# Metabelian Galois Representations

Edray Herber Goins

AMS 2018 Spring Western Sectional Meeting
Special Session on Automorphisms of Riemann Surfaces and Related Topics
Portland State University

Department of Mathematics
Purdue University

April 15, 2018


## Abstract

We are used to working with Galois representations associated to elliptic curves by considering the action of the absolute Galois group on torsion points. However there is a slightly more exotic way to view this construction once we realize that the Tate module of an elliptic curve is just the abelianization of the étale fundamental group of the punctured torus.

In this talk, we discuss how to construct a class of Galois representations by considering covers of elliptic curves which are branched over one point. We discuss how this is related to the question of surjectivity of certain Galois representation, and how to construct representations with image isomorphic to the holomorph of the quaternions. We will not assume extensive knowledge of étale cohomology. This is joint work with Rachel Davis.

`http://www.ams.org/amsmtgs/2248_abstracts/1137-11-340.pdf`

# Outline of Talk

# Group Variety

## Proposition

Denote the set $\mathbb{G}_m = \{(x, y) \in \mathbb{A}^2 \mid xy = 1\}$.

- Denote the operation $\oplus : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ by

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 \cdot x_2, \ y_1 \cdot y_2).$$

  Then $(\mathbb{G}_m, \oplus)$ is an abelian group. In particular, $O_{\mathbb{G}_m} = (1, 1)$ is the identity, and $P = (x, y)$ has inverse $[-1]P = (y, x)$.

- Given any field $K$, the projection map $\mathbb{G}_m(K) \to K^\times$ which sends $(x, y) \mapsto x$ is an isomorphism.

- For any integer $N$, write $[N]P = P \oplus P \oplus \cdots \oplus P = (x^N, y^N)$. The same projection map allows us to identify the $N$-torsion elements $\mathbb{G}_m[N] = \{P \in \mathbb{G}_m(\mathbb{C}) \mid [N]P = O_{\mathbb{G}_m}\} \simeq \mu_N$ with the collection of $N$th roots of unity $\zeta_N$.

# Riemann Sphere

## Proposition

The complex projective line $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ is the sphere

$$S^2(\mathbb{R}) = \left\{ (u, v, w) \in \mathbb{A}^3(\mathbb{R}) \,\middle|\, u^2 + v^2 + w^2 = 1 \right\}.$$

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{C}) & \longrightarrow & S^2(\mathbb{R}) \\ z = \dfrac{u + i\,v}{1 - w} = \dfrac{1 + w}{u - i\,v} & \mapsto & (u, v, w) = \left( \dfrac{2\,\mathrm{Re}\,z}{|z|^2 + 1}, \dfrac{2\,\mathrm{Im}\,z}{|z|^2 + 1}, \dfrac{|z|^2 - 1}{|z|^2 + 1} \right) \\ 0, \quad 1, \quad \infty & \mapsto & (0, 0, -1), \quad (1, 0, 0), \quad (0, 0, 1) \end{array}$$

## Proposition

$X = \mathbb{G}_m(\mathbb{C})$ is the twice punctured Riemann sphere.

$$\mathbb{G}_m(\mathbb{C}) \simeq \mathbb{C}^\times = \mathbb{P}^1(\mathbb{C}) - \{0, \infty\} \simeq S^2(\mathbb{R}) - \{(0, 0, \pm 1)\}.$$

# Monodromy

Fix a positive integer $N$, and consider the composition

$$\begin{array}{rccccc} \beta: & X = \mathbb{G}_m(\mathbb{C}) & \longrightarrow & X & \longrightarrow & Y = \mathbb{P}^1(\mathbb{C}) - \{0, \infty\} \\ & P = (x, y) & & [N]P = (x^N, y^N) & & x^N \end{array}$$

For any $y_0 \in Y$, we have $x_0^N = y_0$ and the inverse image

$$T = \beta^{-1}(y_0) = \left\{ P_k = \left( x_0\, \zeta_N^k,\ x_0^{-1}\, \zeta_N^{-k} \right) \;\middle|\; k \in \mathbb{Z} \right\} \simeq P_0 \oplus \mathbb{G}_m[N].$$

Given a closed loop $\gamma : [0,1] \to Y$, say $\gamma(t) = y_0\, e^{2\pi k i t}$ such that $\gamma(0) = \gamma(1) = y_0$, we can find paths such that $\beta \circ \widetilde{\gamma} = \gamma$.

$$\widetilde{\gamma}: \quad [0,1] \to X, \qquad \widetilde{\gamma}(t) = \left( x_0\, e^{2\pi i k t/N},\ x_0^{-1} e^{-2\pi i k t/N} \right).$$

## Proposition

$$\begin{array}{ccc} \pi_1(Y, y_0) & \twoheadrightarrow & \mathrm{Aut}(T) \\ \| & & \| \\ \mathbb{Z} & \twoheadrightarrow & \mathbb{A}^1(\mathbb{Z}/N\mathbb{Z}) \end{array} \qquad \begin{array}{c} \gamma \longmapsto [P_0 = \widetilde{\gamma}(0) \mapsto \widetilde{\gamma}(1) = P_k] \\ k \longmapsto k \bmod N \end{array}$$

# Galois Representations

- The $N$-torsion $\mathbb{G}_m[N] \simeq \mu_N$ is generated by $T_0 = \left(\zeta_N,\ \zeta_N^{-1}\right)$, while $T \simeq P_0 \oplus \mathbb{G}_m[N]$ is generated by $T_0$ and $P_0 = \left(x_0,\ x_0^{-1}\right)$.
- If $y_0 \in \mathbb{P}^1(\mathbb{Q}) - \{0, \infty\}$, he absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts:

$$\sigma(T_0) = \left(\zeta_N^a,\ \zeta_N^{-a}\right) \qquad = [a]\, T_0$$

$$\sigma(P_0) = \left(x_0\, \zeta_N^k,\ x_0^{-1}\, \zeta_N^{-k}\right) \qquad = [k]\, T_0 \oplus P_0$$

- With respect to the basis $\{T_0, P_0\}$, we have the following diagram:

$$\begin{array}{ccccccccc}
1 & \to & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Aut}(T) & \longrightarrow & \mathrm{Aut}(T) \rtimes \mathrm{Aut}(\mathbb{G}_m[N]) & \to & \mathrm{Aut}(\mathbb{G}_m[N]) & \longrightarrow & 1 \\
 & & \| & & \| & & \| & & \\
1 & \longrightarrow & \mathbb{A}^1(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & AGL_1(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & GL_1(\mathbb{Z}/N\mathbb{Z}) & \to & 1 \\
 & & k & & \begin{bmatrix} a & k \\ & 1 \end{bmatrix} & & a & &
\end{array}$$

## Motivating Question

The monodromy action gives a Galois representation

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{A}^1(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & AGL_1(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & GL_1(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1 \end{array}$$

If we replace the twice punctured sphere $\mathbb{G}_m(\mathbb{C}) \simeq \mathbb{P}^1(\overline{\mathbb{Q}}) - \{0, \infty\}$ with $\mathbb{P}^1(\overline{\mathbb{Q}}) - \{\text{more points}\}$, what kinds of representations do we find?

- Say $Y = \mathbb{P}^1(\overline{\mathbb{Q}}) - \{n+1 \text{ points}\}$. Then the étale fundamental group $\pi_{1,\text{ét}}(Y, y_0)$ is just the profinite completion of the free group on $n$ generators. That is, $\pi_{1,\text{ét}}(Y, y_0)^{\text{ab}} \simeq \mathbb{A}^n(\widehat{\mathbb{Z}})$. Since $Y$ is connected, this group is independent of $y_0$.
- Every free group on $n$ generators can be embedded into the free group on 2 generators. Hence we will focus on $Y = \mathbb{P}^1(\overline{\mathbb{Q}}) - \{0, 1, \infty\}$ such that $\pi_{1,\text{ét}}(Y, y_0)^{\text{ab}} \simeq \mathbb{A}^2(\widehat{\mathbb{Z}})$.

# What is this "Étale Fundamental Group"?

# Belyĭ's Theorem

Let $\beta : \overline{X} \to \mathbb{P}^1(\mathbb{C})$ be a meromorphic function on a Riemann surface $\overline{X}$. We say $P_0 \in X$ is a critical point if $\beta'(P_0) = 0$, and $y_0 \in \mathbb{P}^1(\mathbb{C})$ is a critical value if $y_0 = \beta(P_0)$ for some critical point $P_0 \in \overline{X}$.

**Theorem (André Weil, 1956; Gennadiĭ Vladimirovich Belyĭ, 1979)**

*Let $\overline{X}$ be a compact, connected Riemann surface.*

- *$\overline{X}$ is a smooth, irreducible, projective variety of dimension 1. In particular, $\overline{X}$ is an algebraic variety; that is, it can be defined by polynomial equations.*
- *If $\overline{X}$ can be defined by a polynomial equation $\sum_{i,j} a_{ij}\, x^i\, y^j = 0$ where the coefficients $a_{ij} \in \overline{\mathbb{Q}}$, then there exists a rational function $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which has at most three critical values.*
- *Conversely, if there exists rational function $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which has at most three critical values, then $X$ can be defined by a polynomial equation $\sum_{i,j} a_{ij}\, x^i\, y^j = 0$ where the coefficients $a_{ij} \in \overline{\mathbb{Q}}$.*

# Étale Fundamental Group

## Definition

A rational function $\beta : \overline{X} \to \mathbb{P}^1(\mathbb{C})$ which has at most three critical values $\{0, 1, \infty\}$ is called a Belyĭ map.

Denote $Y = \mathbb{P}^1(\overline{\mathbb{Q}}) - \{0, 1, \infty\}$ as the thrice punctured sphere, and $X = \overline{X} - \{\text{critical points } P_0 \text{ of } \beta\}$. Then $\beta : X \to Y$ is unbranched.

## Definition

For any $Y$, the étale fundamental group $\pi_{1,\text{ét}}(Y)$ keeps track étale covers $\beta : X \to Y$. That is, maps such that

- $X$ is a connected Riemann surface, that is, a curve defined over $\overline{\mathbb{Q}}$,
- $\beta \in \overline{\mathbb{Q}}(X)$ is a rational map, and
- $|\beta^{-1}(y_0)| = \deg(\beta)$ for all $y_0 \in Y$.

# Dessins d'Enfant

Fix a Belyĭ map $\beta : \overline{X} \to \mathbb{P}^1(\mathbb{C})$. Denote the preimages

$$B = \beta^{-1}(\{0\}) \qquad W = \beta^{-1}(\{1\}) \qquad E = \beta^{-1}([0,1]) \qquad X \xrightarrow{\beta} Y$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$\left\{\begin{matrix}\text{black}\\ \text{vertices}\end{matrix}\right\} \qquad \left\{\begin{matrix}\text{white}\\ \text{vertices}\end{matrix}\right\} \qquad \left\{\text{edges}\right\} \qquad \mathbb{A}^3(\mathbb{R})$$

The bipartite graph $\Delta_\beta = (V, E)$ with vertices $V = B \cup W$ and edges $E$ is called Dessin d'Enfant. We embed the graph on $X$ in 3-dimensions.

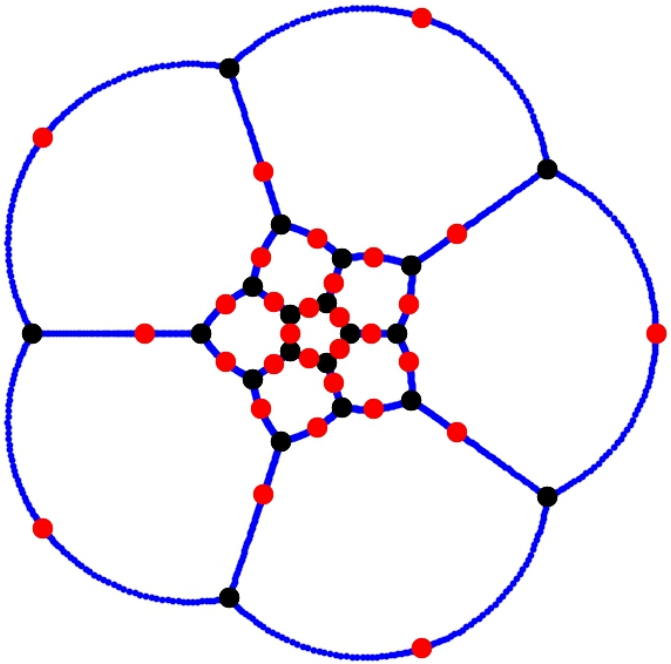
> I do not believe that a mathematical fact has ever struck me quite so strongly as this one, nor had a comparable psychological impact. This is surely because of the very familiar, non-technical nature of the objects considered, of which any child's drawing scrawled on a bit of paper (at least if the drawing is made without lifting the pencil) gives a perfectly explicit example. To such a *dessin* we find associated subtle arithmetic invariants, which are completely turned topsy-turvy as soon as we add one more stroke.
>
> – Alexander Grothendieck, *Esquisse d'un Programme* (1984)

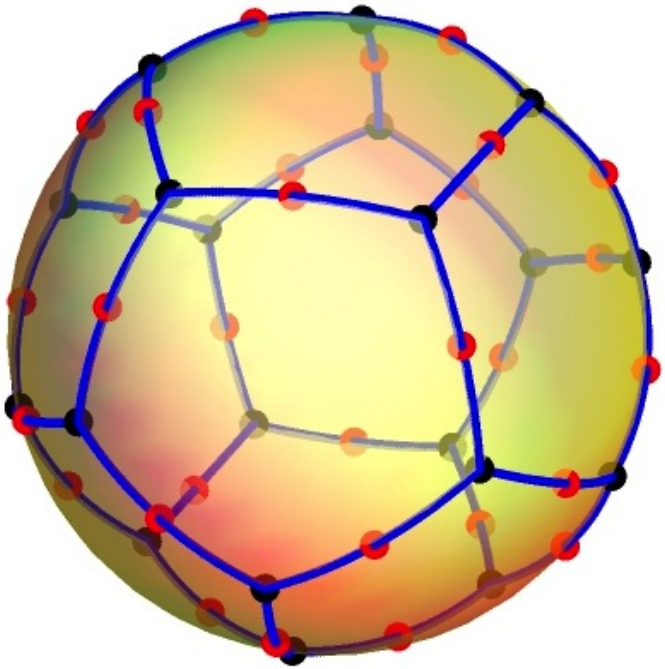
# Examples

Felix Klein constructed the Platonic Solids as the inverse images of the origin $V = \beta^{-1}(\{0\})$ in terms of the Belyĭ maps on $\overline{X} = \mathbb{P}^1(\mathbb{C}) \simeq S^2(\mathbb{R})$.

$$\beta(z) = \begin{cases} \dfrac{(z^n+1)^2}{4\,z^n} & \text{for the regular polygons,} \\ -\dfrac{64\,z^3\,(z^3-1)^3}{(8\,z^3+1)^3} & \text{for the tetrahedron,} \\ \dfrac{108\,z^4\,(z^4-1)^4}{(z^8+14\,z^4+1)^3} & \text{for the octahedron,} \\ \dfrac{(z^8+14\,z^4+1)^3}{108\,z^4\,(z^4-1)^4} & \text{for the cube,} \\ \dfrac{1728\,z^5\,(z^{10}-11\,z^5-1)^5}{(z^{20}+228\,z^{15}+494\,z^{10}-228\,z^5+1)^3} & \text{for the icosahedron,} \\ \dfrac{(z^{20}+228\,z^{15}+494\,z^{10}-228\,z^5+1)^3}{1728\,z^5\,(z^{10}-11\,z^5-1)^5} & \text{for the dodecahedron.} \end{cases}$$

# Rotation Group $A_5$: Dodecahedron





$$\beta(z) = \frac{(z^{20}+228\,z^{15}+494\,z^{10}-228\,z^5+1)^3}{1728\,z^5\,(z^{10}-11\,z^5-1)^5} \;:\; v = 20+30, e = 2\cdot 30, f = 12$$

Let's Consider

$$\overline{X} = E(\mathbb{C}) \simeq \mathbb{T}^2(\mathbb{R})$$

# What is an Elliptic Curve?

## Definition

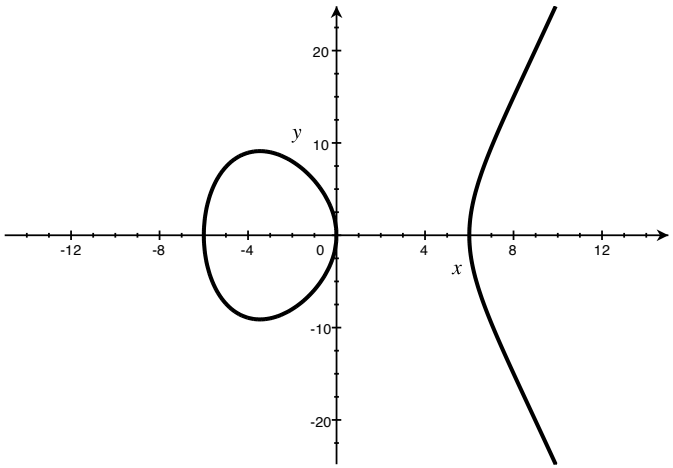
Let $A$ and $B$ be rational numbers such that $4A^3 + 27B^2 \neq 0$. An elliptic curve $E$ is the set of all $(x, y)$ satisfying the equation

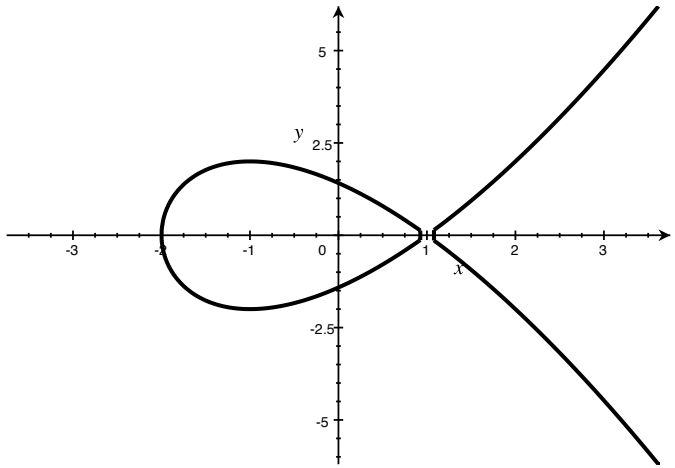
$$y^2 = x^3 + Ax + B.$$

We will also include the "point at infinity" $O_E$.

**Example:** $y^2 = x^3 - 36x$ is an elliptic curve.

**Non-Example:** $y^2 = x^3 - 3x + 2$ is not an elliptic curve.



# Group Law

Given two $K$-rational points on an elliptic curve $E$, we may construct more.

1. Start with two $K$-rational points $P$ and $Q$.
2. Draw a line through $P$ and $Q$.
3. The intersection $P * Q$,is another $K$-rational point on $E$.

## Definition

Let $E$ be an elliptic curve defined over a field $K$, and denote $E(K)$ as the set of $K$-rational points on $E$. Define the operation $\oplus$ as

$$P \oplus Q = (P * Q) * O_E.$$

## Theorem (Henri Poincaré, 1901)

*Let $E$ be an elliptic curve defined over a field $K$. Then $\big(E(K), \oplus\big)$ is an abelian group.*

# Dessins d'Enfant on the Torus

**Theorem**

$$X = E(\mathbb{C}) = \left\{ (x,y) \in \mathbb{A}^2(\mathbb{C}) \,\middle|\, y^2 = x^3 + Ax + B \right\} \cup \{O_E\} \simeq \mathbb{T}^2(\mathbb{R}).$$

With $e_1$, $e_2$, and $e_3$ as distinct complex roots of $x^3 + Ax + B = 0$, write the period lattice $\Lambda = \mathbb{Z}\,w_1 + \mathbb{Z}\,w_2$ in terms of the elliptic integrals

$$w_1 = \frac{1}{\pi} \int_{e_1}^{e_3} \frac{dz}{\sqrt{z^3 + Az + B}} \quad \text{and} \quad w_2 = \frac{1}{\pi} \int_{e_2}^{e_3} \frac{dz}{\sqrt{z^3 + Az + B}}.$$

Define the maps

$$\begin{array}{ccccc} X & \longrightarrow & \mathbb{C}/\Lambda & \longrightarrow & \mathbb{T}^2(\mathbb{R}) \\ & & \theta\, w_1 + \phi\, w_2 & & u = \left(R + r\,\cos\theta\right)\,\cos\phi \\ (x,y) & \mapsto & = \displaystyle\int_{e_1}^{x} \frac{dz}{\sqrt{z^3 + Az + B}} & \mapsto & v = \left(R + r\,\cos\theta\right)\,\sin\phi \\ & & & & w = r\,\sin\theta \end{array}$$

# Belyĭ Maps on Elliptic Curves

$$E:\ y^2 = x^3 + 1 \qquad \beta(x,y) = \frac{y+1}{2}$$

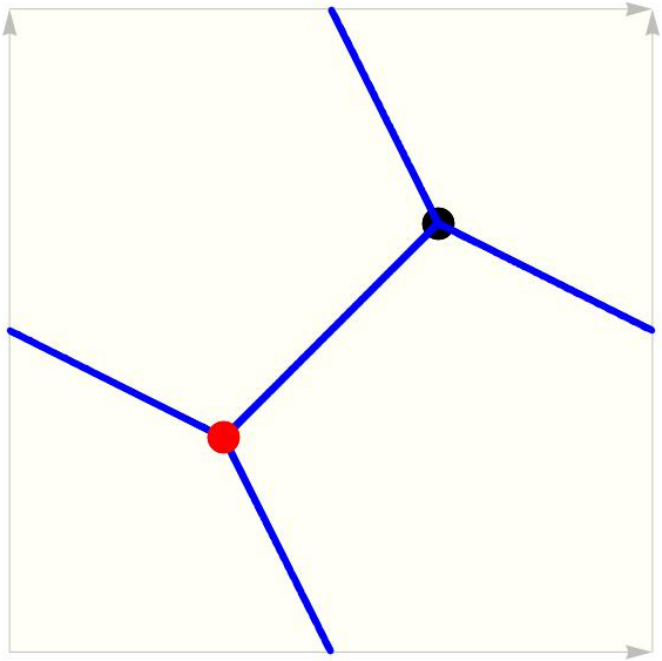
$$E:\ y^2 = x^3 + 5\,x + 10 \qquad \beta(x,y) = \frac{(x-5)\,y + 16}{32}$$

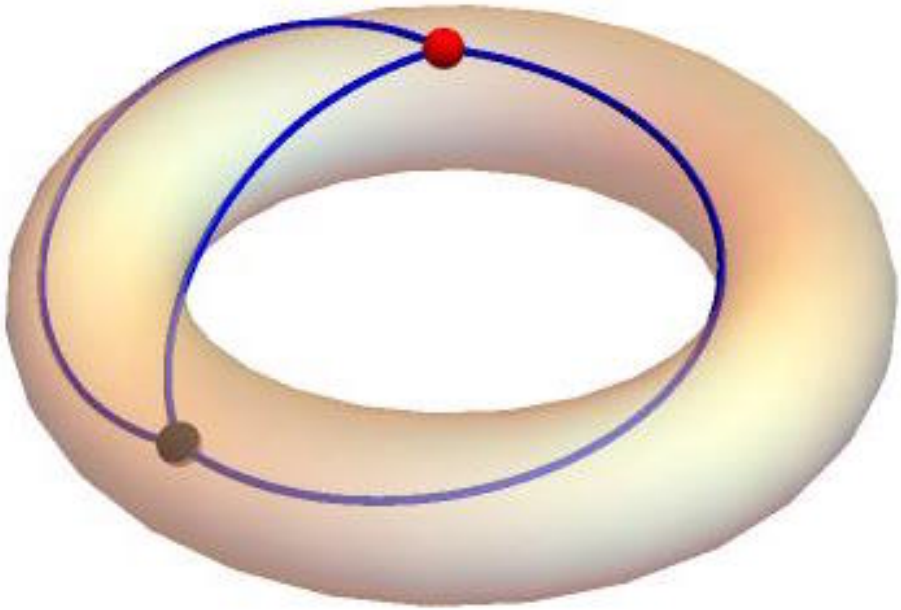
$$E:\ y^2 = x^3 - 120\,x + 740 \qquad \beta(x,y) = \frac{(x+5)\,y + 162}{324}$$

$$E:\ \begin{aligned} y^2 + x\,y + y \\ = x^3 + x^2 + 35\,x - 28 \end{aligned} \qquad \beta(x,y) = \frac{4\left(9\,x\,y - x^3 - 15\,x^2 - 36\,x + 32\right)}{3125}$$

$$E:\ y^2 = x^3 - 15\,x - 10 \qquad \beta(x,y) = \frac{\begin{aligned}\left(3\,x^2 + 12\,x + 5\right)\,y \\ + \left(-10\,x^3 - 30\,x^2 - 6\,x + 6\right)\end{aligned}}{-16\left(9\,x + 26\right)}$$

$$E:\ y^2 + 15\,x\,y + 128\,y = x^3 \qquad \beta(x,y) = \frac{\left(y - x^2 - 17\,x\right)^3}{16384\,y}$$





$$\beta(x,y) = \frac{y+1}{2} \qquad \text{on} \qquad E:\ y^2 = x^3 + 1$$

# Mod $N$ Representation

## Theorem

*Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $N$ be a positive integer.*

- *The map $[N] : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ which sends $P \mapsto P \oplus \cdots \oplus P$ is an étale cover. In fact, $\pi_{1,ét}\big(E(\overline{\mathbb{Q}})\big) \simeq \mathbb{A}^2(\widehat{\mathbb{Z}})$ is generated by such maps.*
- *Denote $E[N] = \big\{P \in E(\mathbb{C}) \,\big|\, [N]P = O_E\big\}$. This abelian group is generated by two elements $T_1$ and $T_2$ such that $E[N] \simeq \mathbb{A}^2(\mathbb{Z}/N\,\mathbb{Z})$.*
- *Fix $Q_0 \in E(\mathbb{Q})$, and consider $T = [N]^{-1}\, Q_0 = P_0 \oplus E[N]$. The absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $T$:*

$$\sigma(T_1) = [a]\,T_1 \oplus [c]\,T_2$$

$$\sigma(T_2) = [b]\,T_1 \oplus [d]\,T_2$$

$$\sigma(P_0) = [e]\,T_1 \oplus [f]\,T_2 \oplus P_0$$

# Mod $N$ Representation

Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $N$ be a positive integer. With respect to the basis $\{T_1, T_2, P_0\}$, we have the following diagram:

$$\begin{array}{ccccccccc}
1 & \to & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[N])\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \overline{\rho}_{E,N} & & \\
1 & \longrightarrow & \mathrm{Aut}(T) & \longrightarrow & \mathrm{Aut}(T) \rtimes \mathrm{Aut}(E[N]) & \longrightarrow & \mathrm{Aut}(E[N]) & \longrightarrow & 1 \\
 & & \| & & \| & & \| & & \\
1 & \longrightarrow & \mathbb{A}^2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & AGL_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & GL_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1
\end{array}$$

$$\begin{bmatrix} e \\ f \end{bmatrix} \qquad \begin{bmatrix} a & b & e \\ c & d & f \\ & & 1 \end{bmatrix} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We actually have the adelic Tate module

$$T(E) = \varprojlim_N E[N] \simeq \prod_\ell T_\ell(E) \simeq \pi_{1,\text{ét}}\left(E(\overline{\mathbb{Q}})\right) \simeq \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}.$$

# Frattini Lifting Theorem

When $N = \ell^n$ for a prime $\ell$, we have the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[N])) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \rho_{E,\ell} & & \downarrow \overline{\rho}_{E,N} & & \\ 1 & \longrightarrow & \ker(\pi_N) & \longrightarrow & GL_2(\mathbb{Z}_\ell) & \xrightarrow{\pi_N} & GL_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1 \end{array}$$

**Theorem**

*Let $\Phi(G)$ denote the Frattini subgroup of $G = GL_2(\mathbb{Z}_\ell)$, that is, the intersection of the maximal subgroups of $G$. Assume that $\ker(\pi_N) \subseteq \Phi(G)$. Then $\rho_{E,\ell}$ is surjective if and only if $\overline{\rho}_{E,N}$ is surjective.*

- Let $N = \ell^n$. Then $\ker(\pi_N) \subseteq \Phi(G)$ if and only if $N \geq 5$. Hence $\rho_{E,\ell}$ is surjective if and only if $\overline{\rho}_{E,N}$ is surjective whenever $N \geq 5$.
- Let $\ell = 2$. In 2011, Tim and Vladimir Dokchitser focused on when $\overline{\rho}_{E,4}$ is surjective but $\rho_{E,2}$ is not surjective.
- Let $\ell = 3$. In 2006, Noam Elkies focused on when $\overline{\rho}_{E,3}$ is surjective but $\rho_{E,3}$ is not surjective.

**Theorem**

*The étale fundamental group of the thrice punctured sphere* $\mathbb{P}^1(\overline{\mathbb{Q}}) - \{0, 1, \infty\}$ *is the same as that for the punctured torus* $E(\overline{\mathbb{Q}}) - \{O_E\}$. *That is, topologically these surfaces are the same.*

$$\pi_1(E(\mathbb{C}) - \{O_E\}) \simeq \langle x, y, z \,|\, [x, y]\, z = 1 \rangle$$

in terms of the commutator $[x, y] = x\, y\, x^{-1}\, y^{-1}$, and

$$\pi_1\big(\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}\big) \simeq \langle \gamma_0, \gamma_1, \gamma_\infty \,|\, \gamma_0\, \gamma_1\, \gamma_\infty = 1 \rangle$$

This gives

$$\begin{array}{lcl} x = {\gamma_1}^{-1} & & \gamma_0 = x\, y \\ y = \gamma_1\, \gamma_0 & \Longleftrightarrow & \gamma_1 = x^{-1} \\ z = \gamma_1\, \gamma_0\, \gamma_\infty & & \gamma_\infty = y^{-1}\, z \end{array}$$

Perhaps we can find interesting étale covers of $X = E(\overline{\mathbb{Q}}) - \{O_E\}$?

# Outer Galois Representations

## Theorem

*Let* $X = E(\overline{\mathbb{Q}}) - \{O_E\}$ *for an elliptic curve* $E$ *over* $\mathbb{Q}$.

- $T(E) = \varprojlim_N E[N] \simeq \prod_\ell T_\ell(E) \simeq \pi_{1,\acute{e}t}(X)^{ab} \simeq \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V & \longrightarrow & \pi_{1,alg}(X) & \longrightarrow & Gal(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & \pi_{1,\acute{e}t}(X) & \longrightarrow & \pi_{1,\acute{e}t}(\overline{X}) & \xrightarrow{\varphi} & \pi_{1,\acute{e}t}\big(Spec\,\mathbb{Q}\big) & \longrightarrow & 1 \end{array}$$

  *for some variety* $\overline{X}$ *over* $\mathbb{Q}$ *such that* $X \simeq \overline{X} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$.

- *There is a continuous representation* $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Out(V)$ *which sends a Galois automorphism* $\sigma = \varphi(w)$ *to the outer automorphism* $v \mapsto w\, v\, w^{-1}$ *mod* $Inn(V)$ *acting on* $V$.

- *Since* $T(E) \simeq V^{ab}$ *is an abelian group, the collection of outer automorphisms* $Out\big(T(E)\big) \simeq Aut\big(T(E)\big) \simeq \prod_\ell GL_2(\mathbb{Z}_\ell)$.

# Metabelian Groups

Consider $N = \ell^n$ for $\ell = 2$. We have a sequence of groups $M_n$ with abelianization $\left(M_n\right)^{\mathsf{ab}} \simeq \mathbb{A}^2(\mathbb{Z}/2^n\,\mathbb{Z}) \simeq E[2^n]$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{A}^{\binom{n}{2}}(\mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & M_n & \longrightarrow & \mathbb{A}^2(\mathbb{Z}/2^n\,\mathbb{Z}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathbb{A}^3(\mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & M_3 & \longrightarrow & \mathbb{A}^2(\mathbb{Z}/8\,\mathbb{Z}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathbb{A}^1(\mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & M_2 & \longrightarrow & \mathbb{A}^2(\mathbb{Z}/4\,\mathbb{Z}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & M_1 & \longrightarrow & \mathbb{A}^2(\mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & 1
\end{array}$$

We will focus on $G$ as the free pro-$\ell$ completion in $\pi_{1,\text{ét}}(X)$ for $X = E(\overline{\mathbb{Q}}) - \{O_E\}$, so that $M_n = G/\Phi\big(\ker(\pi_N)\big)$.

# Relation with Quaternions

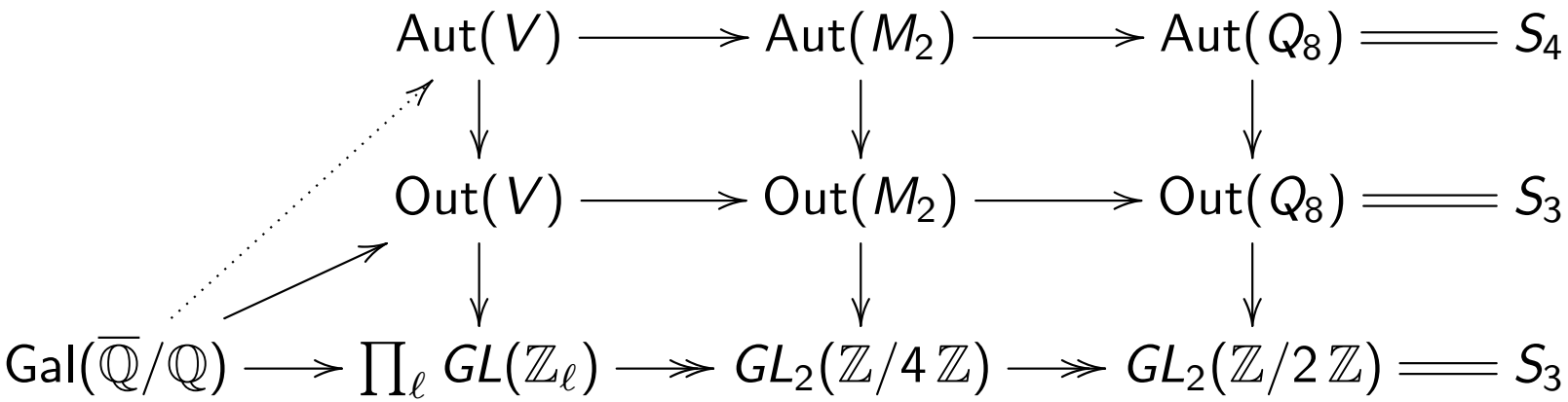
$$M_2 = \left\langle a,\, b \;\middle|\; a^4 = b^4 = [a,b]^2 = 1,\; a\,[a,b]\,a^{-1} = b\,[a,b]\,b^{-1} = [a,b] \right\rangle$$

$$Q_8 = \left\langle i,\, j,\, k \;\middle|\; i^2 = j^2 = k^2 = i\,j\,k = -1 \right\rangle$$

The group homomorphism $M_2 \to Q_8$ defined by $a \mapsto i$ and $b \mapsto j$ yields

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & \left\{ \begin{matrix} 1,\; a^2\,b^2, \\ a^2\,[a,b],\; b^2\,[a,b] \end{matrix} \right\} & \longrightarrow & E[2] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & ((M_2)' \simeq \mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & M_2 & \longrightarrow & ((M_2)^{ab} \simeq E[4]) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & ((Q_8)' \simeq \mathbb{Z}/2\,\mathbb{Z}) & \longrightarrow & Q_8 & \longrightarrow & ((Q_8)^{ab} \simeq E[2]) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Let $V = \pi_{1,\text{ét}}(X)$ for the punctured torus $X = E(\overline{\mathbb{Q}}) - \{O\}$. The canonical map $V \twoheadrightarrow V^{\text{ab}}$ yields the diagram




in terms of the groups

$$M_2 = \left\langle \mathrm{a},\, \mathrm{b} \;\middle|\; \mathrm{a}^4 = \mathrm{b}^4 = [\mathrm{a},\mathrm{b}]^2 = 1,\, \mathrm{a}\,[\mathrm{a},\mathrm{b}]\,\mathrm{a}^{-1} = \mathrm{b}\,[\mathrm{a},\mathrm{b}]\,\mathrm{b}^{-1} = [\mathrm{a},\mathrm{b}] \right\rangle$$

$$Q_8 = \left\langle \mathrm{i},\, \mathrm{j},\, \mathrm{k} \;\middle|\; \mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1 \right\rangle$$

**Question**

Can we always lift an adelic Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\widehat{\mathbb{Z}})$ to a representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V)$?

## Theorem (Rachel Davis, G)

*Denote* $E : y^2 = x^3 + \frac{3\,J_0}{1-J_0}\,x + \frac{2\,J_0}{1-J_0}$ *for* $J_0 \in \mathbb{P}^1(\mathbb{Q}) - \{0, 1, \infty\}$.

- *For each root* $t$ *of* $\left(t^8 + 14\,t^4 + 1\right)^3 - 108\,J_0\,t^4\left(t^4 - 1\right)^4 = 0$, $K = k(t) \subseteq \mathbb{Q}(E[4])$ *is the splitting field of* $q(x) = 432\,J_0\,x^4 + 8\,x + 1$ *with* $Gal(K/k) \simeq S_4$ *over* $k = \mathbb{Q}(\sqrt{-1})$.

- *Denote* $D : w^4 = z^3 + \frac{3\,J_0}{1-J_0}\,z + \frac{2\,J_0}{1-J_0}$. *Then the morphism* $\phi : D \to E$ *defined by* $(z, w) \mapsto [2]\,(z,\, w^2)$ *is unramified outside of* $O_E$ *and yields the group* $Aut(D/E) \simeq Q_8$ *as defined over* $K$.

- *For any point* $P \in E(K) - \{O_E\}$, *let* $L = K\left(\phi^{-1}(P)\right)$. *Then the monodromy action yields the short exact sequence*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Gal(L/K) & \longrightarrow & Gal(L/k) & \longrightarrow & Gal(K/k) & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & Q_8 & \longrightarrow & Hol(Q_8) & \longrightarrow & \left(Aut(Q_8) \simeq S_4\right) & \longrightarrow & 1 \end{array}$$

*In particular, there is a representation* $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(Q_8)$ *which can be realized via* $q(x) = 432\,J_0\,x^4 + 8\,x + 1$.