Origami Galois representations

Rachel Davis
Joint work with Professor Edray Goins
Purdue University

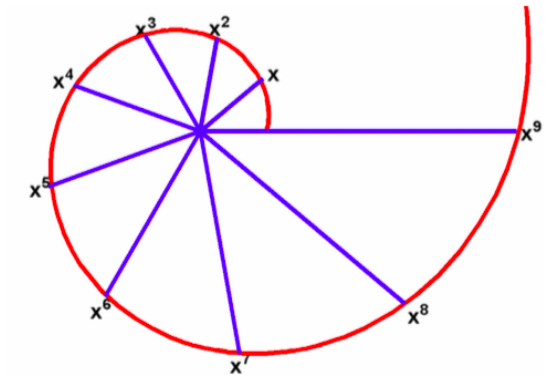
Connecticut Conference on Elliptic Curves and Modular Forms, and Related Topics
University of Connecticut

August 18, 2016

Table of Contents

Table of Contents

Let $\phi : X \to Y \quad X = Y = \mathbb{G}_m =$ multiplicative group $= \mathbb{P}^1(\mathbb{C}) \setminus \{0, \infty\}$.
$\phi : Y \to X$
$\phi : x \mapsto x^N$



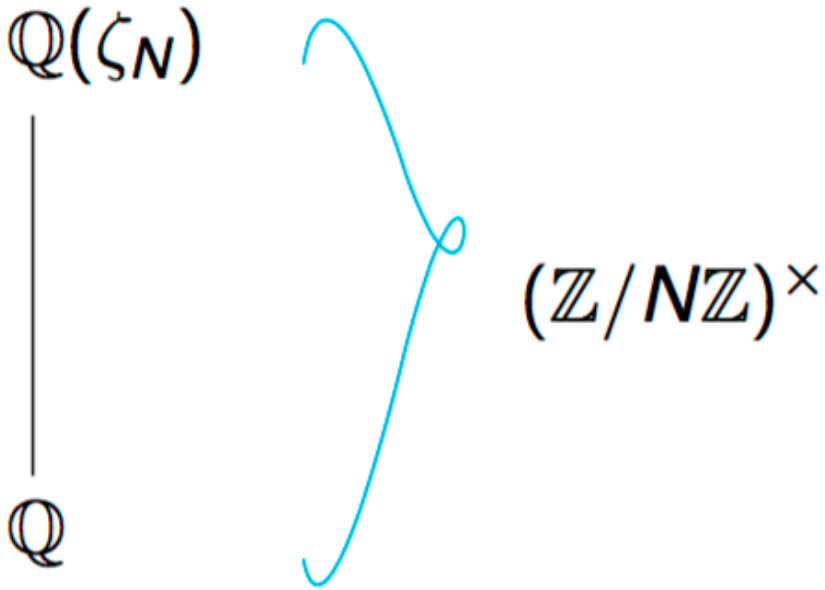
Fix a rational point $p \in \mathbb{G}_m$ (thought of in X, the target of the map ϕ).

Consider the set $V = \phi^{-1}(p) = \{x \in \mathbb{G}_m | \quad \phi(x) = p\}$, i.e. $\{x \in \mathbb{G}_m | \quad x^N = p\}$.

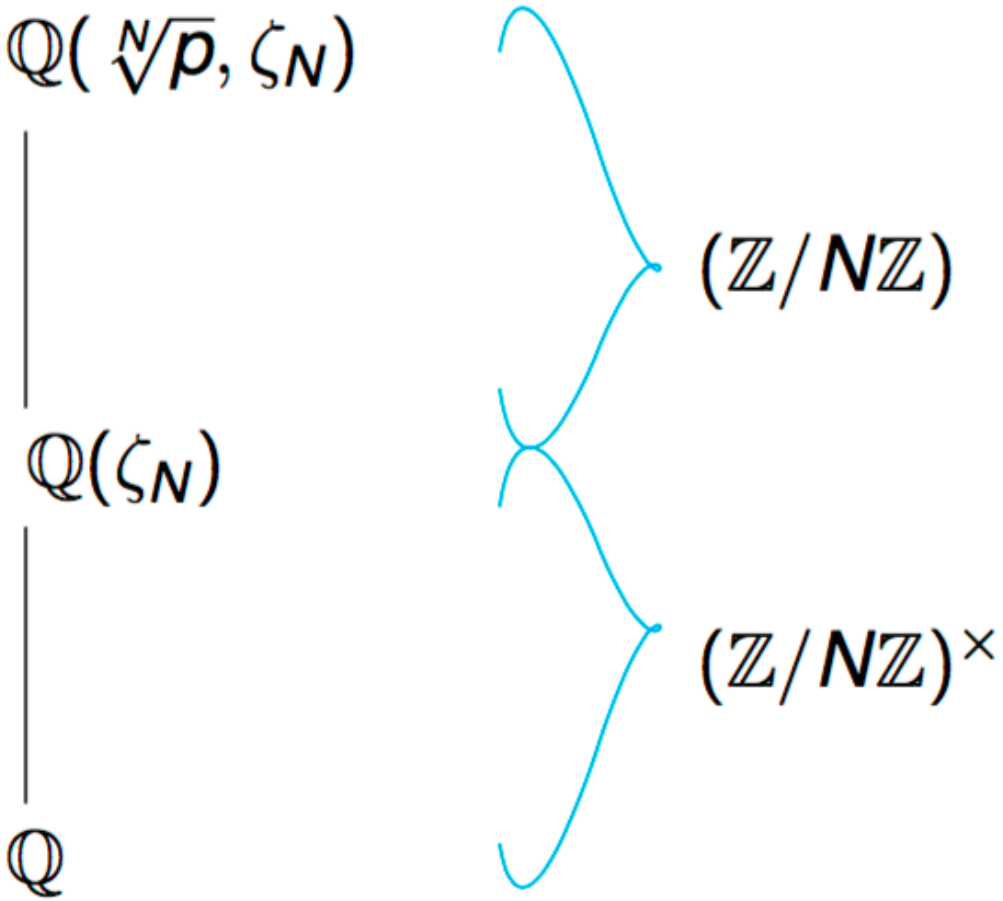
$$f_p(x) = x^N - p$$

First, consider the case that $p = 1$. Then V is the set of solutions to $f_p(x) = x^N - 1$. These are the N^{th} roots of unity.

$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$. Let i, N be relatively prime. Then $\sigma_i : \zeta_N \mapsto \zeta_N^i$.



When $f_p(x) = x^N - p$ is irreducible, the picture becomes the following:



- $\mathrm{Gal}(sf(x^N - p)/\mathbb{Q})$ is a subgroup of $\mathrm{AGL}_1(\mathbb{Z}/N\mathbb{Z})$.
- There is a Galois representation

$$\rho_{N,p} : G_{\mathbb{Q}} \to \mathrm{AGL}_1(\mathbb{Z}/N\mathbb{Z})$$

- This is given by $\sigma \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ such that $\sigma(\zeta_N) = \zeta_N^a$ and $\frac{\sigma(\sqrt[N]{p})}{\sqrt[N]{p}} = \zeta_N^b$ with $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $b \in \mathbb{Z}/N\mathbb{Z}$.

Table of Contents

Let E be an elliptic curve over $\mathbb{Q}$. Fix a positive integer N. We define multiplication by N on E, denoted $[N]$ to be adding a point to itself N times. We define the N-division points of E:

$$E[N] = \left\{ P \in E(\overline{\mathbb{Q}}) : [N]P = \mathcal{O} \right\}.$$

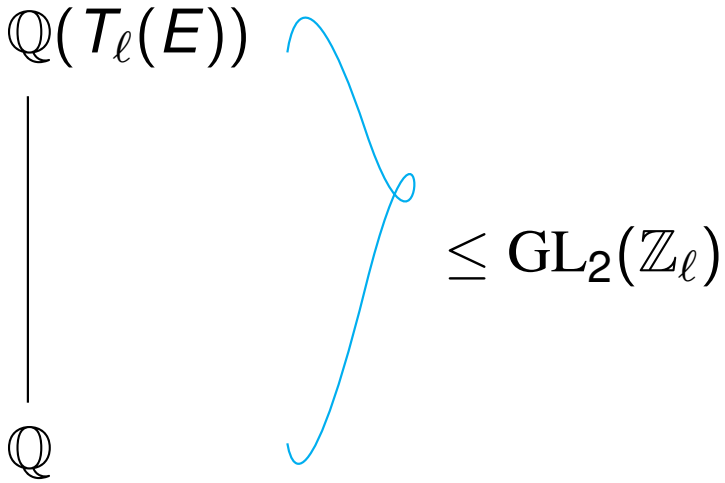
Facts:

- The N-division points form a group that is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. For example, $E[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$, a Klein 4-group.
- The Galois group $G_{\mathbb{Q}}$ permutes the N-division points. We denote the representation by $\overline{\rho}_{E,N}$.

We will write $\mathbb{Q}(E[N])$ to mean the field obtained by adjoining all of the coordinates of the N-division points of E to $\mathbb{Q}$.

Fix a prime ℓ and define the Tate module to be he inverse limit $T_\ell(E) = \varprojlim_n E[\ell^n]$

There is a representation $\rho_{E,\ell}$ from $G_{\mathbb{Q}}$ acting on $T_\ell(E)$ over $\mathbb{Q}$ into $\mathrm{Aut}(\mathbb{Z}_\ell^2)$, which after a choice of basis can be identified with $\mathrm{GL}_2(\mathbb{Z}_\ell)$.



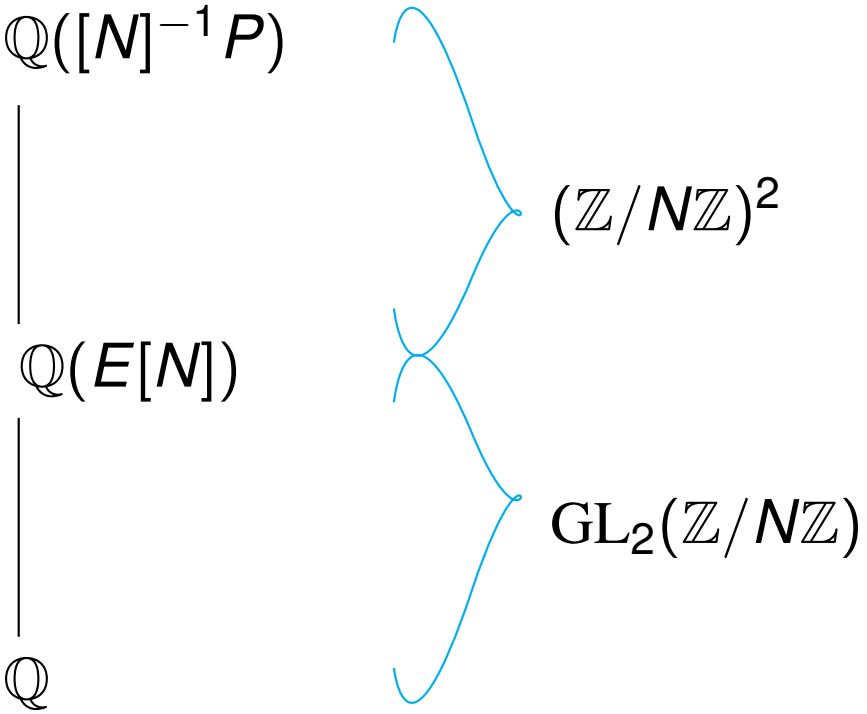
- Consider the case that E is an elliptic curve over $\mathbb{Q}$ without complex multiplication. In this case, a result of Serre shows that the image of $\rho_{E,\ell}$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ. Also, the representation is surjective except for a finite set of primes S_E.
- $\ell = 2$ The map $\rho_{E,2}$ is surjective if and only if $\overline{\rho}_{E,8}$ is surjective.
- $\ell = 3$ The map $\rho_{E,3}$ is surjective if and only if $\overline{\rho}_{E,9}$ is surjective.
- $\ell \geq 5$ The map $\rho_{E,\ell}$ is surjective if and only if $\overline{\rho}_{E,\ell}$ is surjective.

Let E be given by $y^2 = x^3 + Ax + B$. Fix a point $P \in E(\mathbb{Q})$ given by $P = (z : w : 1)$. Consider the set

$$V = [N]^{-1}P = \left\{ Q \in E(\overline{\mathbb{Q}}) | \quad [N]Q = P \right\}.$$

For example, when $P = \mathcal{O}$, this set is the set of N-division points.

This is no longer a group in general, but we can still adjoin the coordinates of such points to $\mathbb{Q}$ and find the Galois group of the extension.


$\mathbb{Q}([N]^{-1}P)$
$\mathbb{Q}(E[N])$
$\mathbb{Q}$
$(\mathbb{Z}/N\mathbb{Z})^2$
$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

The Galois group of $\mathbb{Q}([N]^{-1}P)$ over $\mathbb{Q}$ is a subgroup of the affine general linear group

$$1 \to (\mathbb{Z}/N\mathbb{Z})^2 \to \mathrm{AGL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1$$

e.g. for $N = 2$

$$1 \to (\mathbb{Z}/2\mathbb{Z})^2 \to S_4 \to S_3 \to 1$$

$$\left\{ \begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix} : a, b, c, d, e, f \in (\mathbb{Z}/N\mathbb{Z}) \text{ and } ad - bc \neq 0 \right\}$$

Again, fixing ℓ and taking an inverse limit yields a representation

$$\rho_{E,\ell,P} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{Z}_\ell^2) \simeq \mathrm{AGL}_2(\mathbb{Z}_\ell)$$

Table of Contents

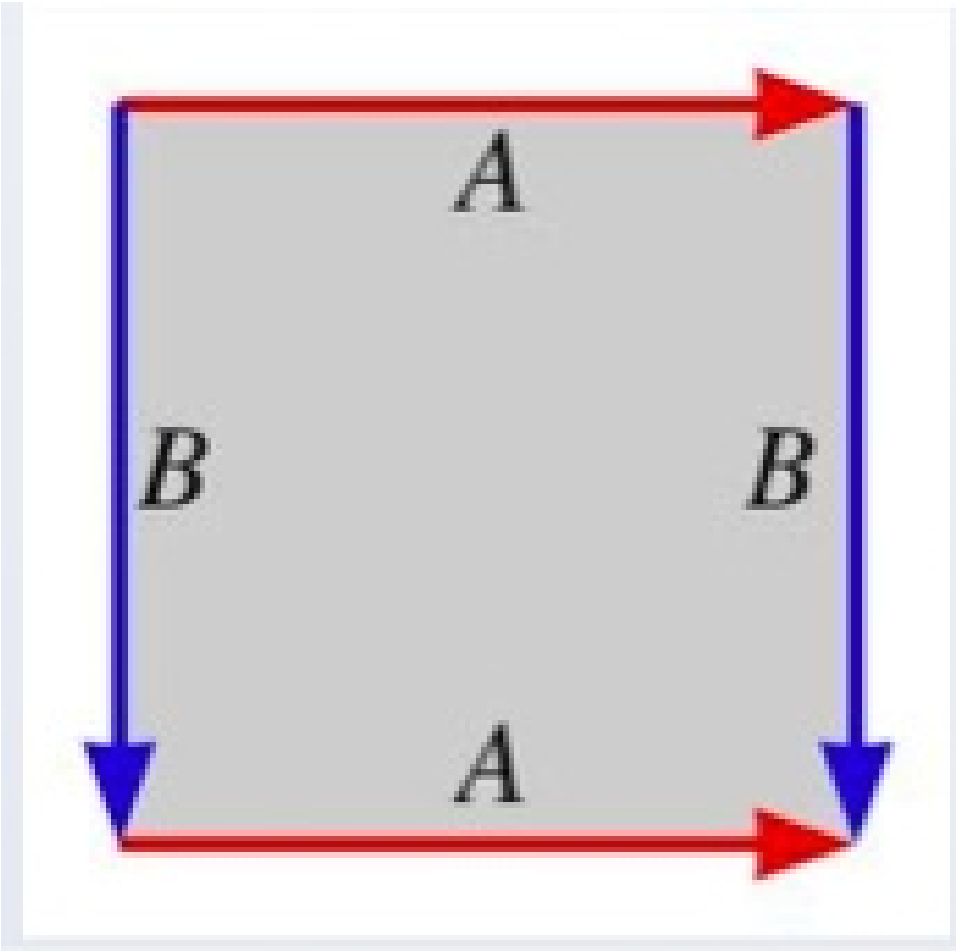
There is an exact sequence (due to Grothendieck and others) of fundamental groups

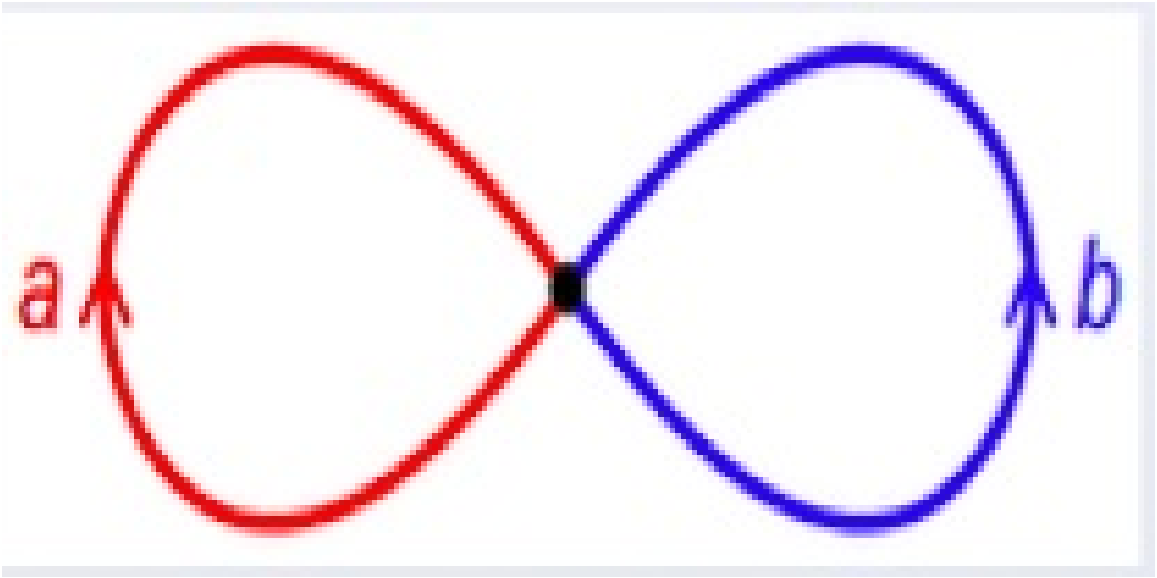
$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}) \to \pi_1(X) \to G_{\mathbb{Q}} \to 1$$

which group-theoretically gives rise to a representation

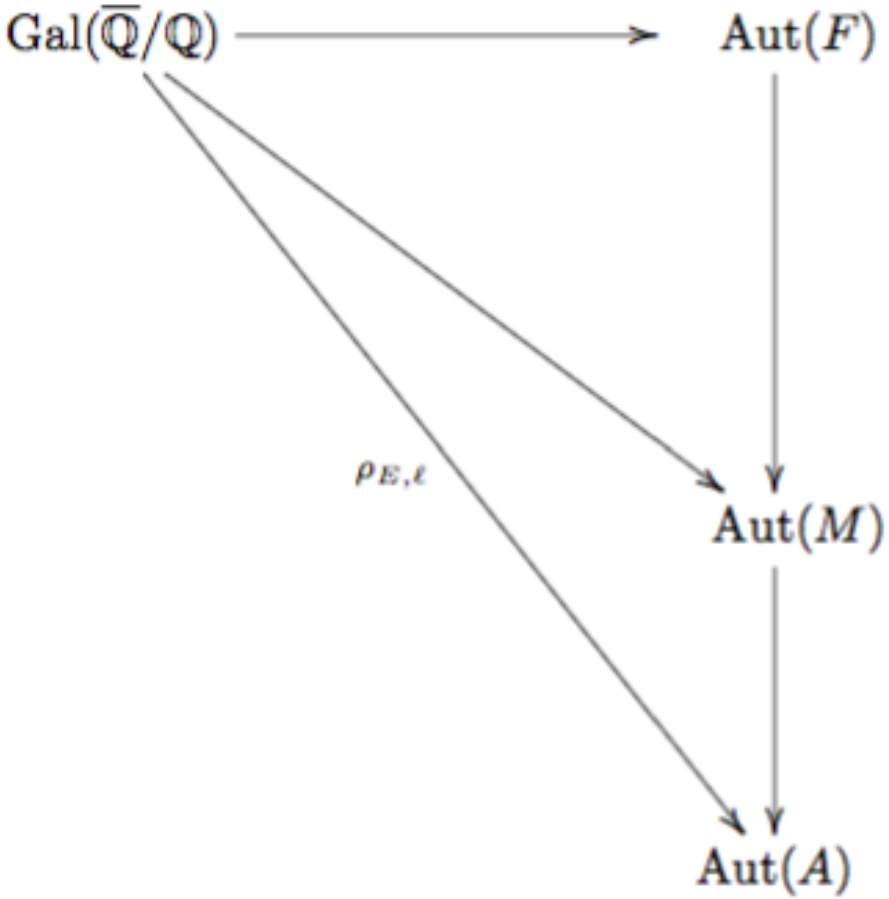
$$\rho_X : G_{\mathbb{Q}} \to \mathrm{Aut}(\pi_1(X_{\overline{\mathbb{Q}}})).$$

There are comparison theorems that allow one to determine the geometric fundamental group by considering the variety X over $\mathbb{C}$.


A
B
B
A


a
b

Any two-generated group should arise as the group of deck transformations of some cover of a once-punctured elliptic curve. So far, we have only encountered the abelian deck groups $\mathbb{Z}_\ell^2$. We will restrict to studying pro-ℓ groups (for now pro-2) and look for some barely non-abelian examples.


$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
$\mathrm{Aut}(F)$
$\rho_{E,\ell}$
$\mathrm{Aut}(M)$
$\mathrm{Aut}(A)$

Define

$$M_2 = \left\{ a, b, c | a^4, b^4, c^2, c = aba^{-1}b^{-1}, ac = ca, bc = cb \right\}$$

Then M_2 is a group of order 32 whose abelianization is $(\mathbb{Z}/4\mathbb{Z})^2$. Also, Q_8, the finite group of order 8 of the quaternions is a characteristic quotient of M_2.

Theorem (D., Goins)

Suppose that

$$\overline{\rho}_{E,8} \text{ and } \overline{\rho}_{E,M_2}$$

are both surjective. Then, the representation to $\mathrm{Aut}(M)$ *is surjective.*

Let E be an elliptic curve over $\mathbb{Q}$.

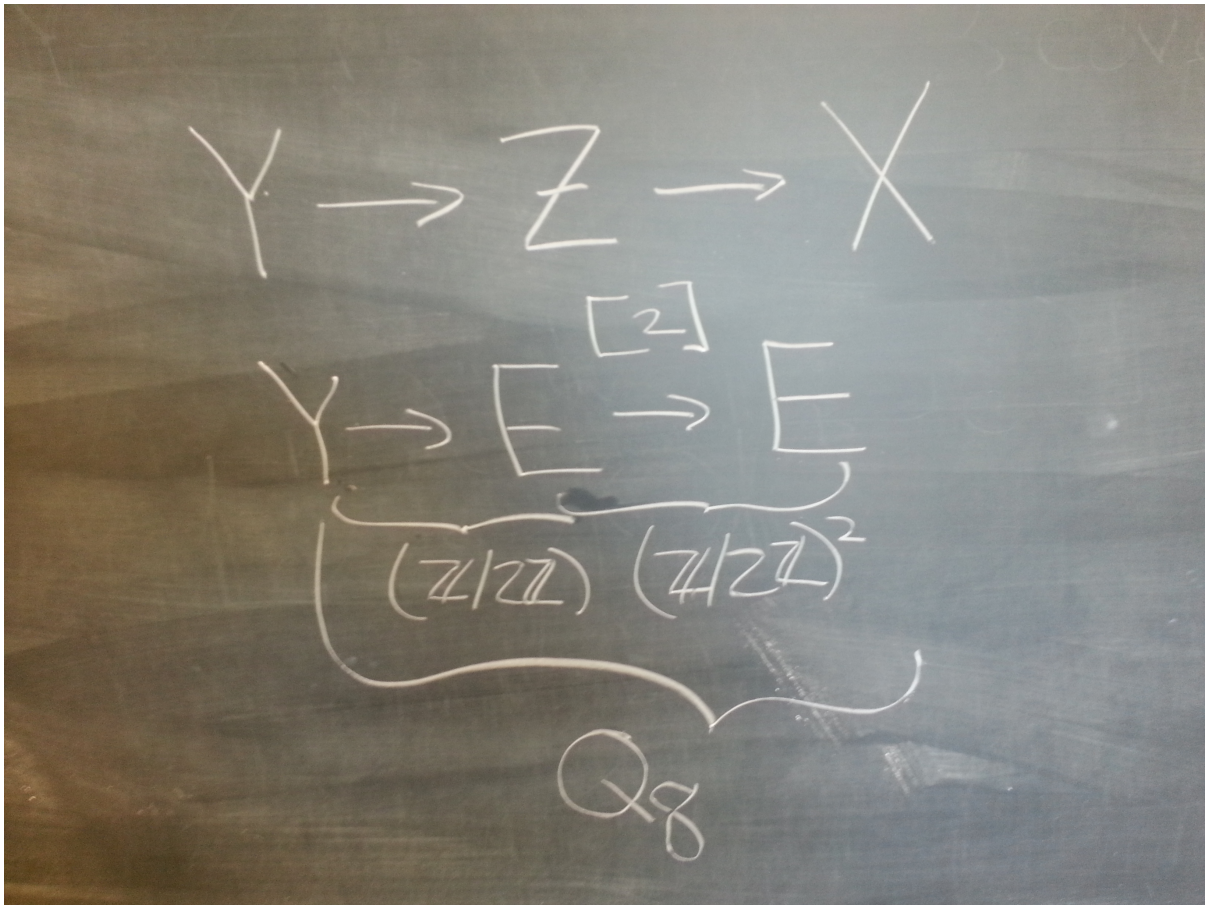
Definition

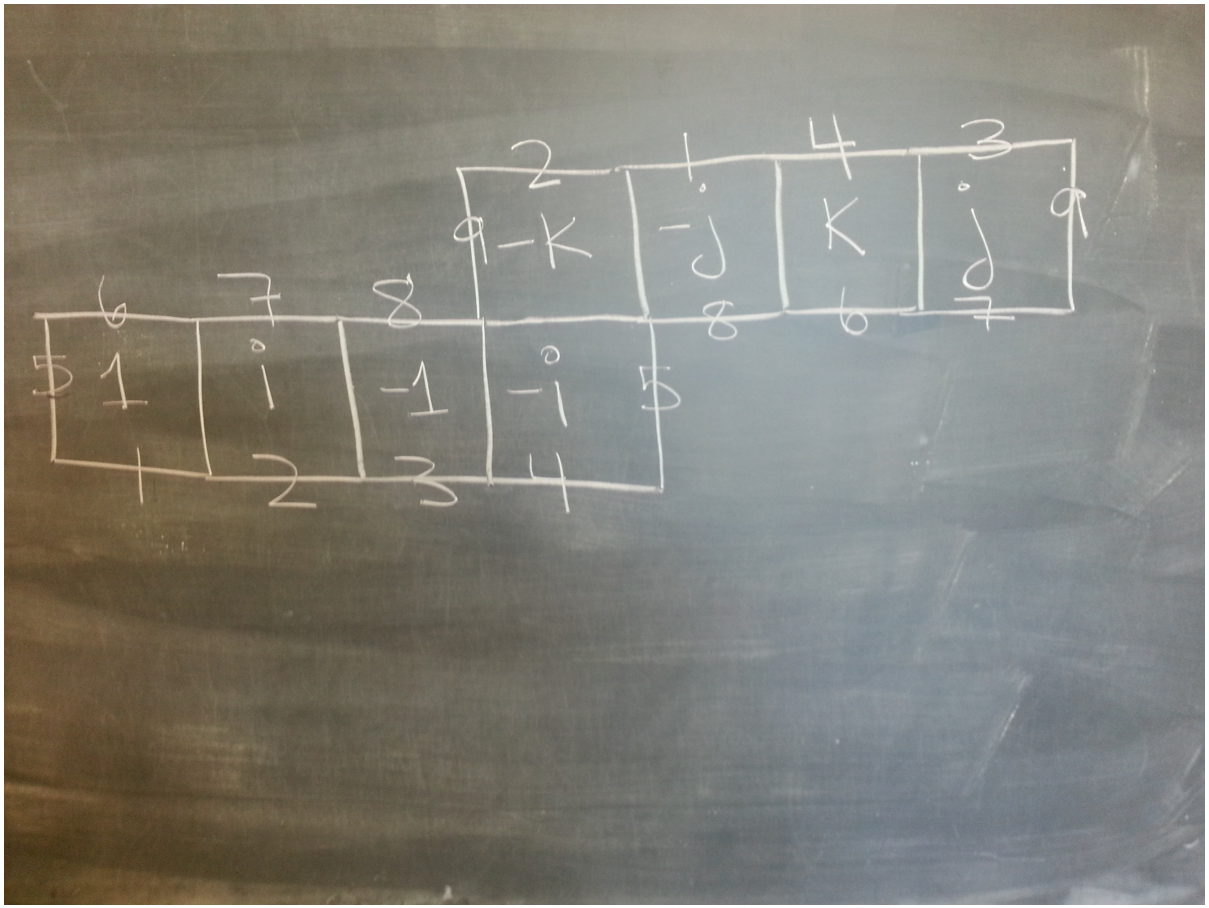
An origami is a pair (C, f) where C is a curve and $f : C \to E$ is a map branched above at most one point.

Definition

A deck transformation or automorphism of a cover $f : C \to E$ is a homeomorphism $g : C \to C$ such that $f \circ g = f$.

Each deck transformation permutes the elements of each fiber. This defines a group action of the the deck transformations on the fibers.


Y → Z → X
[2]
Y → E → E
(Z/2Z) (Z/2Z)²
Q8


2
1
4
3
9
-k
-j
k
j
9
6
7
8
8
6
7
5
1
i
-1
-i
5
4
2
3
4

“An extraordinary origami curve" by Herrlich and Schmithüesen

$$f = 8$$

$$e = \frac{8 \cdot 4}{2} = 16$$

$$v = \frac{8 \cdot 4}{4 \cdot 2} = 4$$

Formula for Euler characteristic:

$$2 - 2g = v - e + f$$

$$\implies g = 3$$

Riemann-Hurwitz formula

$$f : Y \to X$$

Then,

$$2g(Y) - 2 = \deg(f) \cdot (2g(Z) - 2) + \sum_{z \in Z} (e_z - 1)$$

Applying Riemann-Hurwitz with $g(Y) = 3$, $g(X) = 1$, we see that there are 4 points ramified in Y, each with ramification degree 2.

In fact, Herrlich and Schmithüesen give that the map $Y \to Z$ is given by $(x, y) \mapsto (x, y^2)$ and $Y : y^4 = x^3 + Ax + B$. This is an example of a superelliptic curve.

Let $\Delta = -16(4A^3 + 27B^2)$ and w_2, ϕ_2, ψ_2 be the usual division polynomials of elliptic curves as defined e.g. by Silverman. Taking the resultant of $\phi_2 - z\psi_2^2$ and $w_2 - w\psi_2^3$ yields $y^4 - 8wy^3 + 6(2Az + 3B)y^2 - \Delta = 0$. Plugging in y^2 for y yields

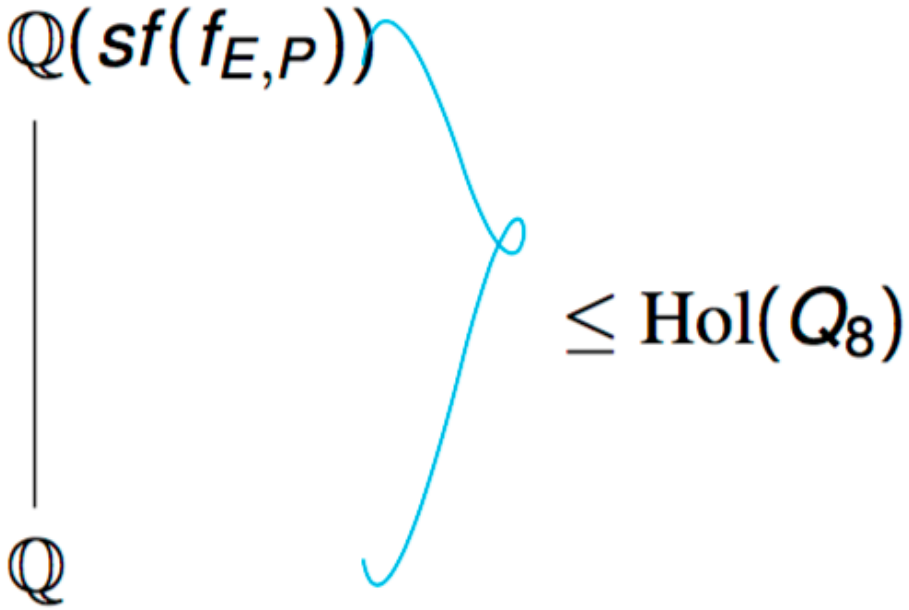
$$f_{E,Q_8,P} = y^8 - 8wy^6 + 6(2Az + 3B)y^4 - \Delta$$

Theorem (D., Goins)

Fix a rational point $P = (z : w : 1) \in E(\mathbb{Q})$. Consider the extension $F_P = \mathbb{Q}(sf(f_{E,Q_8,P}))/\mathbb{Q}$ given by the splitting field of the polynomial $f_{E,Q,8,P}$. Then

$$\mathrm{Gal}(F_P/\mathbb{Q}) \leq \mathrm{Hol}(Q_8)$$

with equality if the polynomial is irreducible.


$\mathbb{Q}(sf(f_{E,P}))$
$\mathbb{Q}$
$\leq \mathrm{Hol}(Q_8)$

$$1 \to Q_8 \to \mathrm{Hol}(Q_8) \to \mathrm{Aut}(Q_8) \simeq S_4 \to 1$$

The group $\mathrm{Hol}(Q_8)$ is a specific group of order 192.

There is a quotient from $\rho_{E,Q_8,P} : G_{\mathbb{Q}} \to \mathrm{Hol}(Q_8)$ to $\rho_{E,Q_8} : G_{\mathbb{Q}} \to \mathrm{Aut}(Q_8)$

Theorem (D., Goins)

The image of the quotient is given by the Galois group of the splitting field of $x^4 - 4\Delta x - 12A\Delta$.

Remark: This quartic polynomial defines the unique S_4-representation contained inside of the 4-division representation of E. (See, for instance, Adelmann's "The decomposition of primes in torsion point fields".)

Thank you! Questions?