Galois theory of a quaternion group origami

Special Session on Automorphisms of Riemann Surfaces and Related Topics
AMS Central Fall Sectional Meeting
Loyola University Chicago, Chicago, IL

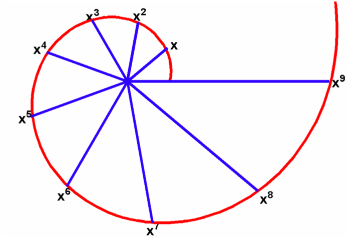
Rachel Davis
Joint work with Professor Edray Goins
Purdue University

October 3, 2015

Table of Contents

Table of Contents

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



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

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

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

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

$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$.
$\sigma_i : \zeta_N \mapsto \zeta_N^i, (i, N) = 1$

$$\left.\begin{array}{c}\mathbb{Q}(\zeta_N)\\ \Big| \\ \mathbb{Q}\end{array}\right\} (\mathbb{Z}/N\mathbb{Z})^\times$$

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

$$
\begin{array}{c}
\mathbb{Q}(\sqrt[N]{p}, \zeta_N) \\
| \\
\mathbb{Q}(\zeta_N) \\
| \\
\mathbb{Q}
\end{array}
\qquad
\begin{array}{l}
\left.\vphantom{\begin{array}{c} a \\ a \end{array}}\right\} (\mathbb{Z}/N\mathbb{Z}) \\
\left.\vphantom{\begin{array}{c} a \\ a \end{array}}\right\} (\mathbb{Z}/N\mathbb{Z})^{\times}
\end{array}
$$

- $\mathrm{Gal}(sf(x^N - p)/\mathbb{Q})$ 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 $\sigma(\zeta_N) = \zeta_N^p$ and $\frac{\sigma(\sqrt[N]{d})}{\sqrt[N]{d}} = \zeta_N^a$, so $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $b \in (\mathbb{Z}/N\mathbb{Z})$.

Table of Contents

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

Definition

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

We study automorphisms of origamis and relate these to polynomials over $\mathbb{Q}$.

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.

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 $G_{\mathbb{Q}}$ sends division points to division points.

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 $\mathbb{Q}$.

The Galois group of $\mathbb{Q}(E[N])$ over $\mathbb{Q}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

$$\begin{array}{c} \mathbb{Q}(E[N]) \\ | \\ \mathbb{Q} \end{array} \quad \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

For example, the Galois group of $\mathbb{Q}(E[2])/\mathbb{Q}$ is a subgroup of the **automorphism** group of $E[2]$ and

$$\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq S_3.$$

After choice of basis,

$$\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}).$$

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

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

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.

$$\begin{tikzcd}
\mathbb{Q}([N]^{-1}P) \arrow[dd, dash] & \\
 & (\mathbb{Z}/N\mathbb{Z})^2 \\
\mathbb{Q}(E[N]) \arrow[dd, dash] & \\
 & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\
\mathbb{Q} &
\end{tikzcd}$$

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 $N = 2$

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

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

There is a representation

$$\rho_{N,P} : G_{\mathbb{Q}} \to \mathrm{AGL}_2(\mathbb{Z}/N\mathbb{Z}).$$

- Let T_1, T_2 is a basis for $E[N]$.
- Suppose $\sigma(T_1) = aT_1 \oplus cT_2$ and $\sigma(T_2) = bT_1 \oplus dT_2$.

- Choose any $Q \in \overline{\mathbb{Q}}$ such that $[N]Q = P$.
- Suppose $\sigma(Q) \ominus Q = eT_1 \oplus fT_2$.

Then the top representation is given by

$$\sigma \mapsto \begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix}$$

Multiplication by 2

$$E : y^2 = x^3 + Ax + B$$

The formula for the x-coordinate of $[2]P = P \oplus P$ $(P = (z : w : 1))$ is the following:

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

Proposition

Fix a rational point $P = (z : w : 1)$. Consider the extension $F_P = \mathbb{Q}(sf([2]^{-1}P))$ over $\mathbb{Q}$, where $F_P/\mathbb{Q}$ is given by the splitting field of the quartic

$$f_{E,P}(x) = (x^4 - 2Ax^2 - 8Bx + A^2) - 4z(x^3 + Ax + B).$$

If this polynomial is irreducible, then $\mathbb{Q}(sf(F_{E,P}))/\mathbb{Q}$ is an S_4-extension. Note that $S_4 = \mathrm{AGL}_2(\mathbb{Z}/2\mathbb{Z})$.

The example

$$1 \to V_4 \to S_4 \to S_3 \to 1$$

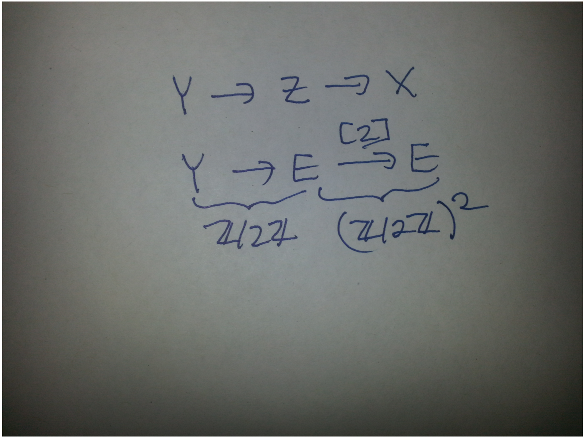
is a specific case of a more general theory. Take the semidirect product of a group and its automorphism group where the action of the quotient on the automorphism group of the normal subgroup is the identity.

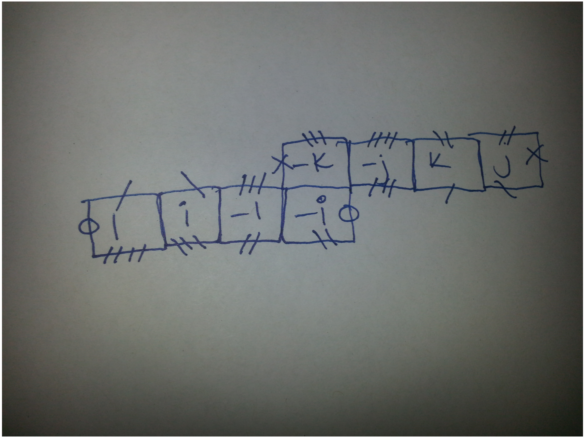
$$1 \to G \to \mathrm{Hol}(G) \to \mathrm{Aut}(G) \to 1$$

Question: What about non-abelian deck groups G?
Example: Q_8 group of quaternions, non-abelian group of order 8.

An origami with the example deck group is studied in a paper titled, "An extraordinary origami curve" by Herrlich and Schithüsen.

Table of Contents


$Y \to Z \to X$
$Y \to E \xrightarrow{[2]} E$
$\mathbb{Z}/2\mathbb{Z}$
$(\mathbb{Z}/2\mathbb{Z})^2$


1
i
−1
−i
−k
−j
k
j

$$f = 8$$

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

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

Formula for Euler characteristic:

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

$$\implies g = 3$$

Riemann-Hurwitz formula

$$f : Y \to Z$$

Then

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

Using the formula, with $g(Y) = 3$ $g(Z) = 1$, we see that there are 4 points in Y above the 2-division points in Z, each with ramification degree 2.

In fact, Herrlich and Schithüsen give that $Y : y^4 = x^3 + Ax + B$. This is an example of a superelliptic curve. The map

$$Y \to Z$$

is given by

$$(x, y) \mapsto (x, y^2)$$

.

Let g be the composition $Y \to Z \to X$. To find the $g^{-1}(P)$ points, we give a formula for multiplication by 2 in terms of the y-coordinates.

$$\phi_2 - z\psi_2^2$$

degree 4 in x

$$\omega_2 - w\psi_2^3$$

degree 6 in x (We will think of y as part of the coefficients).

The resultant polynomial for $P = (z : w : 1)$ is $y^4 - 8wy^3 + 6(2Az + 3B)y^2 - \Delta = 0$. Plugging in y^2 instead of y gives

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

Theorem (D., Goins)

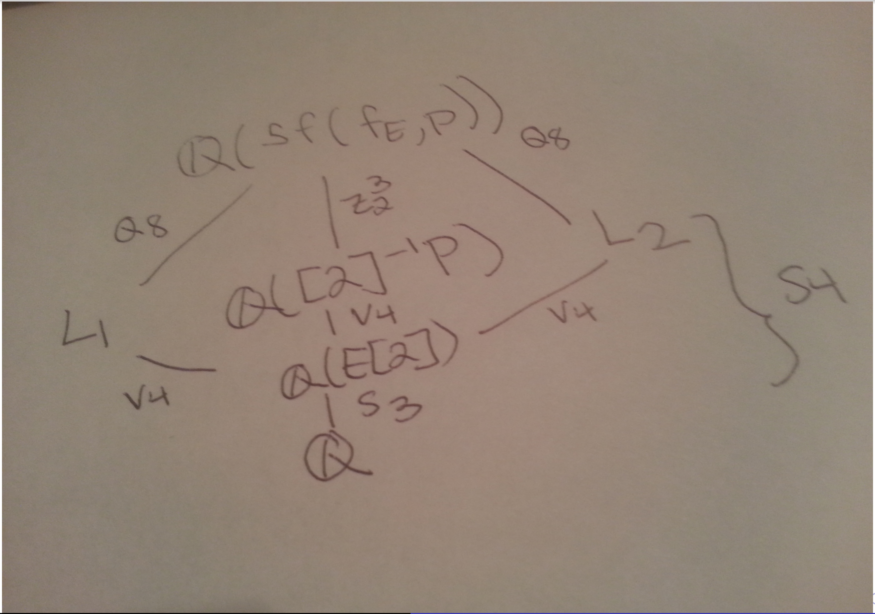
Fix a rational point $P = (z : w : 1)$. Consider the extension $F_P = \mathbb{Q}(sf(f_{E,P}))/\mathbb{Q}$ given by the splitting field of the polynomial $f_{E,P}$. If the polynomial is irreducible, then

$$\mathrm{Gal}(\mathbb{Q}(f_{E,P})/\mathbb{Q}) = \mathrm{Hol}(Q_8).$$

$$\left.\begin{array}{c} \mathbb{Q}(sf(f_{E,P})) \\ \Big| \\ \mathbb{Q} \end{array}\right\} \leq \mathrm{Hol}(Q_8)$$

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

Therefore, $\mathrm{Hol}(Q_8)$ is a specific group of order 192. Let $\Delta = -16(4A^3 + 27B^2)$.


ℚ(sf(f_E, P))
Q8
Z_2^3
Q8
L2
S4
L1
ℚ([2]^{-1}P)
V4
V4
ℚ(E[2])
V4
S3
ℚ

$$
\begin{aligned}
f_1 = {} & y^4 + 4\Delta y^3 + (512B^2\Delta - 2048Bz^3\Delta + 2048Bw^2\Delta \\
& + 2048z^6\Delta - 4096z^3w^2\Delta + 2048w^4\Delta + 6\Delta^2)y^2 \\
& + 1769472w^8\Delta^2 + 331776B^2z^6\Delta^2 - 884736B^2z^3w^2\Delta^2 + \\
& 3538944B^2w^4\Delta^2 + 512B^2\Delta^3 - 512B^2\Delta^2 - 1327104Bz^9\Delta^2 \\
& + 18432w^4\Delta^3 + 2654208Bz^6w^2\Delta^2 + 1327104Bz^3w^4\Delta^2 \\
& - 1024Bz^3\Delta^3 + 10240Bw^2\Delta^3 - 35224100536320w^6z^3\Delta^2 \\
& + 49313740750848w^4z^6\Delta^2 + 1327104z^{12}\Delta^2 \\
& - 5750784z^9w^2\Delta^2 + 9289728z^6w^4\Delta^2 + 2304z^6\Delta^3 - \\
& 6635520z^3w^6\Delta^2 - 9216z^3w^2\Delta^3 + \Delta^4
\end{aligned}
$$

Does L_1 really depend on P? There is an isomorphism from L_1 the the splitting field of $x^4 - 4\Delta x - 12A\Delta$. This is a special polynomial because it defines the S_4 extension contained inside of $\mathbb{Q}(E[4])$. What about L_2?

Thank you. Questions?