition

$$\epsilon_{ab} = \epsilon_a \epsilon_b.$$

The Topology on $\text{Gal}(\bar{K}/K)$

Definition. The basic open sets X_S of $\text{Gal}(\bar{K}/K)$ are given by finite sets of ordered pairs

$$S = \{(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n)\}.$$

Each S determines

$$X_S = \{\sigma \in \text{Gal}(\bar{K}/K) \mid \sigma(\alpha_i) = \beta_i \text{ for } i = 1, 2, \dots, n\}.$$

A necessary and sufficient condition that X_S is non-empty is the following:

$$\begin{aligned} P(\alpha_1, \dots, \alpha_n) = 0 &\Rightarrow P(\beta_1, \dots, \beta_n) = 0 \\ &\forall P(x_1, \dots, x_n) \in K[x_1, \dots, x_n]. \end{aligned}$$

Galois Representations

The action of $\text{Gal}(\bar{K}/K)$ on $E(\bar{K}) = E(\bar{\mathbf{Q}})$ is given on the coordinates.

It is a *group action*.

It gives a natural homomorphism

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Aut}(\mathbf{Q}^\omega \times (\mathbf{Q}/\mathbf{Z})^2) = \text{GL}_\infty(\mathbf{Q}) \times \prod_{\ell \text{ prime}} \text{GL}_2(\mathbf{Z}_\ell).$$

Hilbert Irreducibility

Theorem. *Let K and L be number fields, $K \subset L$. Let $P(x, y) \in L[x, y]$ be an irreducible polynomial. Then there exists an infinite subset S of K such that $P(s, y)$ is irreducible as a polynomial in $L[y]$ for all $s \in S$.*

Example. If $P(x) \in K[x]$ is a non-constant polynomial with distinct roots, then the set

$$\{\sqrt{P(s)} \mid s \in K\}$$

is not contained in any finite extension L of K .

Triples

Lemma. *If $a, b, c, d, e, f \in K$, for every $\sigma \in \text{Gal}(\bar{K}/K)$, every $s \in K$ determines a point on one of the following three curves:*

$$y^2 = (x - a)(x - b)(x - c)(x - d)$$

$$y^2 = (x - c)(x - d)(x - e)(x - f)$$

$$y^2 = (x - e)(x - f)(x - a)(x - b)$$

which is fixed by σ .

Basic Trick

Let ω be a cube root of 1. When

$$c = \omega a, d = \omega b, e = \omega^2 a, f = \omega^2 b,$$

all three of these elliptic curves are isomorphic. Moreover, the quadruple $(\alpha, \beta, \gamma, \delta)$ is projectively equivalent to one of the form $(a, b, \omega a, \omega b)$.