Nonisomorphic curves that become isomorphic over extensions of coprime degrees

Daniel Goldstein[1] Robert M. Guralnick[2]
Everett W. Howe[1] Michael E. Zieve[3]

[1]Center for Communications Research, La Jolla

[2]University of Southern California

[3]Center for Communications Research, Princeton

Special Session on Low Genus Curves and Applications
Joint Mathematics Meetings, San Diego, January 2008

An innocent question.

Suppose

- K is a field,
- L is an extension of K,
- C is a curve over K.

Definition

An *L-twist* of C is a curve D over K, isomorphic to C over L.

Question

Let C and D be curves over $\mathbb{F}_q$.

Suppose D is both an $\mathbb{F}_{q^2}$-twist and a $\mathbb{F}_{q^3}$-twist of C.

Must D be isomorphic to C (over $\mathbb{F}_q$)?

Followup questions.

Suppose D is both an $\mathbb{F}_{q^2}$-twist and a $\mathbb{F}_{q^3}$-twist of C. Must D be isomorphic to C?

If answer is yes:

- Anything special about quadratic and cubic extensions?
- What about infinite base fields?

If answer is no:

- Same questions as above, plus. . .
- Does the answer depend on q?
- Anything special about C and D?

Minimal isomorphism extensions.

Definition

- Let C and D be curves over a field K.
- Let L be a finite extension of K.
- L is a minimal isomorphism extension for C and D if
  - C and D become isomorphic to one another over L,
  - but not over any proper subextension of L/K.

So our original question is:

Question

Do there exist curves C and D over $\mathbb{F}_q$ for which both $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$ are minimal isomorphism extensions?

Answering a different question.

Theorem

Given

- *an arbitrary prime field* K_0 *and*
- *integers* $r > 1$ *and* $s > 1$ *with* $\gcd(r, s) = 1$,

there exist

- *a finite extension* K *of* K_0 *and*
- *two curves* C *and* D *over* K

such that C *and* D *have minimal isomorphism extensions of degrees* r *and* s *over* K.

How to approach these questions.

- Relate the questions to Galois cohomology.
- Turn the cohomology questions into group theory.
- For existence results, make simplifying assumptions!

Galois cohomology – an especially easy case.

Notation and assumptions

- K is a field, $\overline{K}$ its separable closure, $G_K = \mathrm{Gal}(\overline{K}/K)$.
- A is a torsion group on which G_K acts continuously.
- Suppose $G_K \cong \widehat{\mathbb{Z}}$, with topological generator φ.
  - Examples: $K = \mathbb{F}_q$ or $K = \mathbb{C}((t))$.

Definitions

- A cocycle is an element of A.
- Cocycles x_1 and x_2 are cohomologous if $x_2 = y^{-1}x_1y^{\varphi}$ for some $y \in A$.
- $H^1(G_K, A)$ = cohomology classes of cocycles.
- This is a set, with a distinguished element: $[\mathrm{Id}_A]$.
- *Not a group*, unless A is abelian.

Twists and cohomology, with same assumptions on K.

Suppose X is a curve over K, viewed as scheme over $\operatorname{Spec} K$.

If L is an extension of K, set $X_L = X \times_{\operatorname{Spec} K} \operatorname{Spec} L$.

Fundamental facts

- Have bijection: $\left\{\overline{K}\text{-twists of } X\right\}/\cong \longleftrightarrow H^1(G_K, \operatorname{Aut} X_{\overline{K}})$
- *Restriction map*: $H^1(G_K, \operatorname{Aut} X_{\overline{K}}) \longrightarrow H^1(G_L, \operatorname{Aut} X_{\overline{K}})$
  - Suppose L/K separable, degree n.
  - Class of cocycle x goes to class of $xx^{\varphi} \cdots x^{\varphi^{n-1}}$.
- We have

$$\begin{array}{ccc} \left\{\overline{K}\text{-twists of } X\right\}/\cong & \longleftrightarrow & H^1(G_K, \operatorname{Aut} X_{\overline{K}}) \\ \downarrow \text{natural} & & \downarrow \text{restriction} \\ \left\{\overline{K}\text{-twists of } X_L\right\}/\cong & \longleftrightarrow & H^1(G_L, \operatorname{Aut} X_{\overline{K}}) \end{array}$$

The innocent question (cohomological version).

Question

Let $K = \mathbb{F}_q$, and let C be a curve over K.

Suppose an element of $H^1(G_K, \operatorname{Aut} C_{\overline{K}})$ becomes trivial in $H^1(G_{\mathbb{F}_{q^2}}, \operatorname{Aut} C_{\overline{K}})$ and in $H^1(G_{\mathbb{F}_{q^3}}, \operatorname{Aut} C_{\overline{K}})$.

Must it be trivial in $H^1(G_K, \operatorname{Aut} C_{\overline{K}})$?

For theorem: Put C and D on equal footing.

Let $r > 1$ and $s > 1$ be two integers with $\gcd(r, s) = 1$.

Goal:

Find a curve X over $\mathbb{F}_q$ and $x, y \in H^1(G_{\mathbb{F}_q}, \operatorname{Aut} X_{\overline{K}})$ such that

- x and y have the same restrictions to $H^1(G_{\mathbb{F}_{q^r}}, \operatorname{Aut} X_{\overline{K}})$ and to $H^1(G_{\mathbb{F}_{q^s}}, \operatorname{Aut} X_{\overline{K}})$, but
- x and y have different restrictions to $H^1(G_{\mathbb{F}_{q^t}}, \operatorname{Aut} X_{\overline{K}})$ for every proper divisor t of r or of s.

To prove our theorem (for finite fields), we want to do this in every positive characteristic.

Simplifying assumption: Trivial Galois action.

Life is much simpler when G_K acts trivially.

- $H^1(G_K, A) = \{\text{conjugacy classes of } A\}$.
- restriction : $H^1(G_{\mathbb{F}_q}, A) \to H^1(G_{\mathbb{F}_{q^n}}, A)$ is $[x] \mapsto [x^n]$.

New goal:

- Find a group A that has two elements x and y such that
  - x^r is conjugate to y^r;
  - x^s is conjugate to y^s;
  - x^t is not conjugate to y^t for all proper divisors t of r and s.
- Find curve in characteristic p with automorphism group A.
- Extend the base field until $G_{\mathbb{F}_q}$ acts trivially on A.

Nonconstructive solution.

1. Find a group A that has two elements x and y such that
   - x^r is conjugate to y^r;
   - x^s is conjugate to y^s;
   - x^t is not conjugate to y^t for all proper divisors t of r and s.
2. Find curve in characteristic p with automorphism group A.
3. Extend the base field until $G_{\mathbb{F}_q}$ acts trivially on A.

1. Take r odd. $A = D_{4rs} = \langle u, v : u^{2rs} = v^2 = 1, vuv = u^{-1} \rangle$. Take $m \equiv 1 \bmod r$, $m \equiv -1 \bmod 2s$. Set $x = u$, $y = u^m$.
2. Madden and Valentini: Every group occurs as automorphism group of some curve over $\overline{\mathbb{F}}_p$.
3. No control over genus or the extension of $\mathbb{F}_p$ we will need.

More constructive solution.

1. Find a group A that has two elements x and y such that
   - x^r is conjugate to y^r;
   - x^s is conjugate to y^s;
   - x^t is not conjugate to y^t for all proper divisors t of r and s.
2. Find curve in characteristic p with automorphism group A.
3. Extend the base field until $G_{\mathbb{F}_q}$ acts trivially on A.

1. Find integer n that is
   - coprime to characteristic,
   - divisible by at least two odd primes,
   - divisible by a prime $\equiv 1 \bmod 2rs$.

   Take $A = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$. There are good x and y in A.
2. Goldstein and Guralnick: $X(n)$ has automorphism group A.
3. Can take $q = p^2$. Genus is at least $(2rs)^3$.

Very explicit constructions.

Very explicit examples in characteristic p:

- When p does not divide rs.
- When $r = p$ and p does not divide s.

These examples prove theorem in characteristic 0.

For instance:

If K is a field that

- is a finite extension of its prime field,
- has characteristic not dividing $2rs$,
- contains the $4rs$-th roots of unity,

then we can take C and D to be twists of $y^2 = x^{2rs} + 1$.

Original question and some followups.

When $r = 2$ and $s = 3$, are there examples for every q?

- If q is not a power of 3, examples of genus 2.
- If $q = 3^{\text{odd}}$, examples of genus 1.
- If $q = 3^{\text{even}}$, use twists of $X(65)$. Genus is 9913!

Anything special about C and D?

If K is finite, we can show that the geometric automorphism groups of C and $D\ldots$

- are non-abelian;
- have order divisible by rs;
- have order greater than rs.

Two of many open questions.

Specifying all the fields.

Given a field K and two (linearly disjoint?) finite extensions L and M of K:

Do there exist curves C and D over K having L and M as minimal isomorphism extensions?

Specifying an automorphism group over a finite field.

Given

- a finite field $\mathbb{F}_q$,
- a finite group A, and
- an automorphism φ of A,

does there exists a curve over $\mathbb{F}_q$ with geometric automorphism group A, on which Frobenius acts like φ?