17T7 is a Galois group over the rationals

Edgar Costa (MIT)

December 9, 2024, Auckland
Joint meeting of the AMS, AustMS and NZMS: Computational Number Theory

Slides available at edgarcosta.org
Joint work with:
Raymond van Bommel, Noam Elkies, Timo Keller, Samuel Schiavone, and John Voight

Inverse Galois problem

Question: Inverse Galois problem

Is every finite group a Galois group over $\mathbb{Q}$?

Inverse Galois problem

Question: Inverse Galois problem

Is every finite group a Galois group over $\mathbb{Q}$?

This problem welcomes many variations and insights from many areas of mathematics!

Question: Effective inverse Galois problem

Given $G \leq S_d$ transitive, exhibit $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}(f) \simeq G$.

Inverse Galois problem

Question: Inverse Galois problem

Is every finite group a Galois group over $\mathbb{Q}$?

This problem welcomes many variations and insights from many areas of mathematics!

Question: Effective inverse Galois problem

Given $G \leq S_d$ transitive, exhibit $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}(f) \simeq G$.

The L-functions and Modular Forms Database (www.lmfdb.org) provides a catalogue.

Inverse Galois problem

Question: Inverse Galois problem

Is every finite group a Galois group over $\mathbb{Q}$?

This problem welcomes many variations and insights from many areas of mathematics!

Question: Effective inverse Galois problem

Given $G \leq S_d$ transitive, exhibit $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}(f) \simeq G$.

The L-functions and Modular Forms Database (www.lmfdb.org) provides a catalogue.
This is also nicely organized by Klüners–Malle (galoisdb.math.upb.de).

Two groups where the inverse Galois problem is unknown

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16})$$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathrm{PSL}_2(\mathbb{F}_{16})$$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathsf{PSL}_2(\mathbb{F}_{16}) = \mathsf{PGL}_2(\mathbb{F}_{16})$$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathrm{PSL}_2(\mathbb{F}_{16}) = \mathrm{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathsf{PSL}_2(\mathbb{F}_{16}) = \mathsf{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$
$$\Rightarrow \mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}.$$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathsf{PSL}_2(\mathbb{F}_{16}) = \mathsf{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$
$$\Rightarrow \mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}.$$

We also have $\mathsf{Aut}(\mathbb{F}_{16}) \simeq C_4$ (cyclic of order 4) acting coefficientwise,

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathsf{PSL}_2(\mathbb{F}_{16}) = \mathsf{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$
$$\Rightarrow \mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}.$$

We also have $\mathsf{Aut}(\mathbb{F}_{16}) \simeq C_4$ (cyclic of order 4) acting coefficientwise, compatible with the action on $\mathbb{P}^1(\mathbb{F}_{16})$;

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathsf{PSL}_2(\mathbb{F}_{16}) = \mathsf{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$
$$\Rightarrow \mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}.$$

We also have $\mathsf{Aut}(\mathbb{F}_{16}) \simeq C_4$ (cyclic of order 4) acting coefficientwise, compatible with the action on $\mathbb{P}^1(\mathbb{F}_{16})$; we take the extension by $C_2 \leq C_4$

Two groups where the inverse Galois problem is unknown

Ordering by transitive degree d, the inverse Galois problem is known for all groups $G \leq S_d$ with $d \leq 23$ except for two groups.

The first unknown group 23T5 $\simeq M_{23}$ is the Mathieu group on 23 letters.

The remaining group is 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Observe

$$\mathrm{SL}_2(\mathbb{F}_{16}) = \mathrm{PSL}_2(\mathbb{F}_{16}) = \mathrm{PGL}_2(\mathbb{F}_{16}) \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$$

$$\Rightarrow \mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}.$$

We also have $\mathbf{Aut}(\mathbb{F}_{16}) \simeq C_4$ (cyclic of order 4) acting coefficientwise, compatible with the action on $\mathbb{P}^1(\mathbb{F}_{16})$; we take the extension by $C_2 \leq C_4$

giving

$$1 \to \mathrm{SL}_2(\mathbb{F}_{16}) \to 17T7 \to C_2 \to 1.$$

Main theorem

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

Main theorem

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} - 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Main theorem

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^9 - 886x^8 + 2024x^7 - 604x^6 + 2146x^5 + 80x^4 - 1376x^3 - 496x^2 - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

So far, we have 4 polynomials for 17T7.

Main theorem

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

The polynomial

$$\begin{aligned} f(x) = x^{17} &- 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} \\ &- 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490 \end{aligned}$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

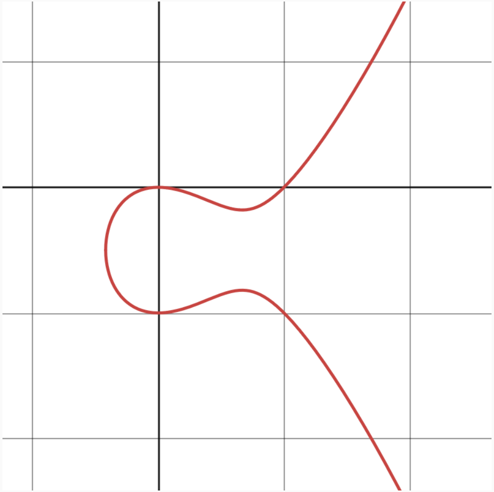
So far, we have 4 polynomials for 17T7.

Question

How does one construct such field?

Matrix Galois groups: from geometry, elliptic curves

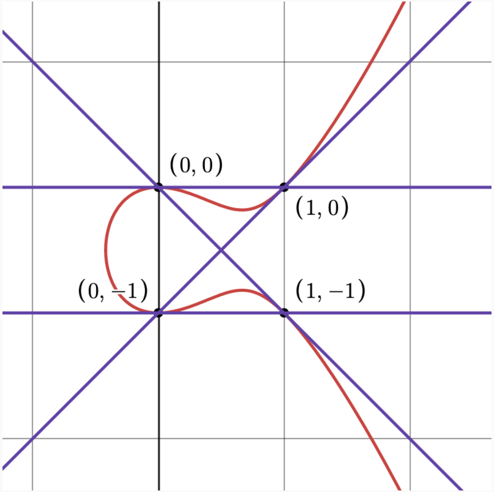
Matrix Galois groups: from geometry, elliptic curves



$$E\colon y^2 + y = x^3 - x^2$$

$$P + Q + R \sim 0$$

Matrix Galois groups: from geometry, elliptic curves



$E\colon y^2 + y = x^3 - x^2$ and $(0,0) \in E[5](\mathbb{Q})$.

$P + Q + R \sim 0$

Elliptic curve torsion

Elliptic curve torsion

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

Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic,

Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$

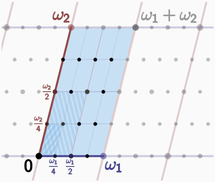
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\text{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\text{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



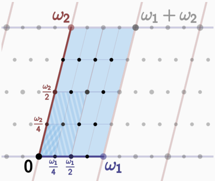
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\text{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\text{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points.

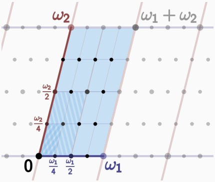
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension

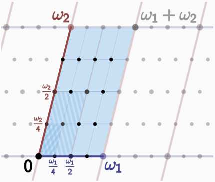
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q})$$

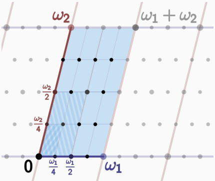
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

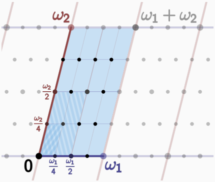
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2 \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

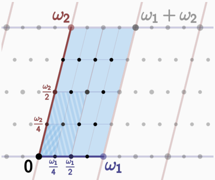
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2 \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For example, for $E\colon y^2 + y = x^3 - x^2$ (11.a3),

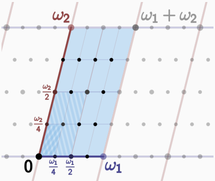
Elliptic curve torsion

Let E be an elliptic curve over $\mathbb{Q}$. For $m \geq 1$, we define the set of *m-torsion points*

$$E[m](\mathbb{Q}^{\mathrm{al}}) := \{P \in E : mP = \infty\}.$$

Since $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and the group law is algebraic, we have

$$E[m](\mathbb{Q}^{\mathrm{al}}) = E[m](\mathbb{C}) \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$



Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2 \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For example, for $E\colon y^2 + y = x^3 - x^2$ (11.a3), the field $\mathbb{Q}(E[5])$ is the splitting field of

$$x^{10} - 3x^9 + 6x^8 + 11x^7 - 29x^6 - 15x^5 - 6x^4 - 55x^3 + 65x^2 + 200x + 100$$

Matrix Galois groups

Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For example, for $E\colon y^2 + y = x^3 - x^2$ (11.a3), the field $\mathbb{Q}(E[5])$ is the splitting field of

$$x^{10} - 3x^9 + 6x^8 + 11x^7 - 29x^6 - 15x^5 - 6x^4 - 55x^3 + 65x^2 + 200x + 100$$

$$\mathrm{Gal}(\mathbb{Q}(E[5]) \,|\, \mathbb{Q}) \not\simeq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

Matrix Galois groups

Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \mid \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For example, for $E\colon y^2 + y = x^3 - x^2$ (11.a3), the field $\mathbb{Q}(E[5])$ is the splitting field of

$$x^{10} - 3x^9 + 6x^8 + 11x^7 - 29x^6 - 15x^5 - 6x^4 - 55x^3 + 65x^2 + 200x + 100$$

$$\mathrm{Gal}(\mathbb{Q}(E[5]) \mid \mathbb{Q}) \not\simeq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \mid \mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}), \quad \text{if } 5 \nmid m$$

Matrix Galois groups

Let $\mathbb{Q}(E[m])$ be the field generated by x and y-coordinates of all m-torsion points. Then $\mathbb{Q}(E[m]) \supseteq \mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \mid \mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[m](\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For example, for $E\colon y^2 + y = x^3 - x^2$ (11.a3), the field $\mathbb{Q}(E[5])$ is the splitting field of

$$x^{10} - 3x^9 + 6x^8 + 11x^7 - 29x^6 - 15x^5 - 6x^4 - 55x^3 + 65x^2 + 200x + 100$$

$$\mathrm{Gal}(\mathbb{Q}(E[5]) \mid \mathbb{Q}) \not\simeq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

and

$$\mathrm{Gal}(\mathbb{Q}(E[m]) \mid \mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}), \quad \text{if } 5 \nmid m$$

Slogan

In number theory, maximal entropy is the norm.

Matrix Galois groups: with endomorphisms

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathrm{End}(E_K)$.

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathbf{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathrm{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathrm{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Thus

$$\mathrm{Gal}(K(E[m]) \mid K)$$

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x,y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathbf{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Thus

$$\mathrm{Gal}(K(E[m]) \,|\, K) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i]/m\mathbb{Z}[i])$$

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathbf{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Thus

$$\mathrm{Gal}(K(E[m]) \mid K) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq \mathrm{GL}_1(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq (\mathbb{Z}[i]/m\mathbb{Z}[i])^{\times}.$$

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x,y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathbf{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Thus

$$\mathrm{Gal}(K(E[m]) \,|\, K) \hookrightarrow \mathbf{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq \mathbf{GL}_1(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq (\mathbb{Z}[i]/m\mathbb{Z}[i])^\times.$$

Indeed, equality holds for $2 \nmid m$.

Matrix Galois groups: with endomorphisms

$$E\colon y^2 = x^3 - x \quad (32.a3)$$

has the additional symmetry $(x, y) \mapsto (-x, iy)$ giving $R = \mathbb{Z}[i] \subset K = \mathbb{Q}(i)$ acting by endomorphisms of E, written $R \hookrightarrow \mathrm{End}(E_K)$. But then we don't just have

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

as a $\mathbb{Z}$-module, but as a $\mathbb{Z}[i]$-module

$$E[m](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{Z}[i]/m\mathbb{Z}[i].$$

Thus

$$\mathrm{Gal}(K(E[m]) \,|\, K) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq \mathrm{GL}_1(\mathbb{Z}[i]/m\mathbb{Z}[i]) \simeq (\mathbb{Z}[i]/m\mathbb{Z}[i])^\times.$$

Indeed, equality holds for $2 \nmid m$.

Slogan

Additional symmetries (endomorphisms) must be respected.

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathsf{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

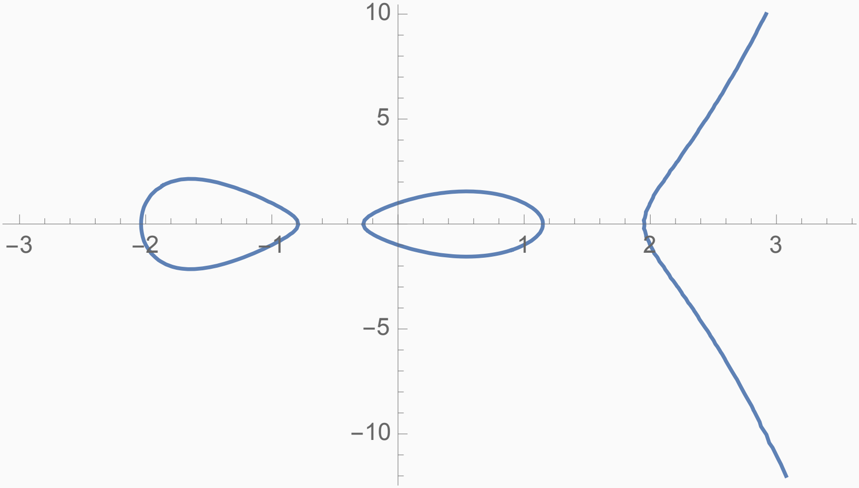
When $g = 1$ and $X = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

$$P + Q + R \sim 0$$

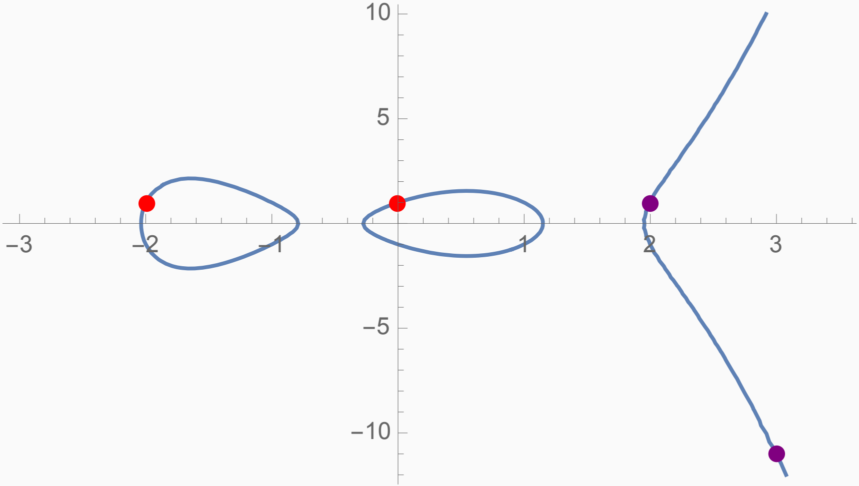
In general, we can think about adding tuples of g-points.

Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$

Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$



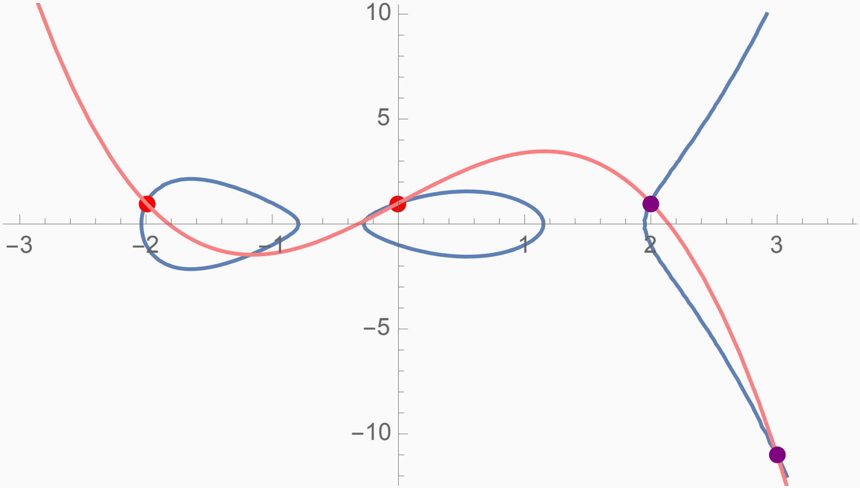
Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$



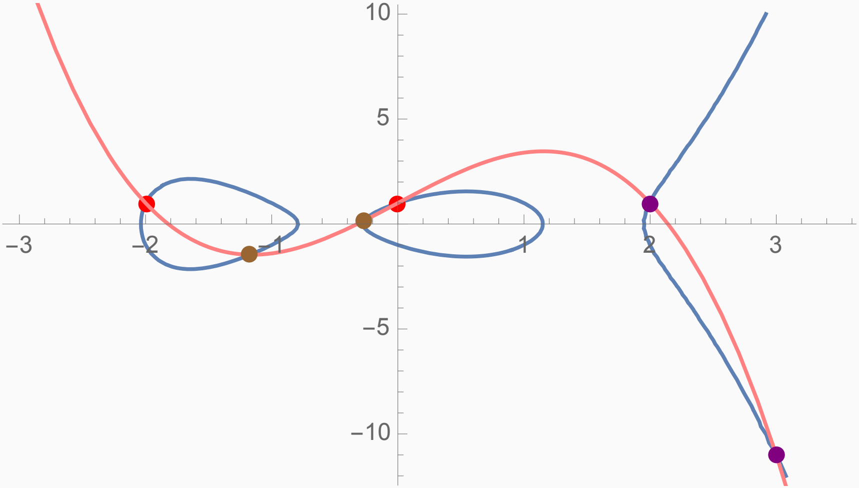
$D_1 := (-2, 1) + (0, 1)$

$D_2 := (2, 1) + (3, -11)$

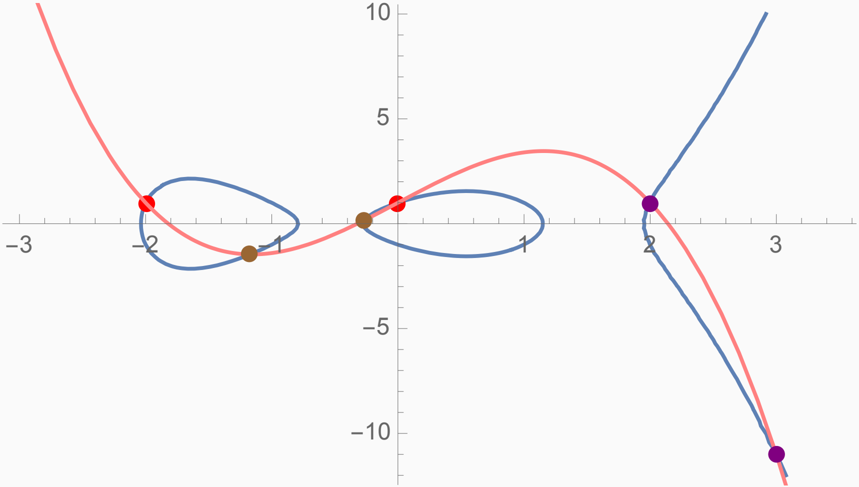
Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$



Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$

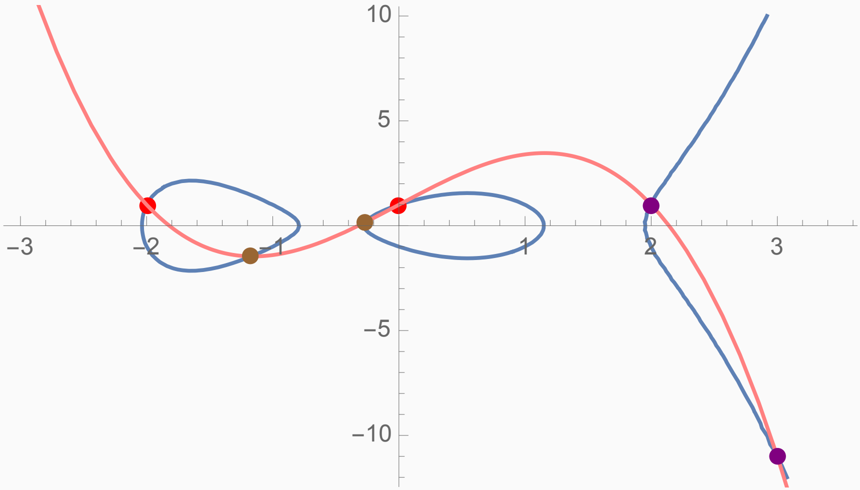


Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$



$$(\textcolor{red}{\bullet} + \textcolor{red}{\bullet}) + (\textcolor{purple}{\bullet} + \textcolor{purple}{\bullet}) + (\textcolor{brown}{\bullet} + \textcolor{brown}{\bullet}) = 0$$

Addition on the Jacobian of a genus 2 curve, e.g, $X : y^2 = x^5 - 5x^3 + 4x + 1$



$$D_3 := \left(\frac{-\sqrt{209}-23}{32}, \frac{-115\sqrt{209}-1333}{2048}\right) + \left(\frac{\sqrt{209}-23}{32}, \frac{115\sqrt{209}-1333}{2048}\right)$$

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

When $g = 1$ and $X = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

$$P + Q + R \sim 0$$

In general, we can think about adding tuples of g-points.

We have $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

When $g = 1$ and $X = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

$$P + Q + R \sim 0$$

In general, we can think about adding tuples of g-points.

We have $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ and again

$$A[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}.$$

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

When $g = 1$ and $X = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

$$P + Q + R \sim 0$$

In general, we can think about adding tuples of g-points.

We have $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ and again

$$A[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}.$$

So

$$\mathrm{Gal}(\mathbb{Q}(A[m]) \,|\, \mathbb{Q}) \hookrightarrow \mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

Jacobians

Let X be a nice (smooth, projective, geometrically integral) curve of genus $g \geq 1$.

Then the group of divisors of degree 0 on X up to linear equivalence is represented by an abelian variety called the *Jacobian* $A := \mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$.

When $g = 1$ and $X = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

$$P + Q + R \sim 0$$

In general, we can think about adding tuples of g-points.

We have $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ and again

$$A[m](\mathbb{Q}^{\mathrm{al}}) \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}.$$

So

$$\mathrm{Gal}(\mathbb{Q}(A[m]) \mid \mathbb{Q}) \hookrightarrow \mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

We can again cut down on the image of Galois by additional endomorphisms.

Galois representation for 17T7

Recall we are trying to get 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$

Galois representation for 17T7

Recall we are trying to get 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

Galois representation for 17T7

Recall we are trying to get $17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

Galois representation for 17T7

Recall we are trying to get $17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathrm{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

Galois representation for 17T7

Recall we are trying to get 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathrm{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

such that over a (real) quadratic field F we acquire endomorphisms:

Galois representation for 17T7

Recall we are trying to get $17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathrm{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

such that over a (real) quadratic field F we acquire endomorphisms:

$$R := \mathrm{End}(A_F) \subseteq K$$

with $[K : \mathbb{Q}] = 4$ and $2R$ *prime*,

Galois representation for 17T7

Recall we are trying to get 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathrm{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

such that over a (real) quadratic field F we acquire endomorphisms:

$$R := \mathrm{End}(A_F) \subseteq K$$

with $[K : \mathbb{Q}] = 4$ and $2R$ *prime*, so

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq (R/2R)^2 \simeq \mathbb{F}_{16}^2.$$

Galois representation for 17T7

Recall we are trying to get $17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathrm{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

such that over a (real) quadratic field F we acquire endomorphisms:

$$R := \mathrm{End}(A_F) \subseteq K$$

with $[K : \mathbb{Q}] = 4$ and $2R$ *prime*, so

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq (R/2R)^2 \simeq \mathbb{F}_{16}^2.$$

Where are we going to find such curve X?

Galois representation for 17T7

Recall we are trying to get 17T7 $\simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{F}_{16}^2$.

As abelian groups, we have $\mathbb{F}_{16}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^8$.

So we look for a curve X over $\mathbb{Q}$ of genus $g = 4$, so for $A = \mathbf{Jac}(X)$ we have

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq \mathbb{F}_2^8;$$

such that over a (real) quadratic field F we acquire endomorphisms:

$$R := \mathbf{End}(A_F) \subseteq K$$

with $[K : \mathbb{Q}] = 4$ and $2R$ *prime*, so

$$A[2](\mathbb{Q}^{\mathrm{al}}) \simeq (R/2R)^2 \simeq \mathbb{F}_{16}^2.$$

Where are we going to find such curve X?

A Hilbert modular form over $F = \mathbb{Q}(\sqrt{3})$ with *Galois alignment*: 2.2.12.1-578.1-d.

Classical Modular forms

Classical Modular forms

A (classical) modular form f of weight k on $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$, is a holomorphic function defined on the the upper half plane $\mathfrak{h} := \{z : \Im(z) > 0\}$ which satisfies the transformation property

$$f(\gamma z) := f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{h}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and holomorphic at all the cusps of Γ (= ∞ points).

Classical Modular forms

A (classical) modular form f of weight k on $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$, is a holomorphic function defined on the the upper half plane $\mathfrak{h} := \{z : \Im(z) > 0\}$ which satisfies the transformation property

$$f(\gamma z) := f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{h}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and holomorphic at all the cusps of Γ (= ∞ points).

If $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, then $f(z) = f(z+1)$ and f has a Fourier expansion

$$f(z) = \sum_{n\geq 0} a_n q^n, \quad q = e^{2\pi i z}.$$

If $a_0 = 0$ and $a_1 = 1$, then f is known as a cusps form.

www.lmfdb.org/ModularForm/GL2/Q/holomorphic/

Classical modular forms to geometry: Eichler–Shimura construction

Classical modular forms to geometry: Eichler–Shimura construction

To an eigenform

$$f = \sum_{n \geq 1} a_n q^n \in S_2^{\mathrm{new}}(\Gamma_0(N)) \qquad a_n \in K_f := \mathbb{Q}(a_1, a_2, a_3, \dots)$$

Classical modular forms to geometry: Eichler–Shimura construction

To an eigenform

$$f = \sum_{n \geq 1} a_n q^n \in S_2^{\mathrm{new}}(\Gamma_0(N)) \qquad a_n \in K_f := \mathbb{Q}(a_1, a_2, a_3, \dots)$$

one can attach an abelian variety $A_f/\mathbb{Q}$ such that

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} \prod_p \left(1 - \tau(a_p) p^{-s} + \chi(p) p^{k-1} p^{-2s}\right)^{-1}$$

Classical modular forms to geometry: Eichler–Shimura construction

To an eigenform

$$f = \sum_{n \geq 1} a_n q^n \in S_2^{\text{new}}(\Gamma_0(N)) \qquad a_n \in K_f := \mathbb{Q}(a_1, a_2, a_3, \dots)$$

one can attach an abelian variety $A_f/\mathbb{Q}$ such that

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \prod_p \left(1 - \tau(a_p) p^{-s} + \chi(p) p^{k-1} p^{-2s}\right)^{-1}$$

If $K_f = \mathbb{Q}$, then A_f is an elliptic curve E_f, and $a_p = p + 1 - \#E(\mathbb{F}_p)$ for $p \nmid \operatorname{disc} E_f$.

Classical modular forms to geometry: Eichler–Shimura construction

To an eigenform

$$f = \sum_{n \geq 1} a_n q^n \in S_2^{\text{new}}(\Gamma_0(N)) \qquad a_n \in K_f := \mathbb{Q}(a_1, a_2, a_3, \dots)$$

one can attach an abelian variety $A_f/\mathbb{Q}$ such that

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \prod_p \left(1 - \tau(a_p) p^{-s} + \chi(p) p^{k-1} p^{-2s}\right)^{-1}$$

If $K_f = \mathbb{Q}$, then A_f is an elliptic curve E_f, and $a_p = p + 1 - \#E(\mathbb{F}_p)$ for $p \nmid \operatorname{disc} E_f$.

This construction can be made explicit via the Jacobian of $X_0(N)$

$$J_0(N) \sim \bigoplus_{M \mid N} \bigoplus_{f \in G_\mathbb{Q} \backslash S_2^{\text{new}}(\Gamma_0(M))} A_f^{\sigma_0(N/M)}$$

Classical modular forms to geometry: Eichler–Shimura construction

To an eigenform

$$f = \sum_{n\geq 1} a_n q^n \in S_2^{\text{new}}(\Gamma_0(N)) \qquad a_n \in K_f := \mathbb{Q}(a_1, a_2, a_3, \dots)$$

one can attach an abelian variety $A_f/\mathbb{Q}$ such that

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \prod_p \left(1 - \tau(a_p)p^{-s} + \chi(p)p^{k-1}p^{-2s}\right)^{-1}$$

If $K_f = \mathbb{Q}$, then A_f is an elliptic curve E_f, and $a_p = p + 1 - \#E(\mathbb{F}_p)$ for $p \nmid \operatorname{disc} E_f$.

This construction can be made explicit via the Jacobian of $X_0(N)$

$$J_0(N) \sim \bigoplus_{M|N} \bigoplus_{f \in G_\mathbb{Q} \backslash S_2^{\text{new}}(\Gamma_0(M))} A_f^{\sigma_0(N/M)}$$

and enables one compute the period matrix of A_f to any desired precision.

Hilbert modular forms to geometry: Eichler–Shimura construction

Replacing $SL_2(\mathbb{Z})$ with $GL_2^+(\mathbb{Z}_F)$, where $F \subset \mathbb{R}$, gives us Hilbert modular forms.

These follow similar transformation rules and also come with Fourier expansions

$$f = a_0 + \sum_{\nu \in \mathcal{D}^{-1}_{>0}} a_\nu q^\nu$$

seen as differential forms in the modular variety $X_0(\mathfrak{N})$ of dimension $\deg F$.

Hilbert modular forms to geometry: Eichler–Shimura construction

Replacing $SL_2(\mathbb{Z})$ with $GL_2^+(\mathbb{Z}_F)$, where $F \subset \mathbb{R}$, gives us Hilbert modular forms.

These follow similar transformation rules and also come with Fourier expansions

$$f = a_0 + \sum_{\nu \in \mathcal{D}_{>0}^{-1}} a_\nu q^\nu$$

seen as differential forms in the modular variety $X_0(\mathfrak{N})$ of dimension $\deg F$.

To an eigenform $f \in S_2^{\text{new}}(\Gamma_0(\mathfrak{N}))$ we also expect the existence of A_f/F, such that:

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \prod_{\mathfrak{p}} \left(1 - \tau(a_\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{-s} + \chi(\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{k-1} \operatorname{Nm}(\mathfrak{p})^{-2s}\right)^{-1}$$

However, for $F \neq \mathbb{Q}$, we no longer have a Jacobian to work with!

Hilbert modular forms to geometry: Eichler–Shimura construction

Replacing $SL_2(\mathbb{Z})$ with $GL_2^+(\mathbb{Z}_F)$, where $F \subset \mathbb{R}$, gives us Hilbert modular forms.

These follow similar transformation rules and also come with Fourier expansions

$$f = a_0 + \sum_{\nu \in \mathcal{D}^{-1}_{>0}} a_\nu q^\nu$$

seen as differential forms in the modular variety $X_0(\mathfrak{N})$ of dimension $\deg F$.

To an eigenform $f \in S_2^{\text{new}}(\Gamma_0(\mathfrak{N}))$ we also expect the existence of A_f/F, such that:

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} \prod_{\mathfrak{p}} \left(1 - \tau(a_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-s} + \chi(\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{k-1}\,\mathrm{Nm}(\mathfrak{p})^{-2s}\right)^{-1}$$

Hilbert modular forms to geometry: Eichler–Shimura construction

Replacing $SL_2(\mathbb{Z})$ with $GL_2^+(\mathbb{Z}_F)$, where $F \subset \mathbb{R}$, gives us Hilbert modular forms.

These follow similar transformation rules and also come with Fourier expansions

$$f = a_0 + \sum_{\nu \in \mathcal{D}^{-1}_{>0}} a_\nu q^\nu$$

seen as differential forms in the modular variety $X_0(\mathfrak{N})$ of dimension $\deg F$.

To an eigenform $f \in S_2^{\text{new}}(\Gamma_0(\mathfrak{N}))$ we also expect the existence of A_f/F, such that:

$$\dim A_f = \deg K_f$$

$$L(A_f, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \prod_{\mathfrak{p}} \left(1 - \tau(a_\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{-s} + \chi(\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{k-1} \operatorname{Nm}(\mathfrak{p})^{-2s}\right)^{-1}$$

However, for $F \neq \mathbb{Q}$, we no longer have a Jacobian to work with!

Eichler–Shimura relations for real quadratic fields

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Let $f \in S_2^{\text{new}}(\Gamma_0(\mathfrak{N}))$ be an eigenform with eigenvalue field K_f.

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Let $f \in S_2^{\mathrm{new}}(\Gamma_0(\mathfrak{N}))$ be an eigenform with eigenvalue field K_f.

There exists abelian varieties $A_f/\mathbb{C}$ and $A_f'/\mathbb{C}$ of dimension $g = \deg K_f$ such that

$$H^1(A_f, \mathbb{Q}) \otimes_{K_f} H^1(A_f', \mathbb{Q}) = H^2(X_0(\mathfrak{N})[f], \mathbb{Q})$$

as K_f-Hodge structures.

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Let $f \in S_2^{\mathrm{new}}(\Gamma_0(\mathfrak{N}))$ be an eigenform with eigenvalue field K_f.

There exists abelian varieties $A_f/\mathbb{C}$ and $A'_f/\mathbb{C}$ of dimension $g = \deg K_f$ such that

$$H^1(A_f, \mathbb{Q}) \otimes_{K_f} H^1(A'_f, \mathbb{Q}) = H^2(X_0(\mathfrak{N})[f], \mathbb{Q})$$

as K_f-Hodge structures.

- The construction is not explicit

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Let $f \in S_2^{\text{new}}(\Gamma_0(\mathfrak{N}))$ be an eigenform with eigenvalue field K_f.

There exists abelian varieties $A_f/\mathbb{C}$ and $A'_f/\mathbb{C}$ of dimension $g = \deg K_f$ such that

$$H^1(A_f, \mathbb{Q}) \otimes_{K_f} H^1(A'_f, \mathbb{Q}) = H^2(X_0(\mathfrak{N})[f], \mathbb{Q})$$

as K_f-Hodge structures.

- The construction is not explicit
- The fields of definition are unknown

Eichler–Shimura relations for real quadratic fields

Theorem (Oda)

Let F be a totally real quadratic field with trivial narrow class group.

Let $f \in S_2^{\mathrm{new}}(\Gamma_0(\mathfrak{N}))$ be an eigenform with eigenvalue field K_f.

There exists abelian varieties $A_f/\mathbb{C}$ and $A'_f/\mathbb{C}$ of dimension $g = \deg K_f$ such that

$$H^1(A_f, \mathbb{Q}) \otimes_{K_f} H^1(A'_f, \mathbb{Q}) = H^2(X_0(\mathfrak{N})[f], \mathbb{Q})$$

as K_f-Hodge structures.

- The construction is not explicit
- The fields of definition are unknown
- A_f are only well defined up to isogeny

Recovering an abelian variety from its L-function via BSD

Recovering an abelian variety from its L-function via BSD

Nonetheless, Oda gives an explicit formula for their periods $\tau(A_f), \tau(A'_f) \in \mathfrak{h}^g$.

$$\tau(A_f) = \left\{ \frac{\Omega^{+-}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}} \qquad \tau(A'_f) = \left\{ \frac{\Omega^{-+}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}}$$

Recovering an abelian variety from its L-function via BSD

Nonetheless, Oda gives an explicit formula for their periods $\tau(A_f), \tau(A'_f) \in \mathfrak{h}^g$.

$$\tau(A_f) = \left\{ \frac{\Omega^{+-}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma: K_f \hookrightarrow \mathbb{C}} \qquad \tau(A'_f) = \left\{ \frac{\Omega^{-+}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma: K_f \hookrightarrow \mathbb{C}}$$

Oda + BSD conjecture

For a quadratic character χ of signature ss', we have

$$\alpha_\chi \Omega^{ss'}(f^\sigma) = -4\pi^2 \sqrt{\operatorname{disc} F} G(\overline{\chi}) L(f^\sigma \otimes \chi, 1) \qquad \text{for some } \alpha_\chi \in \mathbb{Z}_F.$$

Recovering an abelian variety from its L-function via BSD

Nonetheless, Oda gives an explicit formula for their periods $\tau(A_f), \tau(A'_f) \in \mathfrak{h}^g$.

$$\tau(A_f) = \left\{ \frac{\Omega^{+-}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}} \qquad \tau(A'_f) = \left\{ \frac{\Omega^{-+}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}}$$

Oda + BSD conjecture

For a quadratic character χ of signature ss', we have

$$\alpha_\chi \Omega^{ss'}(f^\sigma) = -4\pi^2 \sqrt{\operatorname{disc} F} G(\overline{\chi}) L(f^\sigma \otimes \chi, 1) \qquad \text{for some } \alpha_\chi \in \mathbb{Z}_F.$$

By computing $L(f^\sigma \otimes \chi, 1)$ for several χ, we can guess the periods $\tau(A_f)$ and $\tau(A'_f)$.

This method leads to $\tau(A_f) \in i\mathbb{R}$. Hence, expected to be off by at least a 2-isogeny.

Recovering an abelian variety from its L-function via BSD

Nonetheless, Oda gives an explicit formula for their periods $\tau(A_f), \tau(A'_f) \in \mathfrak{h}^g$.

$$\tau(A_f) = \left\{ \frac{\Omega^{+-}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}} \qquad \tau(A'_f) = \left\{ \frac{\Omega^{-+}}{\Omega^{++}}(f^\sigma) \right\}_{\sigma : K_f \hookrightarrow \mathbb{C}}$$

Oda + BSD conjecture

For a quadratic character χ of signature ss', we have

$$\alpha_\chi \Omega^{ss'}(f^\sigma) = -4\pi^2 \sqrt{\operatorname{disc} F} G(\overline{\chi}) L(f^\sigma \otimes \chi, 1) \qquad \text{for some } \alpha_\chi \in \mathbb{Z}_F.$$

By computing $L(f^\sigma \otimes \chi, 1)$ for several χ, we can guess the periods $\tau(A_f)$ and $\tau(A'_f)$.

This method leads to $\tau(A_f) \in i\mathbb{R}$. Hence, expected to be off by at least a 2-isogeny.

Dembélé showcased such approach for reconstructing elliptic curves over F.

From A_f to the 17 degree polynomial

From A_f to the 17 degree polynomial

We construct $A_f(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda_f$ by taking

$$\Lambda_f := \mathbb{Z}_{K_f} \cdot \tau(A_f) \oplus \mathbb{Z}_{K_f} \cdot (1 \cdots 1)^t$$

From A_f to the 17 degree polynomial

We construct $A_f(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda_f$ by taking

$$\Lambda_f := \mathbb{Z}_{K_f} \cdot \tau(A_f) \oplus \mathbb{Z}_{K_f} \cdot (1 \cdots 1)^t$$

There are 17 abelian fourfolds A_γ that are 2-isogenous to A_f that respect the endomorphism ring, i.e., $\mathrm{End}(A_\gamma) = \mathrm{End}(A_f) = \mathbb{Z}_{K_f}$,

From A_f to the 17 degree polynomial

We construct $A_f(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda_f$ by taking

$$\Lambda_f := \mathbb{Z}_{K_f} \cdot \tau(A_f) \oplus \mathbb{Z}_{K_f} \cdot (1 \cdots 1)^t$$

There are 17 abelian fourfolds A_γ that are 2-isogenous to A_f that respect the endomorphism ring, i.e., $\mathrm{End}(A_\gamma) = \mathrm{End}(A_f) = \mathbb{Z}_{K_f}$, which leads us to define

$$P := \prod_\gamma (t - c_\gamma^4 E_4(A_\gamma)/E_4(A_f)) \in F[t]$$

From A_f to the 17 degree polynomial

We construct $A_f(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda_f$ by taking

$$\Lambda_f := \mathbb{Z}_{K_f} \cdot \tau(A_f) \oplus \mathbb{Z}_{K_f} \cdot (1 \cdots 1)^t$$

There are 17 abelian fourfolds A_γ that are 2-isogenous to A_f that respect the endomorphism ring, i.e., $\mathbf{End}(A_\gamma) = \mathbf{End}(A_f) = \mathbb{Z}_{K_f}$, which leads us to define

$$P := \prod_\gamma (t - c_\gamma^4 E_4(A_\gamma)/E_4(A_f)) \in F[t]$$

Theorem

We have $P \in \mathbb{Q}[t]$ and has Galois group 17T7.

The hunt for the 17 degree polynomial

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathbf{Nm}\,\mathfrak{p} \le 80\,000$ we obtain $\tau(A_f)$ to ~ 85 digits.

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathbf{Nm}\,\mathfrak{p} \leq 80\,000$ we obtain $\tau(A_f)$ to ~ 85 digits.
- We then searched for a 2-isogenous neighbor that looked like a Jacobian.

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathbf{Nm}\,\mathfrak{p} \leq 80\,000$ we obtain $\tau(A_f)$ to ~ 85 digits.
- We then searched for a 2-isogenous neighbor that looked like a Jacobian.
- This lead to the recognition of the first five coefficients of P as rationals.

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathbf{Nm}\,\mathfrak{p} \leq 80\,000$ we obtain $\tau(A_f)$ to ~ 85 digits.
- We then searched for a 2-isogenous neighbor that looked like a Jacobian.
- This lead to the recognition of the first five coefficients of P as rationals.
- With Newton–Raphson method, we refined $\tau(A_f)$ and recognized the $P \in \mathbb{Q}[t]$.

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathrm{Nm}\,\mathfrak{p} \leq 80\,000$ we obtain $\tau(A_f)$ to $\sim$ 85 digits.
- We then searched for a 2-isogenous neighbor that looked like a Jacobian.
- This lead to the recognition of the first five coefficients of P as rationals.
- With Newton–Raphson method, we refined $\tau(A_f)$ and recognized the $P \in \mathbb{Q}[t]$.

The rescaled integer polynomial is

$$
\begin{aligned}
&t^{17} - 155176125916688t^{16} - 39037751234563273371263727 44t^{15} - 56358325729359601656637373021434035279920t^{14} \\
&- 366800840143173954605482375177978351855973622141128420t^{13} \\
&- 1148273598471179728781481033200461057071613065513809470959738416912t^{12} \\
&- 1814416503358004575011887633363669311563353153960463604533351275745379344187064t^{11} \\
&- 1770863661928284803713567743362051511470304070815670165425643871240590168197004899614562992t^{10} \\
&- 20051761816455327745337405137833651123304126616376565312638724924223181384158787750761364528511 \cdots
\end{aligned}
$$

github.com/edgarcosta/EichlerShimuraHMF

The hunt for the 17 degree polynomial

- By computing $a_{\mathfrak{p}}$ for $\mathbf{Nm}\,\mathfrak{p} \leq 80\,000$ we obtain $\tau(A_f)$ to ~ 85 digits.
- We then searched for a 2-isogenous neighbor that looked like a Jacobian.
- This lead to the recognition of the first five coefficients of P as rationals.
- With Newton–Raphson method, we refined $\tau(A_f)$ and recognized the $P \in \mathbb{Q}[t]$.

The rescaled integer polynomial is

$$
\begin{aligned}
&t^{17} - 155176125916688t^{16} - 3903775123456327337126372744t^{15} - 563583257293596016566373730214340352799 20t^{14} \\
&- 366800840143173954605482375177978351855973622141128420t^{13} \\
&- 1148273598471179728781481033200461057071613065513809470959738416912t^{12} \\
&- 1814416503358004575011887633363669311563353153960463604533351275745379344187064t^{11} \\
&- 1770863661928284803713567743362051511470304070815670165425643871240590168197004899614562992t^{10} \\
&- 20051761816455327745337405137833651123304126616376565312638724924223181384158787750761364528511\cdots
\end{aligned}
$$

github.com/edgarcosta/EichlerShimuraHMF

CPU/Human time: ??

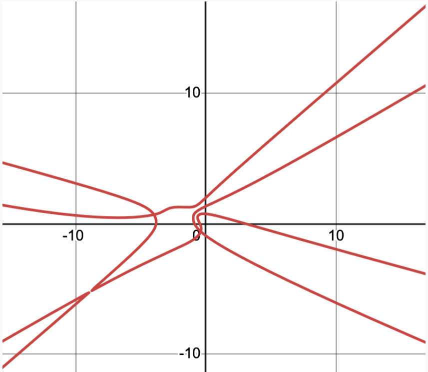
Curve

Curve

With refined $\tau(A_f)$ we were able to numerically reconstruct a genus 4 curve in $\mathbb{P}^3$:

$$-8x^2 + 8xy + 17y^2 - 34xz - 2yz - 28z^2 - 10xw - 9yw - 18zw + 2w^2 = 0$$

$$4x^3 - 6x^2y - 6xy^2 + 12x^2z + 6xyz + 24y^2z - 12xz^2 - 24z^3 + 2x^2w$$
$$+7xyw + 4y^2w + 4xzw - 13yzw - 8z^2w - 20xw^2 - 3zw^2 - 12w^3 = 0$$



Conclusion

Conclusion

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} \\ - 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17\mathrm{T}7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

Conclusion

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.

The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} - 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

- We exhibited a GL_2-modular form over $\mathbb{Q}(\sqrt{3})$ with Galois alignment whose mod 2 Galois representation gives $\mathrm{SL}_2(\mathbb{F}_{16})$.

Conclusion

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.
The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} - 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

- We exhibited a GL_2-modular form over $\mathbb{Q}(\sqrt{3})$ with Galois alignment whose mod 2 Galois representation gives $\mathrm{SL}_2(\mathbb{F}_{16})$.
- To make it effective, we reconstructed first the 2-isogeny polynomial of an abelian fourfold and then a curve with isomorphic Jacobian.

Conclusion

Theorem (van Bommel–C–Elkies–Keller–Schiavone–Voight)

The effective inverse Galois problem holds for the group 17T7.
The polynomial

$$f(x) = x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^{9} - 886x^{8} + 2024x^{7} - 604x^{6} + 2146x^{5} + 80x^{4} - 1376x^{3} - 496x^{2} - 1013x - 490$$

has $\mathrm{Gal}(f) \simeq 17T7 \simeq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$.

- We exhibited a GL_2-modular form over $\mathbb{Q}(\sqrt{3})$ with Galois alignment whose mod 2 Galois representation gives $\mathrm{SL}_2(\mathbb{F}_{16})$.
- To make it effective, we reconstructed first the 2-isogeny polynomial of an abelian fourfold and then a curve with isomorphic Jacobian.
- Are there infinitely many? Who knows