Some Obstructions to Solvable Points on Higher Genus Curves

James Rawson

Rational Points 2023, Schney
28/07/2023

Pál's Theorems

Question

Given a curve defined over $\mathbb{Q}$, is there a point defined over a solvable number field?

Pál's Theorems

Question

Given a curve defined over $\mathbb{Q}$, is there a point defined over a solvable number field?

Theorem (Pál)

Any curve of genus 0, 2, 3 or 4 defined over a field F has a point defined over a solvable extension of F.

Pál's Theorems

Question

Given a curve defined over $\mathbb{Q}$, is there a point defined over a solvable number field?

Theorem (Pál)

Any curve of genus 0, 2, 3 or 4 defined over a field F has a point defined over a solvable extension of F.

Theorem (Pál)

Let F be a local field where the absolute Galois group of the residue field has quotients isomorphic to S_5, $\mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{PSL}_3(\mathbb{F}_3)$, then there are curves of arbitrarily large genus without solvable points over F.

Varieties Parameterising G-Points

Idea: Rational points are easier to study than points over lots of number fields

Varieties Parameterising G-Points

Idea: Rational points are easier to study than points over lots of number fields
Work with Galois orbits instead — C^n/G, where G acts by permutation of factors.

Varieties Parameterising G-Points

Idea: Rational points are easier to study than points over lots of number fields

Work with Galois orbits instead — C^n/G, where G acts by permutation of factors.

Proposition

The rational points of C^n/G are (unions of) Galois orbits of points defined over number fields with Galois groups contained in G.

General Type

Definition

A smooth variety is of general type if its canonical divisor is big

For example, curves of genus at least 2, as the canonical divisor has a non-trivial section.

General Type

Definition

A smooth variety is of general type if its canonical divisor is big

For example, curves of genus at least 2, as the canonical divisor has a non-trivial section.

Conjecture (Bombieri-Lang)

Rational points are not dense on varieties of general type

G-Points are of General Type

Theorem (R.)

Let G be a transitive subgroup of S_n containing m transpositions of the form $(1, i), i \neq 1$, and C a curve of genus $g \geq 2$. If $g > m+1$, then C^n/G is of general type.

G-Points are of General Type

Theorem (R.)

Let G be a transitive subgroup of S_n containing m transpositions of the form $(1, i), i \neq 1$, and C a curve of genus $g \geq 2$. If $g > m + 1$, then C^n/G is of general type.

Corollary

For any solvable group $G \subset S_n$, and C a curve of genus ≥ 5, under the Bombieri-Lang conjecture rational points are not dense on C^n/G.

At Least 1 Transposition

Let H be the subgroup of G generated by the transpositions. It is normal in G, and isomorphic to a product of S_{m+1}. Moreover, $(m+1)|n$, and $G/H \hookrightarrow S_d$, $d = \frac{n}{m+1}$.

At Least 1 Transposition

Let H be the subgroup of G generated by the transpositions. It is normal in G, and isomorphic to a product of S_{m+1}. Moreover, $(m+1)|n$, and $G/H \hookrightarrow S_d$, $d = \frac{n}{m+1}$.
The quotient variety can therefore be identified with $(\mathrm{Sym}^{m+1} C)^d/(G/H)$. This surjects onto $\mathrm{Sym}^d(\mathrm{Sym}^{m+1} C)$, which is of general type for $g > m+1$.

No Transpositions

The singular points of C^n/G lie within codimension 2 or smaller sets, those where 3 or more coordinates on C^n are the same, or 2 or more pairs are the same. Let X be the resolution.

$$\begin{tikzcd}
C^n \arrow[dr] \arrow[dd, "\pi_1"] & & \\
& C^n/G \arrow[dl, "\pi_2"] & X \arrow[l] \arrow[dll, bend left, "\phi"] \\
\mathrm{Sym}^n C & &
\end{tikzcd}$$

No Transpositions

The singular points of C^n/G lie within codimension 2 or smaller sets, those where 3 or more coordinates on C^n are the same, or 2 or more pairs are the same. Let X be the resolution.

$$\begin{tikzcd}
C^n \arrow[dr] \arrow[dd, "\pi_1"] & & \\
& C^n/G \arrow[dl, "\pi_2"] & X \arrow[l] \arrow[dll, bend left, "\phi"] \\
\mathrm{Sym}^n C & &
\end{tikzcd}$$

The ramification locus of π_1 is the big diagonal, and the same is true of π_2 (away from singular points). Applying Riemann-Hurwitz to π_1 and ϕ shows $K_X \sim_{\mathbb{Q}} \phi^* \pi_{1*} K_{C^n} + E$

Few $\mathbb{P}^1$s

Definition

A rational curve $D \subset \mathrm{Sym}^n C$ is of fibre type if for a generic $P \in C$, there is precisely one point of D which contains P (as a divisor). A curve, D, in C^n/G is of fibre type if the image of D in $\mathrm{Sym}^n C$ is, and it maps injectively onto that image.

Few $\mathbb{P}^1$s

Definition

A rational curve $D \subset \mathrm{Sym}^n C$ is of fibre type if for a generic $P \in C$, there is precisely one point of D which contains P (as a divisor). A curve, D, in C^n/G is of fibre type if the image of D in $\mathrm{Sym}^n C$ is, and it maps injectively onto that image.

Theorem (R.)

Suppose C^n/G contains a curve of fibre type, then C has a morphism to $\mathbb{P}^1$ with Galois group contained in G.

Few $\mathbb{P}^1$s

Definition

A rational curve $D \subset \mathrm{Sym}^n C$ is of fibre type if for a generic $P \in C$, there is precisely one point of D which contains P (as a divisor). A curve, D, in C^n/G is of fibre type if the image of D in $\mathrm{Sym}^n C$ is, and it maps injectively onto that image.

Theorem (R.)

Suppose C^n/G contains a curve of fibre type, then C has a morphism to $\mathbb{P}^1$ with Galois group contained in G.

Theorem (Zariski)

A very general curve of genus at least 7 has no solvable morphisms.

Proof

Assume $D \subset C^n/G$ is of fibre-type, and let $D' \subset \mathrm{Sym}^n C$ be its image.

- Step 1: Find a morphism — rational curves in the symmetric power are contracted, and so the points are linearly equivalent divisors. The condition on points shows that just one function works for all of the points of the curve, D'.
- Step 2: The fibres of this morphism are the divisors — for each point of $\mathbb{P}^1$, the fibre above it is the divisor corresponding to this point on D'.
- Step 3: Check the Galois group of the morphism — Pick a number field, K, large enough that D has infinitely many points over this number field. Every fibre of C above a rational point has Galois group over K contained in G, so by Hilbert Irreducibility, the Galois group of the morphism is contained in G.

Example 1

Example

The modular curve $X_0(34)$ has finitely many points defined over cyclic cubic extensions of $\mathbb{Q}$.

Example 1

Example

The modular curve $X_0(34)$ has finitely many points defined over cyclic cubic extensions of $\mathbb{Q}$.

Proof.

- The rank of $J_0(34)$ is 0, so $J_0(34)(\mathbb{Q})$ is finite
- Rational points of $\mathrm{Sym}^3 X_0(34)$ are confined to finitely many $\mathbb{P}^1$s
- These pullback to either 2 $\mathbb{P}^1$s or a ramified double cover in $X_0(34)^3/A_3$
- As $X_0(34)$ has no automorphisms of order 3, there can be no split $\mathbb{P}^1$s
- Ramification occurs where the discriminant of the morphism vanishes to odd order, and so the cover ramifies in at least 8 points, so is neither rational or elliptic.

□

More Examples

Example

For any number field, K, there are finitely many cyclic cubic extensions, L, of K such that $C(L) \neq C(K)$ for the curve C defined as follows.

$$C := \begin{cases} y^2 + y = x^3 - x \\ z^3 - 3z = x^5 \end{cases}$$

Example

Assuming the Bombieri-Lang conjecture, for any number field K, the modular curve $X_{sp}^{+}(13)$ has finitely many points defined over cyclic cubic extensions of K.