ManinFest (Algebra, Geometry and Physics: a mathematical mosaic)

Non-isogenous elliptic curves and hyperelliptic jacobians

Yuri Zarhin (Penn State/MPIM)

Non-isogenous AV

Non-isogenous AV

A vague question:

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

find an easy "purely algebraic" way (under natural additional conditions) to decide whether they are **non**-isogenous ($X \not\sim Y$).

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

find an easy "purely algebraic" way (under natural additional conditions) to decide whether they are **non**-isogenous ($X \not\sim Y$).

We deal with hyperelliptic jacobians $X = J(C_f), Y = J(C_h)$, where

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

find an easy "purely algebraic" way (under natural additional conditions) to decide whether they are **non**-isogenous ($X \not\sim Y$).

We deal with hyperelliptic jacobians $X = J(C_f), Y = J(C_h)$, where

- $f(x), h(x)$ are polynomials of the same degree $n \geq 3$ without repeated roots;

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

find an easy "purely algebraic" way (under natural additional conditions) to decide whether they are **non**-isogenous ($X \not\sim Y$).

We deal with hyperelliptic jacobians $X = J(C_f), Y = J(C_h)$, where

- $f(x), h(x)$ are polynomials of the same degree $n \geq 3$ without repeated roots;
- C_f and C_h are smooth projective models of plane affine curves $y^2 = f(x)$, $y^2 = h(x)$, respectively.

Non-isogenous AV

A vague question: Given two abelian varieties X, Y of the same dimension over an algebraically closed field,

find an easy "purely algebraic" way (under natural additional conditions) to decide whether they are **non**-isogenous ($X \not\sim Y$).

We deal with hyperelliptic jacobians $X = J(C_f), Y = J(C_h)$, where

- $f(x), h(x)$ are polynomials of the same degree $n \geq 3$ without repeated roots;
- C_f and C_h are smooth projective models of plane affine curves $y^2 = f(x),\ y^2 = h(x)$, respectively.

Wanted: easy to check conditions on f and h that give:

$$J(C_f) \not\sim J(C_h).$$

Elliptic curves

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always:

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always: Counterexample:

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always: Counterexample: $K = \mathbb{Q}$:

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always: Counterexample: $K = \mathbb{Q}$:
$f(x) = x^3 - 2$ **irreducible**,

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always: Counterexample: $K = \mathbb{Q}$:
$f(x) = x^3 - 2$ **irreducible**, $h(x) = x^3 - 1$ **reducible**.

Elliptic curves

$f(x), h(x) \in \mathbb{C}[x]$ are two cubic polynomials.
When $C_f \not\sim C_h$?

Guess: The polynomials should be **very different** (?).

Example: Assume that there is a subfield $K \subset \mathbb{C}$ such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K, $h(x)$ is reducible over K.

May be, then $C_f \not\sim C_h$?

Not always: Counterexample: $K = \mathbb{Q}$:
$f(x) = x^3 - 2$ **irreducible**, $h(x) = x^3 - 1$ **reducible**. Curves $C_f : y^2 = x^3 - 2$ and $C_h : y^2 = x^3 - 1$ are even **isomorphic** over $\mathbb{C}$.

It's essentially **the only** counterexample.

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

If the elliptic curves C_f and C_h are isogenous then they both are isogenous to $y^2 = x^3 - 1$.

Idea of proof

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

If the elliptic curves C_f and C_h are isogenous then they both are isogenous to $y^2 = x^3 - 1$.

Idea of proof Isogeny exists $\overset{Assumptions}{\Longrightarrow}$

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

If the elliptic curves C_f and C_h are isogenous then they both are isogenous to $y^2 = x^3 - 1$.

Idea of proof Isogeny exists $\overset{Assumptions}{\Longrightarrow}$
$\exists$ isogeny ϕ **not defined** over K $\overset{Galois}{\Longrightarrow}$

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

If the elliptic curves C_f and C_h are isogenous then they both are isogenous to $y^2 = x^3 - 1$.

Idea of proof Isogeny exists $\overset{Assumptions}{\Longrightarrow}$
$\exists$ isogeny ϕ **not defined** over K $\overset{Galois}{\Longrightarrow}$
$\exists$ another isogeny $\psi : C_f \to C_h$ that is a **Galois conjugate** of ϕ such that $\phi = c \circ \psi$, where $c \in \mathrm{End}^0(C_h)^*$ has order 3

It's essentially **the only** counterexample. Namely,

Proposition 1 (Z, 2021).

Let f, h, K be such that

A: $f(x), h(x) \in K[x]$;

B: $f(x)$ is irreducible over K,
$h(x)$ is reducible over K.

If the elliptic curves C_f and C_h are isogenous then they both are isogenous to $y^2 = x^3 - 1$.

Idea of proof Isogeny exists $\overset{Assumptions}{\Longrightarrow}$
$\exists$ isogeny ϕ **not defined** over K $\overset{Galois}{\Longrightarrow}$
$\exists$ another isogeny $\psi : C_f \to C_h$ that is a **Galois conjugate** of ϕ such that $\phi = c \circ \psi$, where $c \in \mathrm{End}^0(C_h)^*$ has order 3 $\Longrightarrow$
$\mathrm{End}^0(C_h) \supset \mathbb{Q}(c) \cong \mathbb{Q}(\sqrt{-3})$.

When irreducible polynomials are very different?

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark.

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark. Since both f, h are cubic, we may assume that $\mathrm{Gal}(f/K) = \mathbf{S}_3,\ \mathrm{Gal}(h/K) = \mathbf{A}_3$.

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark. Since both f, h are cubic, we may assume that $\mathrm{Gal}(f/K) = \mathbf{S}_3,\ \mathrm{Gal}(h/K) = \mathbf{A}_3$.

Proposition 3, (Z, 2021).

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark. Since both f, h are cubic, we may assume that $\mathrm{Gal}(f/K) = \mathbf{S}_3$, $\mathrm{Gal}(h/K) = \mathbf{A}_3$.

Proposition 3, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with both Galois groups $\cong \mathbf{S}_3$.

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark. Since both f, h are cubic, we may assume that $\mathrm{Gal}(f/K) = \mathbf{S}_3$, $\mathrm{Gal}(h/K) = \mathbf{A}_3$.

Proposition 3, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with both Galois groups $\cong \mathbf{S}_3$.
If the splitting fields of $f(x)$ and $h(x)$ are linearly disjoint over K

When irreducible polynomials are very different?

Proposition 2, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with **non-isomorphic** Galois groups.

Then $C_f \not\sim C_h$.

Remark. Since both f, h are cubic, we may assume that $\mathrm{Gal}(f/K) = \mathbf{S}_3$, $\mathrm{Gal}(h/K) = \mathbf{A}_3$.

Proposition 3, (Z, 2021).

Let $f, h, K \subset \mathbb{C}$ be such that both $f(x), h(x) \in K[x]$ are irreducible cubic polynomials with both Galois groups $\cong \mathbf{S}_3$.
If the splitting fields of $f(x)$ and $h(x)$ are linearly disjoint over K then

$$C_f \not\sim C_h.$$

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$,

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x - 2)(x^2 + 2x - 11)$

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2+2x-11)$ reducible;
- C_f is isomorphic to C_g;

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2+2x-11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :
  $\mathrm{End}(C_f) = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathrm{End}(C_h) = \mathbb{Z}[\sqrt{-3}]$ (see Silverman's book "Advanced topics on Ell. Curves");

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :
  $\mathrm{End}(C_f) = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathrm{End}(C_h) = \mathbb{Z}[\sqrt{-3}]$ (see Silverman's book "Advanced topics on Ell. Curves");

By Prop. 1, either $C_f \not\sim C_h$ or $C_f \sim C_h \sim C_g$

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :
  $\mathrm{End}(C_f) = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathrm{End}(C_h) = \mathbb{Z}[\sqrt{-3}]$ (see Silverman's book "Advanced topics on Ell. Curves");

By Prop. 1, either $C_f \not\sim C_h$ or $C_f \sim C_h \sim C_g$

The latter is true, because

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2+2x-11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :
  $\mathrm{End}(C_f) = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathrm{End}(C_h) = \mathbb{Z}[\sqrt{-3}]$ (see Silverman's book "Advanced topics on Ell. Curves");

By Prop. 1, either $C_f \not\sim C_h$ or $C_f \sim C_h \sim C_g$

The latter is true, because the End. Algebras are the same:
$\mathrm{End}^0(C_h) = \mathrm{End}(C_h) \otimes \mathbb{Q} = \mathrm{End}^0(C_f) = \mathrm{End}(C_f) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-3})$.

Elliptic curves: examples

Example 1. $K = \mathbb{Q}$,

- $g(x) = x^3 - 1$;
- $f(x) = x^3 - 2$, irreducible with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$;
- $h(x) = x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ reducible;
- C_f is isomorphic to C_g;
- C_f is not isomorphic to C_h :
  the Endomorphisms Rings are different :
  $\mathrm{End}(C_f) = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathrm{End}(C_h) = \mathbb{Z}[\sqrt{-3}]$ (see Silverman's book "Advanced topics on Ell. Curves");

By Prop. 1, either $C_f \not\sim C_h$ or $C_f \sim C_h \sim C_g$

The latter is true, because the End. Algebras are the same:
$\mathrm{End}^0(C_h) = \mathrm{End}(C_h) \otimes \mathbb{Q} = \mathrm{End}^0(C_f) = \mathrm{End}(C_f) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-3})$.

Example 2.

Example 2. $K = \mathbb{Q}, \ a \in \mathbb{Z},$

Example 2. $K = \mathbb{Q}, \ \ a \in \mathbb{Z},$

$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x].$

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).
- By Prop. 2, if $f(x) \in \mathbb{Q}[x]$ is any cubic irreducible polynomial with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).
- By Prop. 2, if $f(x) \in \mathbb{Q}[x]$ is any cubic irreducible polynomial with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$ then $C_f \not\sim C_{h_a}$.

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).
- By Prop. 2, if $f(x) \in \mathbb{Q}[x]$ is any cubic irreducible polynomial with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$ then $C_f \not\sim C_{h_a}$.
- In particular, one may take $f(x) = x^3 - 2$ or $x^3 - x - 1$

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).
- By Prop. 2, if $f(x) \in \mathbb{Q}[x]$ is any cubic irreducible polynomial with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$ then $C_f \not\sim C_{h_a}$.
- In particular, one may take $f(x) = x^3 - 2$ or $x^3 - x - 1$
- Since C_{h_a} is **not** isogenous to $y^2 = x^3 - 2$, it is **not** isogenous to $y^2 = x^3 - 1$ as well.

Example 2. $K = \mathbb{Q}$, $a \in \mathbb{Z}$,
$h_a(x) = x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x]$.

- $h_a(x)$ is irreducible and $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$ (D. Shanks, 1974).
- By Prop. 2, if $f(x) \in \mathbb{Q}[x]$ is any cubic irreducible polynomial with $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$ then $C_f \not\sim C_{h_a}$.
- In particular, one may take $f(x) = x^3 - 2$ or $x^3 - x - 1$
- Since C_{h_a} is **not** isogenous to $y^2 = x^3 - 2$, it is **not** isogenous to $y^2 = x^3 - 1$ as well.
- By Prop. 1, $C_{h_a} \not\sim C_u$ for any cubic reducible polynomial $u(x) \in \mathbb{Q}[x]$ without repeated roots.

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that 2 mod n is a primitive root.

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \ldots,\ n = 3, 5, 11, 13, 19, 29, \ldots.$)

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \ldots,\ n = 3, 5, 11, 13, 19, 29, \ldots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \ldots,\ n = 3, 5, 11, 13, 19, 29, \ldots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;
- $\bar{K}$ - an algebraic closure of K;

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \dots,\ n = 3, 5, 11, 13, 19, 29, \dots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;
- $\bar{K}$ - an algebraic closure of K;
- $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ - the absolute Galois group of K.

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that 2 mod n is a primitive root. (E.g., $g = 1, 2, 5, 6, 9, 14, \ldots,\ n = 3, 5, 11, 13, 19, 29, \ldots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;
- $\bar{K}$ - an algebraic closure of K;
- $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ - the absolute Galois group of K.
- $f(x), h(x) \in K[x]$ - degree n polynomials without repeated roots.

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \dots,\ n = 3, 5, 11, 13, 19, 29, \dots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;
- $\bar{K}$ - an algebraic closure of K;
- $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ - the absolute Galois group of K.
- $f(x), h(x) \in K[x]$ - degree n polynomials without repeated roots.
- $\mathcal{R}_f, \mathcal{R}_h \subset \bar{K}$ - the n-element sets of roots of $f(x)$ and $h(x)$ respectively.
- $K(\mathcal{R}_f)$ and $K(\mathcal{R}_h)$ - the splitting fields of $f(x)$ and $h(x)$ respectively.

Generalizations. Data/Notation

- $n = 2g + 1$ - an **odd prime** such that
  2 mod n is a primitive root.
  (E.g., $g = 1, 2, 5, 6, 9, 14, \ldots,\ n = 3, 5, 11, 13, 19, 29, \ldots.$)
- K - a field with $\mathrm{char}(K) \neq 2$;
- $\bar{K}$ - an algebraic closure of K;
- $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ - the absolute Galois group of K.
- $f(x), h(x) \in K[x]$ - degree n polynomials without repeated roots.
- $\mathcal{R}_f, \mathcal{R}_h \subset \bar{K}$ - the n-element sets of roots of $f(x)$ and $h(x)$ respectively.
- $K(\mathcal{R}_f)$ and $K(\mathcal{R}_h)$ - the splitting fields of $f(x)$ and $h(x)$ respectively.

Notation:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - primitive root $f(x), h(x) \in K[x]$ - degree n polynomials no repeated roots.

Notation:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - primitive root $f(x), h(x) \in K[x]$ - degree n polynomials no repeated roots.

- $\mathsf{Gal}(f/K) = \mathsf{Gal}(K(\mathcal{R}_f)/K) \subset \mathrm{Perm}(\mathcal{R}_f)$

Notation:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - primitive root $f(x), h(x) \in K[x]$ - degree n polynomials no repeated roots.

- $\mathrm{Gal}(f/K) = \mathrm{Gal}(K(\mathcal{R}_f)/K) \subset \mathrm{Perm}(\mathcal{R}_f)$
  $\mathrm{Gal}(h/K) = \mathrm{Gal}(K\mathcal{R}_h)/K) \subset \mathrm{Perm}(\mathcal{R}_h)$ -
  the Galois groups of $f(x)$ and $h(x)$ viewed as permutation groups.

Notation:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - primitive root $f(x), h(x) \in K[x]$ - degree n polynomials no repeated roots.

- $\mathrm{Gal}(f/K) = \mathrm{Gal}(K(\mathcal{R}_f)/K) \subset \mathrm{Perm}(\mathcal{R}_f)$
  $\mathrm{Gal}(h/K) = \mathrm{Gal}(K\mathcal{R}_h)/K) \subset \mathrm{Perm}(\mathcal{R}_h)$ -
  the Galois groups of $f(x)$ and $h(x)$ viewed as permutation groups.
- The hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ are g-dimensional abelian varieties over K.

Notation:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - primitive root $f(x), h(x) \in K[x]$ - degree n polynomials no repeated roots.

- $\mathrm{Gal}(f/K) = \mathrm{Gal}(K(\mathcal{R}_f)/K) \subset \mathrm{Perm}(\mathcal{R}_f)$
  $\mathrm{Gal}(h/K) = \mathrm{Gal}(K\mathcal{R}_h)/K) \subset \mathrm{Perm}(\mathcal{R}_h)$ -
  the Galois groups of $f(x)$ and $h(x)$ viewed as permutation groups.
- The hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ are g-dimensional abelian varieties over K.

We are interested in their endomorphisms, homomorphisms, isogenies that are defined over $\bar{K}$.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.
Then either $J(C_f) \not\sim J(C_h)$

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.
Then either $J(C_f) \not\sim J(C_h)$ or they both are abelian varieties of CM type over $\bar{K}$

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.
Then either $J(C_f) \not\sim J(C_h)$ or they both are abelian varieties of CM type over $\bar{K}$ with multiplication by the nth cyclotomic field $\mathbb{Q}(\sqrt[n]{1})$.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.
Then either $J(C_f) \not\sim J(C_h)$ or they both are abelian varieties of CM type over $\bar{K}$ with multiplication by the nth cyclotomic field $\mathbb{Q}(\sqrt[n]{1})$.

Remark Proposition 1 is the case $n = 3$ of Theorem 1.

Generalizations:

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim.root, $f(x), h(x) \in K[x]$ - deg.n polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

From elliptic curves to hyperelliptic jacobians of arbitrary dimensions;
from $\mathbb{C}$ to fields of arbitrary characteristic $\neq 2$.

Theorem 1 (Z, 2021)

Let $f(x)$ be irreducible over K and $h(x)$ reducible over K.
Then either $J(C_f) \not\sim J(C_h)$ or they both are abelian varieties of CM type over $\bar{K}$ with multiplication by the nth cyclotomic field $\mathbb{Q}(\sqrt[n]{1})$.

Remark Proposition 1 is the case $n = 3$ of Theorem 1.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial, $h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),
It is known (Z, 2000) that $J(C_f)$ is absolutely simple and $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),
It is known (Z, 2000) that $J(C_f)$ is absolutely simple and $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$. Thus it is **not** of CM type.

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),
It is known (Z, 2000) that $J(C_f)$ is absolutely simple and $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$. Thus it is **not** of CM type.

Take any $h(x)$, reducible over $\mathbb{Q}$, same degree, no repeated roots

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),
It is known (Z, 2000) that $J(C_f)$ is absolutely simple and $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$. Thus it is **not** of CM type.

Take any $h(x)$, reducible over $\mathbb{Q}$, same degree, no repeated roots (e.g., $h(x) = x^n - 1$).
By Theorem 1,

$$J(C_f) \not\sim J(C_h).$$

Hyperelliptic jacobians: $K = \mathbb{Q}$

Example 1. $f(x) = x^n - 2$ - irreducible polynomial,
$h(x) = x^n - 1$ - a reducible polynomial.
The hyperelliptic curves C_f and C_h are isomorphic over $\bar{\mathbb{Q}}$. $\Longrightarrow$ $J(C_f)$ and $J(C_h)$ are isomorphic over $\bar{\mathbb{Q}}$ abelian varieties of CM type over $\bar{\mathbb{Q}}$ with multiplication by $\mathbb{Q}(\sqrt[n]{1})$.

Example 2. $f(x) = x^n - x - x - 1$ is an irreducible, with doubly transitive $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_n$ (E.S. Selmer 1956, Nart/Vila 1979, H. Osada 1987),
It is known (Z, 2000) that $J(C_f)$ is absolutely simple and $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$. Thus it is **not** of CM type.

Take any $h(x)$, reducible over $\mathbb{Q}$, same degree, no repeated roots (e.g., $h(x) = x^n - 1$).
By Theorem 1,

$$J(C_f) \not\sim J(C_h).$$

Theorem 2 (Z, 2021)

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$)

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$) or the following hold.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$) or the following hold.

(i) $p = \mathrm{char}(K) > 0$ and $p \not\equiv 1 \bmod n$.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$) or the following hold.

(i) $p = \mathrm{char}(K) > 0$ and $p \not\equiv 1 \mod n$.

(ii) Both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$) or the following hold.

(i) $p = \mathrm{char}(K) > 0$ and $p \not\equiv 1 \mod n$.

(ii) Both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.

Reminder: AV is **supersingular** if it is isogenuos to E^n, where E is an elliptic curve s.t. $\mathrm{End}^0(C)$ is a quaternion $\mathbb{Q}-$algebra.

Theorem 2 (Z, 2021)

Suppose that $\mathrm{char}(K) \neq 2$ and

- $f(x), h(x) \in K[x]$ - degree n polynomials, no repeated roots;
- $n = 2g + 1$ is odd prime, 2 mod n - primitive root;
- both $f(x)$ and $h(x)$ are irreducible over K;
- their splitting fields are linearly disjoint over K.
- $\mathrm{Gal}(f)$ is doubly transitive.

Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0, \ \mathrm{Hom}(J(C_h), J(C_f)) = 0$ (and $J(C_f) \not\sim J(C_h)$) or the following hold.

(i) $p = \mathrm{char}(K) > 0$ and $p \not\equiv 1 \mod n$.

(ii) Both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.

Reminder: AV is **supersingular** if it is isogenuos to E^n, where E is an elliptic curve s.t. $\mathrm{End}^0(C)$ is a quaternion $\mathbb{Q}-$algebra.

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that $2 \mod n$ is a primitive root,

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that $2 \mod n$ is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that $2 \mod n$ is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K.

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that $2 \bmod\ n$ is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K.
  (It remains true even if $\mathrm{Gal}(f/K)$ is just doubly transitive.)

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K. (It remains true even if $\mathrm{Gal}(f/K)$ is just doubly transitive.)

By Theorem 2, $J(C_f) \not\sim J(C_h)$.

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that $2 \bmod n$ is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K. (It remains true even if $\mathrm{Gal}(f/K)$ is just doubly transitive.)

By Theorem 2, $J(C_f) \not\sim J(C_h)$.

E.g., take $K = \mathbb{Q}, g = 2, n = 5$, $f(x) = x^5 - x - 1$ (with $\mathrm{Gal}(f/K) = \mathbf{S}_5$)

Remark Propositions 2 and 3 correspond to the case $n = 3$.

Example 3. Take any $K, \mathrm{char}(K) = 0$,

$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,

$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,

$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.

Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K. (It remains true even if $\mathrm{Gal}(f/K)$ is just doubly transitive.)

By Theorem 2, $J(C_f) \not\sim J(C_h)$.

E.g., take $K = \mathbb{Q}, g = 2, n = 5$, $f(x) = x^5 - x - 1$ (with $\mathrm{Gal}(f/K) = \mathbf{S}_5$) and $h(x) = x^5 - 110x^3 - 55x^2 + 2310x + 979$ (with $\mathrm{Gal}(h/K) = \mathbb{Z}/5\mathbb{Z}$, D.S. Dummit, 1991).

Remark Propositions 2 and 3 correspond to the case $n = 3$.
Example 3. Take any $K, \mathrm{char}(K) = 0$,
$n = 2g + 1$ - an odd prime such that 2 mod n is a primitive root,
$f(x) \in K[x]$ - an irr. pol. with doubly transitive $\mathrm{Gal}(f/K) = \mathbf{S}_n$,
$h(x) \in K[x]$ an irr. pol.with cyclic $\mathrm{Gal}(h/K) = \mathbb{Z}/n\mathbb{Z}$.
Then:

- $\mathrm{Gal}(f/K) = \mathbf{S}_n$ has **no normal subgroups** of index n $\Longrightarrow$
- $\mathrm{Gal}(h/K)$ is **not** isomorphic to a quotient of $\mathrm{Gal}(f/K)$ $\Longrightarrow$
- $K(\mathcal{R}_f) \cap K(\mathcal{R}_h) = K \quad (\text{in } \bar{K})$ $\Longrightarrow$
- **splitting fields** of $f(x)$ and $h(x)$ are **linearly disjoint** over K. (It remains true even if $\mathrm{Gal}(f/K)$ is just doubly transitive.)

By Theorem 2, $J(C_f) \not\sim J(C_h)$.

E.g., take $K = \mathbb{Q}, g = 2, n = 5$, $f(x) = x^5 - x - 1$ (with $\mathrm{Gal}(f/K) = \mathbf{S}_5$) and $h(x) = x^5 - 110x^3 - 55x^2 + 2310x + 979$ (with $\mathrm{Gal}(h/K) = \mathbb{Z}/5\mathbb{Z}$, D.S. Dummit, 1991).

Main Idea of the proof of Theorem 1.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g + 1.$

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g + 1$. We have:

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g + 1$. We have:

- $\mathrm{Hom}(X, Y)/2 \subset \mathrm{Hom}(X[2], Y[2])$.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g + 1$. We have:

- $\mathrm{Hom}(X, Y)/2 \subset \mathrm{Hom}(X[2], Y[2])$.
- If the Galois module $X[2]$ is **absolutely simple,** and the Galois module $Y[2]$ is **simple**, and the corresponding field extensions are **linearly disjoint**, then $\mathrm{Hom}(X[2], Y[2])$ is simple.

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g+1$. We have:

- $\mathrm{Hom}(X, Y)/2 \subset \mathrm{Hom}(X[2], Y[2])$.
- If the Galois module $X[2]$ is **absolutely simple,** and the Galois module $Y[2]$ is **simple**, and the corresponding field extensions are **linearly disjoint**, then $\mathrm{Hom}(X[2], Y[2])$ is simple.
- Thus either $\mathrm{Hom}(X, Y)/2 = \{0\}$ (i.e., $\mathrm{Hom}(X, Y) = 0$) or $\dim_{\mathbb{F}_2} \mathrm{Hom}(X, Y)/2 = 4g^2$ (i.e., $\mathrm{rk}\,\mathrm{Hom}(X, Y) = 4g^2$).

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g+1$. We have:

- $\mathrm{Hom}(X, Y)/2 \subset \mathrm{Hom}(X[2], Y[2])$.
- If the Galois module $X[2]$ is **absolutely simple,** and the Galois module $Y[2]$ is **simple**, and the corresponding field extensions are **linearly disjoint**, then $\mathrm{Hom}(X[2], Y[2])$ is simple.
- Thus either $\mathrm{Hom}(X, Y)/2 = \{0\}$ (i.e., $\mathrm{Hom}(X, Y) = 0$) or $\dim_{\mathbb{F}_2} \mathrm{Hom}(X, Y)/2 = 4g^2$ (i.e., $\mathrm{rk}\, \mathrm{Hom}(X, Y) = 4g^2$).

The latter can happen **iff** $\mathrm{char}(K) > 0$ and both X and Y are supersingular abelian varieties (Z, 2003).

Main Idea of the proof of Theorem 1. Assumptions of the theorem imply that

- any isogeny $\phi : J(C_f) \to J(C_h)$ is **not** defined over K.
- The Galois action on the isogeny ϕ gives (as a "ratio" of two isogenies) an element in $\mathrm{End}^0(C_h)$ of multiplicative order n.

Main Idea of the proof of Theorem 2. Take $X = C_f, Y = C_g, \dim X = \dim Y = g,\ n = 2g+1$. We have:

- $\mathrm{Hom}(X, Y)/2 \subset \mathrm{Hom}(X[2], Y[2])$.
- If the Galois module $X[2]$ is **absolutely simple,** and the Galois module $Y[2]$ is **simple**, and the corresponding field extensions are **linearly disjoint**, then $\mathrm{Hom}(X[2], Y[2])$ is simple.
- Thus either $\mathrm{Hom}(X, Y)/2 = \{0\}$ (i.e., $\mathrm{Hom}(X, Y) = 0$) or $\dim_{\mathbb{F}_2} \mathrm{Hom}(X, Y)/2 = 4g^2$ (i.e., $\mathrm{rk}\,\mathrm{Hom}(X, Y) = 4g^2$).

The latter can happen **iff** $\mathrm{char}(K) > 0$ and both X and Y are supersingular abelian varieties (Z, 2003).

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,
$X[d]$ - the kernel of multiplication by d in $X(\bar{K})$.

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,
$X[d]$ - the kernel of multiplication by d in $X(\bar{K})$.

Facts

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,
$X[d]$ - the kernel of multiplication by d in $X(\bar{K})$.

Facts

(i) $X[d]$ is a free $\mathbb{Z}/d\mathbb{Z}$-submodule of rank $2g$ and the $\mathrm{Gal}(K)$-submodule of $X(\bar{K})$.

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,
$X[d]$ - the kernel of multiplication by d in $X(\bar{K})$.

Facts

(i) $X[d]$ is a free $\mathbb{Z}/d\mathbb{Z}$-submodule of rank $2g$ and the $\mathrm{Gal}(K)$-submodule of $X(\bar{K})$.

(ii) $K_{d,X} \subset \bar{K}$ - the (sub)field of definition of all points from $X[d]$ is a finite Galois extension of K.

Towards proofs of Theorems 1,2

The main ingredients of the proofs are **Key Lemma**, **Special Case of Theorem 1**, and **Useful Lemma**.

Notation and assumptions

X - an AV of dimension g over a field K, $\mathrm{char}(K) \neq 2$.
d - positive integer that is **not** divisible by $\mathrm{char}(K)$,
$X[d]$ - the kernel of multiplication by d in $X(\bar{K})$.

Facts

(i) $X[d]$ is a free $\mathbb{Z}/d\mathbb{Z}$-submodule of rank $2g$ and the $\mathrm{Gal}(K)$-submodule of $X(\bar{K})$.

(ii) $K_{d,X} \subset \bar{K}$ - the (sub)field of definition of all points from $X[d]$ is a finite Galois extension of K.
$\tilde{G}_{d,X} = \mathrm{Gal}(K_{d,X}/K)$ stands for the Galois group of this extension.

$\dim(X) = g \geq 1 \quad n := 2g + 1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

$\dim(X) = g \geq 1 \quad n := 2g+1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple

$\dim(X) = g \geq 1 \quad n := 2g + 1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

  (a) n is a prime such that

$\dim(X) = g \geq 1 \quad n := 2g+1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

(a) n is a prime such that $2 \bmod n$ is a primitive root;

$\dim(X) = g \geq 1 \quad n := 2g + 1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

   (a) n is a prime such that $2 \bmod n$ is a primitive root;

   (b) $\#(\tilde{G}_{2,X})$ is divisible by n.

$\dim(X) = g \geq 1 \quad n := 2g+1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

  (a) n is a prime such that $2 \bmod n$ is a primitive root;

  (b) $\#(\tilde{G}_{2,X})$ is divisible by n.

(vi) $K_{2,X} \subset K_{4,X}$;

$\dim(X) = g \geq 1 \quad n := 2g + 1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

  (a) n is a prime such that $2 \bmod n$ is a primitive root;

  (b) $\#(\tilde{G}_{2,X})$ is divisible by n.

(vi) $K_{2,X} \subset K_{4,X}$; either the equality holds or $\mathrm{Gal}(K_{4,X}/K_{2,X})$ - **finite commutative group of exponent 2**.

$\dim(X) = g \geq 1 \quad n := 2g + 1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

  (a) n is a prime such that $2 \bmod n$ is a primitive root;

  (b) $\#(\tilde{G}_{2,X})$ is divisible by n.

(vi) $K_{2,X} \subset K_{4,X}$; either the equality holds or $\mathrm{Gal}(K_{4,X}/K_{2,X})$ - **finite commutative group of exponent 2**.

(vii) Our main tool: **all endomorphisms of X are defined over** $K_{4,X}$ (A. Silverberg, 1992).

$\dim(X) = g \geq 1 \quad n := 2g+1$

(iv) $X[2]$ - $2g$-dimensional vector space over $\mathbb{F}_2$.

(v) (P. Goodman, 2021) The $\mathrm{Gal}(K)$-module $X[2]$ is simple if

(a) n is a prime such that $2 \bmod n$ is a primitive root;

(b) $\#(\tilde{G}_{2,X})$ is divisible by n.

(vi) $K_{2,X} \subset K_{4,X}$; either the equality holds or $\mathrm{Gal}(K_{4,X}/K_{2,X})$ - **finite commutative group of exponent 2**.

(vii) Our main tool: **all endomorphisms of X are defined over** $K_{4,X}$ (A. Silverberg, 1992).

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X = J(C_f), Y = J(C_h)$ where $f(x), h(x) \in K[x]$ - odd degree polynomials without repeated roots.

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X = J(C_f), Y = J(C_h)$ where $f(x), h(x) \in K[x]$ - odd degree polynomials without repeated roots. $\Rightarrow$

$K(X[2]) = K(\mathcal{R}_f), \ \tilde{G}_{2,X} = \mathrm{Gal}(f/K);$

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X = J(C_f), Y = J(C_h)$ where $f(x), h(x) \in K[x]$ - odd degree polynomials without repeated roots. $\Rightarrow$

$K(X[2]) = K(\mathcal{R}_f), \ \tilde{G}_{2,X} = \mathrm{Gal}(f/K);$

$K(Y[2]) = K(\mathcal{R}_h), \ \tilde{G}_{2,Y} = \mathrm{Gal}(h/K).$

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X = J(C_f), Y = J(C_h)$ where $f(x), h(x) \in K[x]$ - odd degree polynomials without repeated roots. $\Rightarrow$

$K(X[2]) = K(\mathcal{R}_f),\ \tilde{G}_{2,X} = \mathrm{Gal}(f/K);$

$K(Y[2]) = K(\mathcal{R}_h),\ \tilde{G}_{2,Y} = \mathrm{Gal}(h/K).$

$\Rightarrow K(Y[2]) = K$ **iff** $h(x)$ splits completely over K.

Remark $\mathrm{Gal}(f/K)$ is **doubly transitive**

$X[2]$ and $Y[2]$ for **hyperelliptic jacobians**

$X = J(C_f), Y = J(C_h)$ where $f(x), h(x) \in K[x]$ - odd degree polynomials without repeated roots. $\Rightarrow$

$K(X[2]) = K(\mathcal{R}_f),\ \tilde{G}_{2,X} = \mathrm{Gal}(f/K);$

$K(Y[2]) = K(\mathcal{R}_h),\ \tilde{G}_{2,Y} = \mathrm{Gal}(h/K).$

$\Rightarrow K(Y[2]) = K$ **iff** $h(x)$ splits completely over K.

Remark $\mathrm{Gal}(f/K)$ is **doubly transitive iff** the centralizer of $\tilde{G}_{2,X}$ in $\mathrm{End}_{\mathbb{F}_2}(X[2])$ is $\mathbb{F}_2$ (S. Mori, 1977).

Key Lemma

Key Lemma

Suppose that

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;
- $n = 2g + 1$ is a **prime** such that 2 mod n a **primitive root**;

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;
- $n = 2g + 1$ is a **prime** such that 2 mod n a **primitive root**; X and Y are g-dimensional abelian varieties over K that are **isogenous over $\bar{K}$**;

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;
- $n = 2g + 1$ is a **prime** such that 2 mod n a **primitive root**; X and Y are g-dimensional abelian varieties over K that are **isogenous over** $\bar{K}$;
- $K_{2,Y} = K$ (i.e. all order 2 points on Y are defined over K);

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;
- $n = 2g + 1$ is a **prime** such that 2 mod n a **primitive root**; X and Y are g-dimensional abelian varieties over K that are **isogenous over** $\bar{K}$;
- $K_{2,Y} = K$ (i.e. all order 2 points on Y are defined over K);
- degree $[K_{2,X} : K]$ is divisible by n.

Key Lemma

Suppose that

- $\mathrm{char}(K) \neq 2$;
- $n = 2g + 1$ is a **prime** such that 2 mod n a **primitive root**; X and Y are g-dimensional abelian varieties over K that are **isogenous over $\bar{K}$**;
- $K_{2,Y} = K$ (i.e. all order 2 points on Y are defined over K);
- degree $[K_{2,X} : K]$ is divisible by n.

Then both X and Y are abelian varieties of CM type over $\bar{K}$ with **multiplication by the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.**

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f)$, $Y = J(C_h)$. h splits $\Rightarrow$ $\tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$
$\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$
$\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

$n = \deg(f)$ is a prime $+ f(x)$ irreducible

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$
$\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

$n = \deg(f)$ is a prime + $f(x)$ irreducible $\Rightarrow$ $\#(\mathrm{Gal}(f/K))$ is divisible by n, i.e., $\#(\tilde{G}_{2,X})$ is divisible by n

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$
$\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

$n = \deg(f)$ is a prime + $f(x)$ irreducible $\Rightarrow$ $\#(\mathrm{Gal}(f/K))$ is divisible by n, i.e., $\#(\tilde{G}_{2,X})$ is divisible by n $\overset{Goodman}{\Longrightarrow}$ the $\mathrm{Gal}(K)$-module $X[2]$ is simple.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$ $\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

$n = \deg(f)$ is a prime + $f(x)$ irreducible $\Rightarrow \#(\mathrm{Gal}(f/K))$ is divisible by n, i.e., $\#(\tilde{G}_{2,X})$ is divisible by n $\overset{Goodman}{\Longrightarrow}$ the $\mathrm{Gal}(K)$-module $X[2]$ is simple.

By **Key Lemma**, either $J(C_f) = X \not\sim Y = J(C_h)$ or both $J(C_f)$ and $J(C_h)$ are AV of CM type over $\bar{K}$ with multiplication by $\mathbb{Q}(\zeta_n)$.

Application

$n = \deg(f) = \deg(h)$ - odd prime, 2 mod n - prim. root, $f(x), h(x) \in K[x]$ - polynomials with simple roots, $\mathrm{char}(K) \neq 2$.

Special case of Theorem 1 Assume that $f(x) \in K[x]$ is irreducible, $h(x) \in K[x]$ completely splits. Then either $J(C_f) \not\sim J(C_h)$ or both jacobians are AV of **CM type** over $\bar{K}$ with **multiplication by the** n**th cyclotomic field** $\mathbb{Q}(\zeta_n)$.

Proof $X = J(C_f), Y = J(C_h)$. h splits $\Rightarrow \tilde{G}_{2,Y} = \mathrm{Gal}(h/K) = \{1\}$ $\Rightarrow Y[2] \subset Y(K)$ is the trivial $\mathrm{Gal}(K)$-module.

$n = \deg(f)$ is a prime + $f(x)$ irreducible $\Rightarrow$ $\#(\mathrm{Gal}(f/K))$ is divisible by n, i.e., $\#(\tilde{G}_{2,X})$ is divisible by n $\overset{Goodman}{\Longrightarrow}$ the $\mathrm{Gal}(K)$-module $X[2]$ is simple.

By **Key Lemma**, either $J(C_f) = X \not\sim Y = J(C_h)$ or both $J(C_f)$ and $J(C_h)$ are AV of CM type over $\bar{K}$ with multiplication by $\mathbb{Q}(\zeta_n)$.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g+1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g+1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow$

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow$

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \quad \Longrightarrow$

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$ similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g+1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$ similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \dots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2.

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg).

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g+1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi\,|_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$ similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m\phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg). We prove

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg). We prove

1. There exists $H \subset \mathrm{Gal}(K_{4,X\times Y}/K)$, $H \cong \mathbb{Z}/n\mathbb{Z}$ and a group homomorphism $c : H \to \mathrm{End}^0(Y)^*$ defined by

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg). We prove

1. There exists $H \subset \mathrm{Gal}(K_{4,X\times Y}/K)$, $H \cong \mathbb{Z}/n\mathbb{Z}$ and a group homomorphism $c : H \to \mathrm{End}^0(Y)^*$ defined by $\sigma(\phi) = c(\sigma) \circ \phi$ for all $\sigma \in H$.

Idea of the proof of Key Lemma

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$ similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \dots \quad \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X \times Y}$ (Silverberg). We prove

1. There exists $H \subset \mathrm{Gal}(K_{4,X\times Y}/K)$, $H \cong \mathbb{Z}/n\mathbb{Z}$ and a group homomorphism $c : H \to \mathrm{End}^0(Y)^*$ defined by $\sigma(\phi) = c(\sigma) \circ \phi$ for all $\sigma \in H$.
2. $\forall$ non-trivial $\sigma \in H$,

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$
similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg). We prove

1. There exists $H \subset \mathrm{Gal}(K_{4,X\times Y}/K)$, $H \cong \mathbb{Z}/n\mathbb{Z}$ and a group homomorphism $c : H \to \mathrm{End}^0(Y)^*$ defined by $\sigma(\phi) = c(\sigma) \circ \phi$ for all $\sigma \in H$.
2. $\forall$ non-trivial $\sigma \in H$, $c(\sigma)$ has multiplicative order n $\Longrightarrow$

Idea of the proof of Key Lemma

$\mathrm{char}(K) \neq 2$, $n = 2g + 1$ prime, 2 mod n a primitive root

We have: $X \sim Y$, $K_{2,Y} = K$, $n \mid [K_{2,X} : K]$.
We want : $\mathrm{End}^0(Y) \supset \mathbb{Q}(\zeta_n)$. Let $\phi : X \to Y$ be isogeny.
Case 1. ϕ is defined over K.
By Goodman, $X[2]$ is simple $\Longrightarrow \phi \mid_{X[2]} = 0 \Longrightarrow \phi = 2\phi_1 \Longrightarrow$ similar: $\phi_1 = 2\phi_2, \phi_2 = 2\phi_3 \ldots \Longrightarrow \phi = 2^m \phi_m$ for any m.
$\mathrm{Hom}(X, Y) \cong \mathbb{Z}^r \Longrightarrow \phi = 0$ is **NOT** an isogeny. Contradiction.

Case 2. ϕ is not defined over K but defined over $K_{4,X\times Y}$ (Silverberg). We prove

1. There exists $H \subset \mathrm{Gal}(K_{4,X\times Y}/K)$, $H \cong \mathbb{Z}/n\mathbb{Z}$ and a group homomorphism $c : H \to \mathrm{End}^0(Y)^*$ defined by $\sigma(\phi) = c(\sigma) \circ \phi$ for all $\sigma \in H$.
2. $\forall$ non-trivial $\sigma \in H$, $c(\sigma)$ has multiplicative order $n \Longrightarrow$ $\mathrm{End}^0(Y)$ contains the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\implies [\tilde{K} : K]$ is a power of 2. Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\implies$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^{H}$, we get

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M. $\Longrightarrow$ $\exists$ an L-isogeny $u : X \to Y$ that is **not** defined over M.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2.
Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M. $\Longrightarrow$ $\exists$ an L-isogeny $u : X \to Y$ that is **not** defined over M. $\Longrightarrow$ $\exists \sigma \in \mathrm{Gal}(L/M)$ such that $\sigma u \neq u$.

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2. Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.

Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M. $\Longrightarrow$ $\exists$ an L-isogeny $u : X \to Y$ that is **not** defined over M. $\Longrightarrow$ $\exists \sigma \in \mathrm{Gal}(L/M)$ such that $\sigma u \neq u$.

Then the cocycle $c : \mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(L/M) \to \mathrm{End}_L^0(Y)^*$ defined by $\sigma(u) = c(\sigma)u \ \forall \sigma \in \mathrm{Gal}(L/M)$

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2. Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}_{4,X}^H$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M. $\Longrightarrow$ $\exists$ an L-isogeny $u : X \to Y$ that is **not** defined over M. $\Longrightarrow$ $\exists \sigma \in \mathrm{Gal}(L/M)$ such that $\sigma u \neq u$.

Then the cocycle $c : \mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(L/M) \to \mathrm{End}^0_L(Y)^*$ defined by
$\sigma(u) = c(\sigma)u \ \forall \sigma \in \mathrm{Gal}(L/M)$
is a **nontrivial** group homomorphism

Constructing non-trivial $c : H \to \mathrm{End}^0(Y)^*$

Step 1. Change K to $\tilde{K} = K_{4,Y}$. $\Longrightarrow$ $[\tilde{K} : K]$ is a power of 2. Since n is an odd prime, $n \mid [\tilde{K}_{2,X} : \tilde{K}]$ still holds $\Longrightarrow$ there is a subgroup $H \subset \mathrm{Gal}(\tilde{K}_{4,X}/\tilde{K})$, $H \cong \mathbb{Z}/n\mathbb{Z}$.
Taking $L = \tilde{K}_{4,X}$ and $M = \tilde{K}^H_{4,X}$, we get

- $M_{4,Y} = M$, $\mathrm{Gal}(L/M) \cong \mathbb{Z}/n\mathbb{Z}$ and $M_{2,X} = M_{4,X} = L$;
- all endomorphisms of Y are defined over M;
- all homomorphisns $X \to Y$ are defined over L.

Step 2. The $\mathrm{Gal}(M)$-module $X[2]$ is **simple**, $\mathrm{Gal}(M)$-module $Y[2]$ is **trivial** $\Longrightarrow$ similar to **Case 1** every isogeny $X \to Y$ is **not** defined over M. $\Longrightarrow$ $\exists$ an L-isogeny $u : X \to Y$ that is **not** defined over M. $\Longrightarrow$ $\exists \sigma \in \mathrm{Gal}(L/M)$ such that $\sigma u \neq u$.

Then the cocycle $c : \mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(L/M) \to \mathrm{End}^0_L(Y)^*$ defined by
$\sigma(u) = c(\sigma)u \ \forall \sigma \in \mathrm{Gal}(L/M)$
is a **nontrivial** group homomorphism $\Longrightarrow$ has order n.

Useful Lemma

Lemma, (Z, 2003)

Let X and Y are positive-dimensional abelian varieties over K that enjoys the following properties.

Useful Lemma

Lemma, (Z, 2003)

Let X and Y are positive-dimensional abelian varieties over K that enjoys the following properties.

(i) The $\mathrm{Gal}(K)$-module $X[2]$ is absolutely simple.

Useful Lemma

Lemma, (Z, 2003)

Let X and Y are positive-dimensional abelian varieties over K that enjoys the following properties.

(i) The $\mathrm{Gal}(K)$-module $X[2]$ is absolutely simple.

(ii) The $\mathrm{Gal}(K)$-module $Y[2]$ is simple.

Useful Lemma

Lemma, (Z, 2003)

Let X and Y are positive-dimensional abelian varieties over K that enjoys the following properties.

(i) The $\mathrm{Gal}(K)$-module $X[2]$ is absolutely simple.

(ii) The $\mathrm{Gal}(K)$-module $Y[2]$ is simple.

(iii) The fields $K(X[2])$ and $K(Y[2])$ are linearly disjoint over K.

Useful Lemma

Lemma, (Z, 2003)

Let X and Y are positive-dimensional abelian varieties over K that enjoys the following properties.

(i) The Gal(K)-module $X[2]$ is absolutely simple.

(ii) The Gal(K)-module $Y[2]$ is simple.

(iii) The fields $K(X[2])$ and $K(Y[2])$ are linearly disjoint over K.

Then:

1. The Gal(K)-module $\mathrm{Hom}_{\mathbb{F}_2}(X[2], Y[2])$ is simple.
2. Either
$\mathrm{Hom}(X, Y) = \{0\}, \ \mathrm{Hom}(Y, X) = \{0\}$
or $\mathrm{char}(K) > 0$ and both X and Y are supersingular abelian varieties.