Galois groups of rational functions with non-trivial automorphisms

Rafe Jones

College of the Holy Cross

October 3, 2009

Galois representations from elliptic curves

A classic problem: let E be an elliptic curve defined over $\mathbb{Q}$, and consider the extension K_∞ of $\mathbb{Q}$ obtained by adjoining the torsion points $E[p^n]$ for all $n \geq 1$.

Galois representations from elliptic curves

A classic problem: let E be an elliptic curve defined over $\mathbb{Q}$, and consider the extension K_∞ of $\mathbb{Q}$ obtained by adjoining the torsion points $E[p^n]$ for all $n \geq 1$.

Let G_∞ be the Galois group of K_∞ over $\mathbb{Q}$.

Galois representations from elliptic curves

A classic problem: let E be an elliptic curve defined over $\mathbb{Q}$, and consider the extension K_∞ of $\mathbb{Q}$ obtained by adjoining the torsion points $E[p^n]$ for all $n \geq 1$.

Let G_∞ be the Galois group of K_∞ over $\mathbb{Q}$.

Because $E[p^n] \cong (\mathbb{Z}/p\mathbb{Z})^2$, we have $G_\infty \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$.

Galois representations from elliptic curves

A classic problem: let E be an elliptic curve defined over $\mathbb{Q}$, and consider the extension K_∞ of $\mathbb{Q}$ obtained by adjoining the torsion points $E[p^n]$ for all $n \geq 1$.

Let G_∞ be the Galois group of K_∞ over $\mathbb{Q}$.

Because $E[p^n] \cong (\mathbb{Z}/p\mathbb{Z})^2$, we have $G_\infty \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$.

Problem: What is $[\mathrm{GL}_2(\mathbb{Z}_p) : G_\infty]$?

Now suppose that E has complex multiplication, i.e. there is an endomorphism α of E that is not $[m]$ for any m.

Now suppose that E has complex multiplication, i.e. there is an endomorphism α of E that is not $[m]$ for any m.

Then G_∞ must commute with α, and thus injects into either

a Borel subgroup $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$ or a Cartan subgroup $\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$

Now suppose that E has complex multiplication, i.e. there is an endomorphism α of E that is not $[m]$ for any m.

Then G_∞ must commute with α, and thus injects into either

$$\text{a Borel subgroup } \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \qquad \text{or a Cartan subgroup } \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$$

(assuming we replace $\mathbb{Q}$ by the CM field of E, conjugate appropriately, and possibly allow the coefficients to live in the ring of integers of a quadratic extension of $\mathbb{Q}_p$)

Now suppose that E has complex multiplication, i.e. there is an endomorphism α of E that is not $[m]$ for any m.

Then G_∞ must commute with α, and thus injects into either

$$\text{a Borel subgroup } \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \qquad \text{or a Cartan subgroup } \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$$

(assuming we replace $\mathbb{Q}$ by the CM field of E, conjugate appropriately, and possibly allow the coefficients to live in the ring of integers of a quadratic extension of $\mathbb{Q}_p$)

In fact, for all but finitely many p, G_∞ injects into a Cartan subgroup C.

Problem: What is $[C : G_\infty]$?

Problem: What is $[C : G_\infty]$?

Answer: (Serre 1972) If E has no CM, then $[\mathrm{GL}_2(\mathbb{Z}_p) : G_\infty] < \infty$. If E has CM and $G_\infty \hookrightarrow C$, then $[C : G_\infty] < \infty$. Moreover, in either case for all but finitely many p the index is 1.

Dynamical analogues

In the previous setup, we could have defined K_∞ to be obtained from $\mathbb{Q}$ by adjoining all preimages of O under iteration of the map $[p]$ on E.

Dynamical analogues

In the previous setup, we could have defined K_∞ to be obtained from $\mathbb{Q}$ by adjoining all preimages of O under iteration of the map $[p]$ on E.

Let's replace E by $\mathbb{P}^1$, and replace $[p]$ by a rational map $\phi \in \mathbb{Q}(x)$.

Dynamical analogues

In the previous setup, we could have defined K_∞ to be obtained from $\mathbb{Q}$ by adjoining all preimages of O under iteration of the map $[p]$ on E.

Let's replace E by $\mathbb{P}^1$, and replace $[p]$ by a rational map $\phi \in \mathbb{Q}(x)$.

Let $K_n = \mathbb{Q}(\phi^{-n}(0)$, $K_\infty = \bigcup_n K_n$, $G_\infty = \mathrm{Gal}(K_\infty/\mathbb{Q})$.

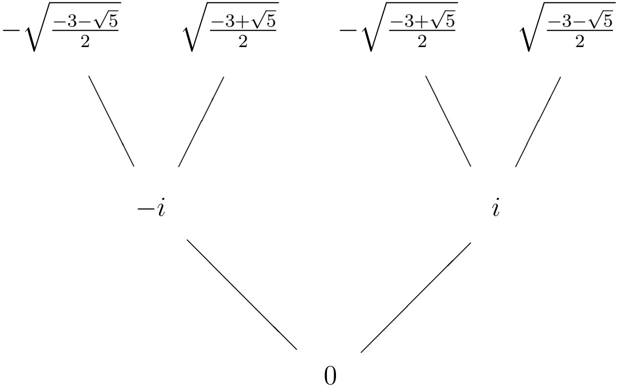
Dynamical analogues

In the previous setup, we could have defined K_∞ to be obtained from $\mathbb{Q}$ by adjoining all preimages of O under iteration of the map $[p]$ on E.

Let's replace E by $\mathbb{P}^1$, and replace $[p]$ by a rational map $\phi \in \mathbb{Q}(x)$.

Let $K_n = \mathbb{Q}(\phi^{-n}(0)$, $K_\infty = \bigcup_n K_n$, $G_\infty = \mathrm{Gal}(K_\infty/\mathbb{Q})$.

Unlike the elliptic curves case, $\phi^{-n}(0)$ has no group structure, but $T_0 := \bigcup_n \phi^{-n}(0)$ has a natural tree structure. So $G_\infty \hookrightarrow \mathrm{Aut}(T_0)$.


$-\sqrt{\frac{-3-\sqrt{5}}{2}}$
$\sqrt{\frac{-3+\sqrt{5}}{2}}$
$-\sqrt{\frac{-3+\sqrt{5}}{2}}$
$\sqrt{\frac{-3-\sqrt{5}}{2}}$
$-i$
i
0

First two levels of preimage tree T_0 for $\phi(x) = \frac{x^2+1}{x}$, initial point 0.

Problem: Is $[\mathrm{Aut}(T_0) : G_\infty] < \infty$?

Problem: Is $[\mathrm{Aut}(T_0) : G_\infty] < \infty$?

Even restricting to quadratic polynomials, there are very few results. It is known that $[\mathrm{Aut}(T_0) : G_\infty] < \infty$ for

- $\phi(x) = x^2 + a$, for $a > 0, a \equiv 1, 2 \bmod 4$ and $a < 0, a \equiv 0 \bmod 4$ (Stoll 1992),
- $\phi(x) = x^2 - ax + a$, $a \in \mathbb{Z}$
  $\phi(x) = x^2 + ax - 1, a \in \mathbb{Z} \setminus \{0, 2\}$ (RJ 2008).

Dynamical complex multiplication

When ϕ commutes with another map $\alpha \in \mathbb{Q}(x)$ fixing 0, then the action of G_∞ on T_0 must commute with the action of α on T_0.

Dynamical complex multiplication

When ϕ commutes with another map $\alpha \in \mathbb{Q}(x)$ fixing 0, then the action of G_∞ on T_0 must commute with the action of α on T_0.

Ritt (1922): except for very unusual ϕ, α must have degree 1, and thus be a Mobius transformation.

Dynamical complex multiplication

When ϕ commutes with another map $\alpha \in \mathbb{Q}(x)$ fixing 0, then the action of G_∞ on T_0 must commute with the action of α on T_0.

Ritt (1922): except for very unusual ϕ, α must have degree 1, and thus be a Mobius transformation.

Let $\mathrm{Aut}(\phi)$ be the group of Mobius transformations commuting with ϕ.

Dynamical complex multiplication, quadratic case

If $\deg \phi = 2$, then apart from two exceptional maps, either $\#\mathrm{Aut}(\phi) = 1$ or $\#\mathrm{Aut}(\phi) = 2$.

Dynamical complex multiplication, quadratic case

If $\deg \phi = 2$, then apart from two exceptional maps, either $\#\mathrm{Aut}(\phi) = 1$ or $\#\mathrm{Aut}(\phi) = 2$.

The Galois group of $\mathbb{Q}\left(\bigcup_n \phi^{-n}(b)\right)$ over $\mathbb{Q}$ is determined by the $\mathrm{PGL}_2(\mathbb{Q})$-conjugacy class of the pair (ϕ, b).

Dynamical complex multiplication, quadratic case

If $\deg \phi = 2$, then apart from two exceptional maps, either $\#\mathrm{Aut}(\phi) = 1$ or $\#\mathrm{Aut}(\phi) = 2$.

The Galois group of $\mathbb{Q}\left(\bigcup_n \phi^{-n}(b)\right)$ over $\mathbb{Q}$ is determined by the $\mathrm{PGL}_2(\mathbb{Q})$-conjugacy class of the pair (ϕ, b).

Proposition

Let (ϕ, b) consist of a quadratic rational function ϕ and basepoint $b \in \mathbb{P}^1(\mathbb{Q})$ such that ϕ commutes with a Mobius transformation α of order 2 and $\alpha(b) = b$. Then (ϕ, b) is conjugate to

$$\left(\frac{k(x^2+m)}{cx}, 0\right)$$

for some $k, m, c \in \mathbb{Z}$.

Fix $\phi = \frac{k(x^2+m)}{cx}$ and $\alpha(x) = -x$.

Fix $\phi = \frac{k(x^2+m)}{cx}$ and $\alpha(x) = -x$.

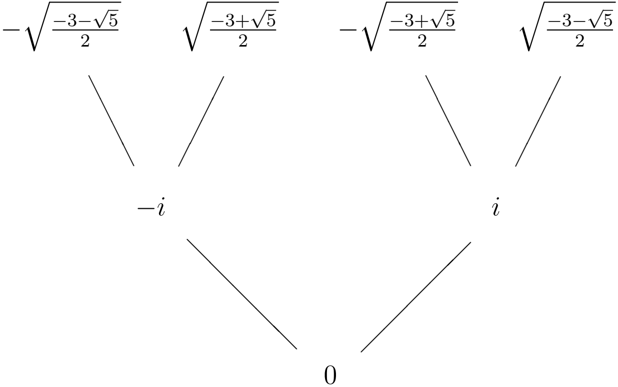
Then $G_\infty \hookrightarrow C(\alpha)$, where $C(\alpha)$ is the centralizer in $\mathrm{Aut}(T_0)$ of the involution induced by α.

Fix $\phi = \frac{k(x^2+m)}{cx}$ and $\alpha(x) = -x$.

Then $G_\infty \hookrightarrow C(\alpha)$, where $C(\alpha)$ is the centralizer in $\mathrm{Aut}(T_0)$ of the involution induced by α.

Remark

Let $T_{0,n}$ be the truncation of T_0 to the first n levels only, and define $C_n(\alpha)$ similarly. Then $C_n(\alpha)$ contains a subgroup of index two that is isomorphic to $\mathrm{Aut}(T_{0,n-1})$.



$-\sqrt{\frac{-3-\sqrt{5}}{2}}$ $\sqrt{\frac{-3+\sqrt{5}}{2}}$ $-\sqrt{\frac{-3+\sqrt{5}}{2}}$ $\sqrt{\frac{-3-\sqrt{5}}{2}}$

$-i$ i

0

$$C_2(\alpha) = \{e, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$$

Theorems for quadratic rational functions

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and define $p_n(x)$ to be the numerator of $\phi^n(x)$. Suppose that for all $n \geq 2$, $kp_n(1)$ is not a square in $\mathbb{Z}$. Then $[C(\alpha) : G_\infty] < \infty$.

Theorems for quadratic rational functions

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and define $p_n(x)$ to be the numerator of $\phi^n(x)$. Suppose that for all $n \geq 2$, $kp_n(1)$ is not a square in $\mathbb{Z}$. Then $[C(\alpha) : G_\infty] < \infty$.

Remark: $p_n(1)$ is the numerator of the *n*th term of the orbit of 1, which is a critical point of ϕ (the other is -1).

Theorems for quadratic rational functions

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and define $p_n(x)$ to be the numerator of $\phi^n(x)$. Suppose that for all $n \geq 2$, $kp_n(1)$ is not a square in $\mathbb{Z}$. Then $[C(\alpha) : G_\infty] < \infty$.

Remark: $p_n(1)$ is the numerator of the *n*th term of the orbit of 1, which is a critical point of ϕ (the other is -1).

Example

If $k = 1$, then $p_n(1)$ is the left coordinate in the recurrence given by $(r_0, s_0) = (1, 1)$, $(r_n, s_n) = (r_{n-1}^2 + s_{n-1}^2, r_{n-1}s_{n-1})$, which proceeds

$$(1, 1), (2, 1), (5, 2), (29, 10), (941, 290), \ldots$$

One can check that in the above example, $p_n(1) \equiv 2 \bmod 3$ for all $n \geq 2$, so the Theorem applies.

Corollary

Suppose that $\phi = \frac{k(x^2+1)}{x}$ *and* $k \bmod 24 \notin \{2, 6, 8, 12, 14, 18, 20\}$*. Then* $[C(\alpha) : G_\infty] < \infty$*.*

One can check that in the above example, $p_n(1) \equiv 2 \bmod 3$ for all $n \geq 2$, so the Theorem applies.

Corollary

Suppose that $\phi = \frac{k(x^2+1)}{x}$ *and* $k \bmod 24 \notin \{2, 6, 8, 12, 14, 18, 20\}$. *Then* $[C(\alpha) : G_\infty] < \infty$.

Proof: Find p such that for k satisfying certain congruences $\bmod p$, $p_n(1)$ is a fixed non-square $\bmod p$ for all $n \geq 2$.

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ *for* $k \in \mathbb{Z}$*, and suppose that* $p_n(1)$ *is not a square for all* $n \geq 2$*. Let* v_p *denote the* p*-adic valuation, and assume in addition that* $v_p(k) = 0$ *for all primes* p *dividing some* $p_j(1)$ *for* $\psi = (x^2+1)/x$*. Then* $G_\infty \cong C(\alpha)$*.*

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and suppose that $p_n(1)$ is not a square for all $n \geq 2$. Let v_p denote the p-adic valuation, and assume in addition that $v_p(k) = 0$ for all primes p dividing some $p_j(1)$ for $\psi = (x^2+1)/x$. Then $G_\infty \cong C(\alpha)$.

So $G_\infty \cong C(\alpha)$ for $k = 1, 3, 7, 9, 11, 13, 17, 19, 21, \ldots$.

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and suppose that $p_n(1)$ is not a square for all $n \geq 2$. Let v_p denote the p-adic valuation, and assume in addition that $v_p(k) = 0$ for all primes p dividing some $p_j(1)$ for $\psi = (x^2+1)/x$. Then $G_\infty \cong C(\alpha)$.

So $G_\infty \cong C(\alpha)$ for $k = 1, 3, 7, 9, 11, 13, 17, 19, 21, \ldots$.

Remark: Recall that $p_j(1)$ for $\psi = (x^2+1)/x$ is given by the left coordinate in the recurrence $(r_0, s_0) = (1, 1)$, $(r_n, s_n) = (r_{n-1}^2 + s_{n-1}^2, r_{n-1}s_{n-1})$. Thus a prime dividing some $p_j(1)$ must be the sum of two squares, and therefore is 1 mod 4.

Theorem (RJ-Michelle Manes)

Let $\phi = \frac{k(x^2+1)}{x}$ for $k \in \mathbb{Z}$, and suppose that $p_n(1)$ is not a square for all $n \geq 2$. Let v_p denote the p-adic valuation, and assume in addition that $v_p(k) = 0$ for all primes p dividing some $p_j(1)$ for $\psi = (x^2+1)/x$. Then $G_\infty \cong C(\alpha)$.

So $G_\infty \cong C(\alpha)$ for $k = 1, 3, 7, 9, 11, 13, 17, 19, 21, \ldots$.

Remark: Recall that $p_j(1)$ for $\psi = (x^2+1)/x$ is given by the left coordinate in the recurrence $(r_0, s_0) = (1, 1)$, $(r_n, s_n) = (r_{n-1}^2 + s_{n-1}^2, r_{n-1}s_{n-1})$. Thus a prime dividing some $p_j(1)$ must be the sum of two squares, and therefore is 1 mod 4.

Moreover, one can show the natural density of the set of primes dividing some $p_j(1)$ is zero.

Proof strategy:

1. Show that if there exists a prime $p \in \mathbb{Z}$ that ramifies in $K_n := K(\phi^{-n}(0))$ but not in $K_{n-1} := K(\phi^{-(n-1)}(0))$, then $\mathrm{Gal}(K_n/K_{n-1}) \cong (\ker C_n(\alpha) \to C_{n-1}(\alpha))$.

Proof strategy:

1. Show that if there exists a prime $p \in \mathbb{Z}$ that ramifies in $K_n := K(\phi^{-n}(0))$ but not in $K_{n-1} := K(\phi^{-(n-1)}(0))$, then $\mathrm{Gal}(K_n/K_{n-1}) \cong (\ker C_n(\alpha) \to C_{n-1}(\alpha))$.
2. Show that $\mathrm{Disc}\; p_n$ is divisible only by primes dividing $kp_n(1)$ (c.f. talk of John Cullinan).

Proof strategy:

1. Show that if there exists a prime $p \in \mathbb{Z}$ that ramifies in $K_n := K(\phi^{-n}(0))$ but not in $K_{n-1} := K(\phi^{-(n-1)}(0))$, then $\mathrm{Gal}(K_n/K_{n-1}) \cong (\ker C_n(\alpha) \to C_{n-1}(\alpha))$.
2. Show that $\mathrm{Disc}\ p_n$ is divisible only by primes dividing $kp_n(1)$ (c.f. talk of John Cullinan).
3. Use the fact that $\gcd(kp_i(1), kp_j(1))$ is a power of k (since $\phi(0) = \infty$ and $\phi(\infty) = \infty$) to show that if δ_n is not a square, then apart from finitely many exceptional n, there is some p with $v_p(kp_n(1))$ odd and $v_p(kp_i(1)) = 0$ for $i < n$. This proves the finite index theorem.

Proof strategy:

1. Show that if there exists a prime $p \in \mathbb{Z}$ that ramifies in $K_n := K(\phi^{-n}(0))$ but not in $K_{n-1} := K(\phi^{-(n-1)}(0))$, then $\mathrm{Gal}(K_n/K_{n-1}) \cong (\ker C_n(\alpha) \to C_{n-1}(\alpha))$.
2. Show that $\mathrm{Disc}\, p_n$ is divisible only by primes dividing $kp_n(1)$ (c.f. talk of John Cullinan).
3. Use the fact that $\gcd(kp_i(1), kp_j(1))$ is a power of k (since $\phi(0) = \infty$ and $\phi(\infty) = \infty$) to show that if δ_n is not a square, then apart from finitely many exceptional n, there is some p with $v_p(kp_n(1))$ odd and $v_p(kp_i(1)) = 0$ for $i < n$. This proves the finite index theorem.
4. Assume that $v_q(k) = 0$ for all q dividing $p_j(1)$ for $\psi = (x^2 + 1)/x$. Show that in this case $kp_n(1)$ is divisible to an odd power by a prime not dividing k, for all n.