Effective Computation of Hodge Cycles

Edgar Costa (MIT)

July 30, 2025, Global Portuguese Mathematicians

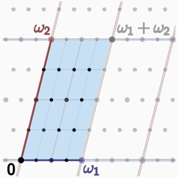
Slides available at edgarcosta.org.

Joint work with Nicholas Mascot, Jeroen Sijsling, John Voight, and Emre Can Sertöz

Wallpaper symmetries

Given a lattice generated by $\phi_1, \phi_2 \in \mathbb{C}$

$$\Lambda = \mathbb{Z} \cdot \phi_1 + \mathbb{Z} \cdot \phi_2 =$$

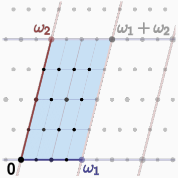


What are the possible symmetries?

Wallpaper symmetries

Given a lattice generated by $\phi_1, \phi_2 \in \mathbb{C}$

$$\Lambda = \mathbb{Z} \cdot \phi_1 + \mathbb{Z} \cdot \phi_2 =$$

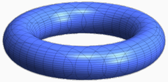


What are the possible symmetries?

What if we ask about rotations around 0?

- $\{\pm 1\}$, e.g., generic lattice
- $\{\pm 1, \pm i\}$, e.g., square lattice $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot i$
- $e^{\pm \pi i/3}$, e.g., hexagonal

From wallpaper to a doughnut

By forming the quotient, we obtain a torus $\mathbb{T} := \mathbb{C}/\Lambda \simeq$ 

Translations in Λ are now are trivial on $\mathbb{T}$.

Question

Which automorphisms $z \mapsto \alpha z$, for $\alpha \in \mathbb{C}$, descend to $\mathbb{T}$?

In other words, when there is a $R \in M_2(\mathbb{Z})$ such that

$$\alpha \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} = \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} R?$$

Symmetries of $\mathbb{T}$ correspond to the invertible maps, i.e., $R \in \mathbf{GL}_2(\mathbb{Z})$.

By dropping the invertible requirement we get endomorphisms, and these form an algebra!

For example, $\mathbb{Z} \subseteq \mathbf{End}(\mathbb{T}) \simeq \mathbf{End}(\Lambda)$, via multiplication by n (as a scalar or matrix).

From doughnuts to elliptic curves

Today, we are particularly interested in solving equations of the form

$$\alpha \left(\phi_{i,j}\right)_{i,j} = \left(\phi_{i,j}\right)_{i,j} R, \qquad \alpha \in M_g(\mathbb{Q}^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z})$$

where ϕ are integrals capturing geometric and arithmetic information.

From doughnuts to elliptic curves

Today, we are particularly interested in solving equations of the form

$$\alpha \left(\phi_{i,j}\right)_{i,j} = \left(\phi_{i,j}\right)_{i,j} R, \qquad \alpha \in M_g(\mathbb{Q}^{\mathsf{al}}), \quad R \in M_{2g}(\mathbb{Z})$$

where ϕ are integrals capturing geometric and arithmetic information.

From doughnuts to elliptic curves

Today, we are particularly interested in solving equations of the form

$$\alpha\left(\phi_{i,j}\right)_{i,j}=\left(\phi_{i,j}\right)_{i,j}R, \qquad \alpha\in M_g(\mathbb{Q}^{\mathsf{al}}), \quad R\in M_{2g}(\mathbb{Z})$$

where ϕ are integrals capturing geometric and arithmetic information.

For example:

$$\phi=\oint_\gamma \omega,$$

where $\gamma\in \mathrm{H}_1(C,\mathbb{Z})\simeq\mathbb{Z}^{2g}$ and $\omega\in\mathrm{H}^1(C,\Omega_C)\simeq\mathbb{Q}^g$, for a genus g curve C.

From doughnuts to elliptic curves

Today, we are particularly interested in solving equations of the form

$$\alpha \left(\phi_{i,j}\right)_{i,j} = \left(\phi_{i,j}\right)_{i,j} R, \qquad \alpha \in M_g(\mathbb{Q}^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z})$$

where ϕ are integrals capturing geometric and arithmetic information.

For example:

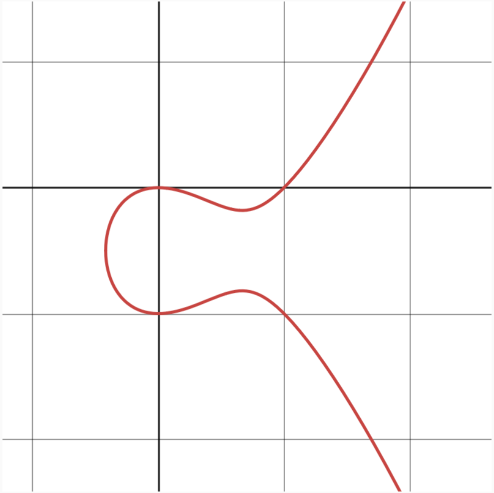
$$\phi = \oint_\gamma \omega,$$

where $\gamma \in \mathrm{H}_1(C, \mathbb{Z}) \simeq \mathbb{Z}^{2g}$ and $\omega \in \mathrm{H}^1(C, \Omega_C) \simeq \mathbb{Q}^g$, for a genus g curve C.

For example, if $g = 1$, we may take $C\colon y^2 = f(x)$, with $\deg f = 3$, and $\omega = dx/\sqrt{f(x)}$.

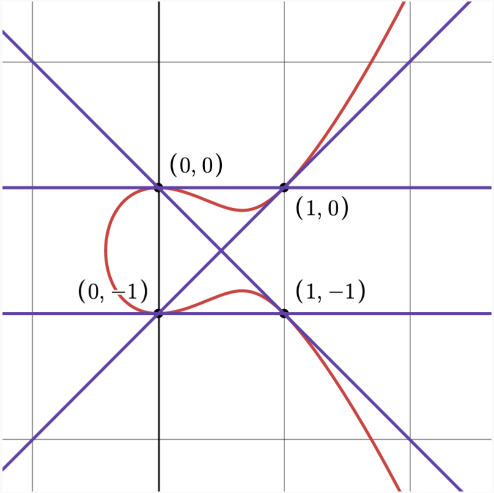
In this case, C is an elliptic curve, named after the elliptic integral $\int dx/\sqrt{f(x)}$.

Elliptic curves group structure



$$E\colon y^2 + y = x^3 - x^2$$
$$P + Q + R \sim 0$$

Elliptic curves group structure



$$E\colon y^2 + y = x^3 - x^2, \qquad \mathbb{Z}/5\mathbb{Z} \simeq E(\mathbb{Q}).$$

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

Endomorphisms of elliptic curves

There are two types of elliptic curves:

Ordinary: $\operatorname{End} E_{\mathbb{Q}^{\text{al}}} = Z$, i.e., the only endomorphisms are multiplication by n.

Complex Multiplication: $\mathbb{Z} \subsetneq \operatorname{End} E_{\mathbb{Q}^{\text{al}}} \subsetneq \mathbb{Q}(\sqrt{-d})$

Endomorphisms of elliptic curves

There are two types of elliptic curves:

Ordinary: $\operatorname{End} E_{\mathbb{Q}^{\text{al}}} = Z$, i.e., the only endomorphisms are multiplication by n.

Complex Multiplication: $\mathbb{Z} \subsetneq \operatorname{End} E_{\mathbb{Q}^{\text{al}}} \subsetneq \mathbb{Q}(\sqrt{-d})$

In other words, if $\phi_2/\phi_1 \in \mathbb{Q}(\sqrt{-d})$, then

$$\alpha \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} = \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} R, \qquad \alpha \in \mathbb{Q}^{\text{al}}, \quad R \in M_2(\mathbb{Z})$$

has solutions with $\alpha \in \mathbb{Q}(\sqrt{-d})$.

Endomorphisms of elliptic curves

There are two types of elliptic curves:

Ordinary: $\mathrm{End}\, E_{\mathbb{Q}^{\mathrm{al}}} = Z$, i.e., the only endomorphisms are multiplication by n.

Complex Multiplication: $\mathbb{Z} \subsetneq \mathrm{End}\, E_{\mathbb{Q}^{\mathrm{al}}} \subsetneq \mathbb{Q}(\sqrt{-d})$

In other words, if $\phi_2/\phi_1 \in \mathbb{Q}(\sqrt{-d})$, then

$$\alpha \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} = \begin{pmatrix} \phi_1 & \phi_2 \end{pmatrix} R, \qquad \alpha \in \mathbb{Q}^{\mathrm{al}}, \quad R \in M_2(\mathbb{Z})$$

has solutions with $\alpha \in \mathbb{Q}(\sqrt{-d})$.

Elliptic curves with CM are isolated points in their moduli space $\simeq \mathbb{P}^1$.

The possible list of d is finite. If $E/\mathbb{Q}$, then $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.

Jacobians

Curves no longer have a group structure for $g > 1$.

Instead, we associate to them an abelian variety called the *Jacobian* $A := \mathrm{Jac}(C)$, the group of divisors of degree 0 on C up to linear equivalence.

Jacobians

Curves no longer have a group structure for $g > 1$.

Instead, we associate to them an abelian variety called the *Jacobian* $A := \mathrm{Jac}(C)$, the group of divisors of degree 0 on C up to linear equivalence.

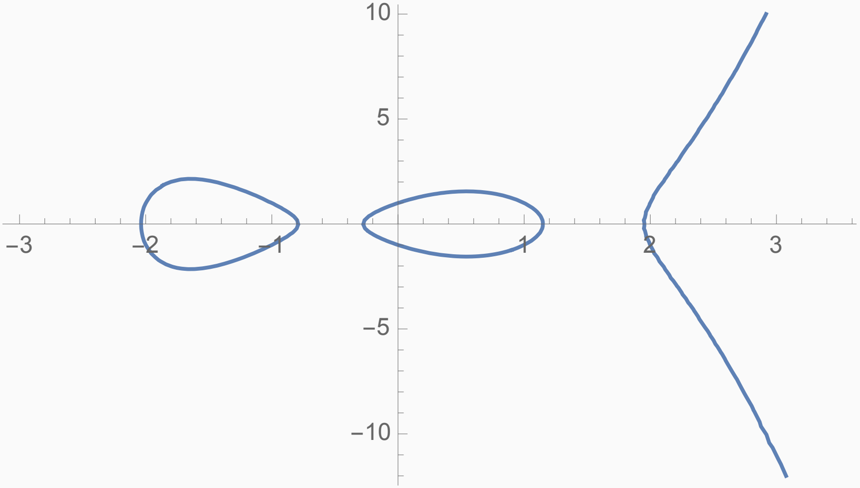
When $g = 1$ and $C = E$ is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$ by $P \mapsto [P - \infty]$.

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

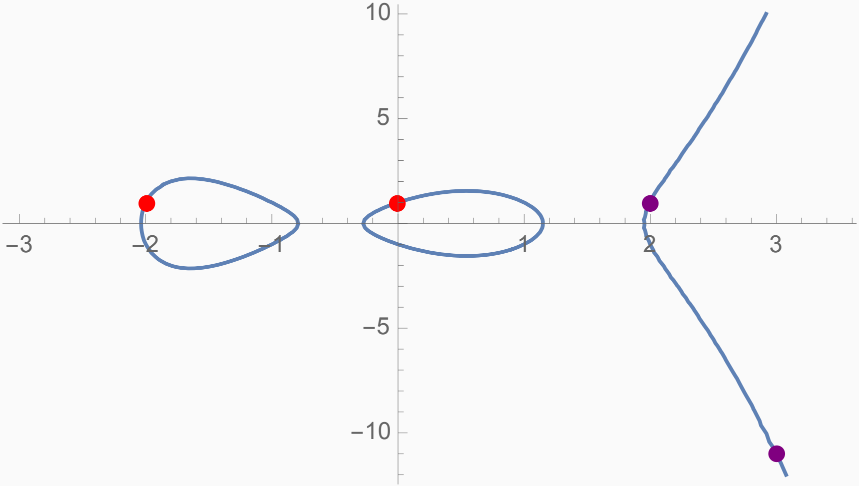
In general, we can think about adding tuples of g-points.

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

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



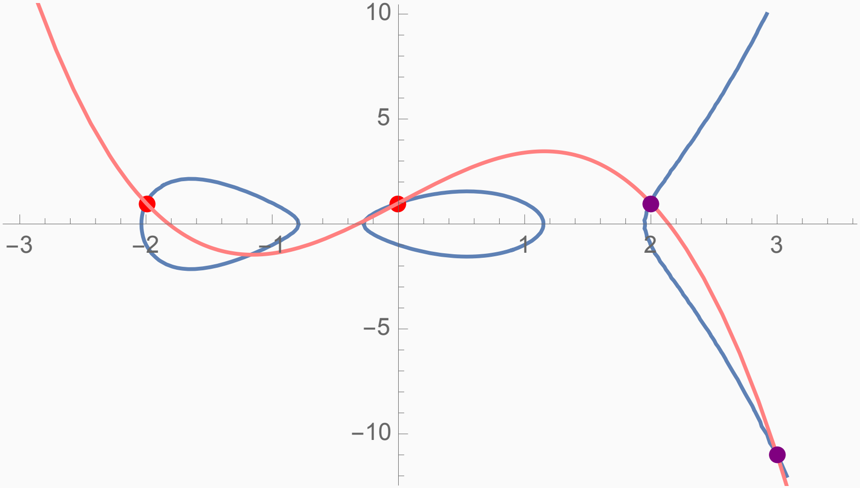
Addition on the Jacobian of a genus 2 curve, e.g, $C : y^2 = x^5 - 5x^3 + 4x + 1$



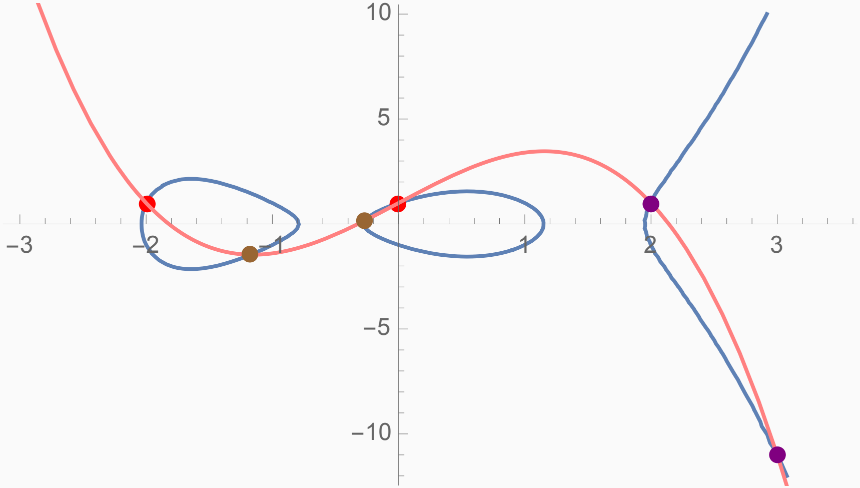
$D_1 := (-2, 1) + (0, 1)$

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

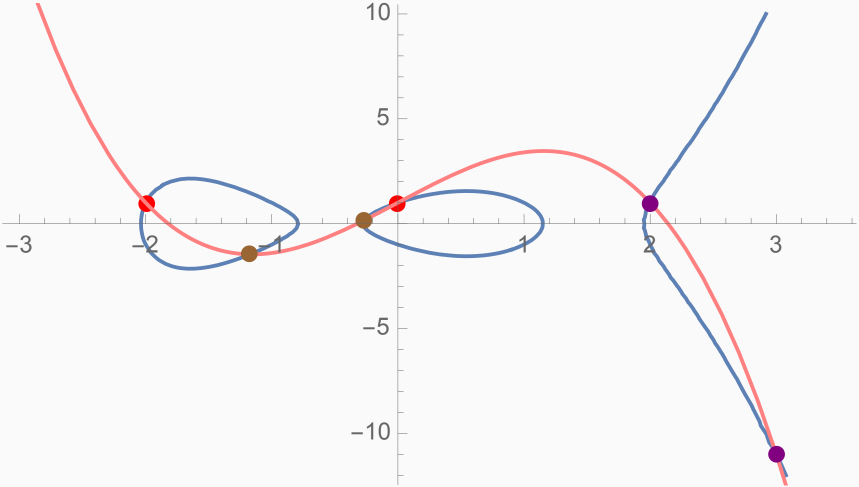
Addition on the Jacobian of a genus 2 curve, e.g, $C : y^2 = x^5 - 5x^3 + 4x + 1$



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

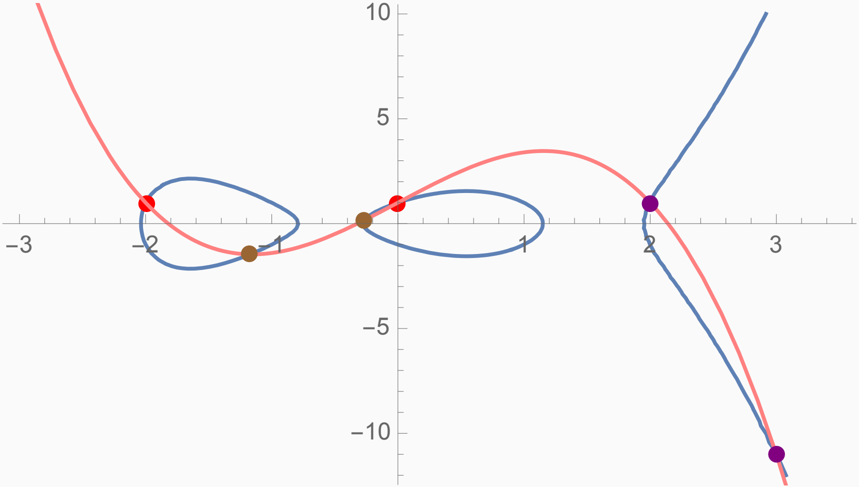


Addition on the Jacobian of a genus 2 curve, e.g, $C : y^2 = x^5 - 5x^3 + 4x + 1$



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

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



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

Our setup

Let C be a nice (smooth, projective, geometrically integral) curve over k of genus g given by equations. Let J be the Jacobian of C.

Goal

Given the equations of C, compute the endomorphism ring $\mathbf{End}\, J^{\mathrm{al}}$.

Our setup

Let C be a nice (smooth, projective, geometrically integral) curve over k of genus g given by equations. Let J be the Jacobian of C.

Goal

Given the equations of C, compute the endomorphism ring $\mathrm{End}\, J^{\mathrm{al}}$.

- Finding interesting examples. Generically $\mathrm{End}\, J^{\mathrm{al}} = \mathbb{Z}$.

Our setup

Let C be a nice (smooth, projective, geometrically integral) curve over k of genus g given by equations. Let J be the Jacobian of C.

Goal

Given the equations of C, compute the endomorphism ring $\mathbf{End}\, J^{\mathrm{al}}$.

- Finding interesting examples. Generically $\mathbf{End}\, J^{\mathrm{al}} = \mathbb{Z}$.
- If $\mathbf{End}\, J$ contains non-trivial idempotents, we can hope to decompose J into abelian varieties of smaller dimension.
- If $\mathbf{End}\, J$ is non-trivial, then this allows us to find a modular form that describes the arithmetic properties of J and C.
- Can be used to show transcendence of 1-periods (Ouaknine–Worrell–Sertöz)

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick a k-basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick a k-basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick a k-basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model
- Using Λ, we can hope to understand J analytically...
  and perhaps even be able to transfer these results to the algebraic setting.

Heuristic solution

By picking a k-basis for $H^0(C, \Omega_C)$, we have

$$\operatorname{End}(J) = \{T \in M_g(k) \mid T\Lambda \subset \Lambda\}$$

Hence, if Π is a period matrix for C, i.e., $\Lambda = \Pi\mathbb{Z}^{2g}$, then we are reduced to finding a $\mathbb{Z}$-basis of the solutions (T, R) to

$$T\Pi = \Pi R, \qquad T \in M_g(k^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z}).$$

Heuristic solution

By picking a k-basis for $H^0(C, \Omega_C)$, we have

$$\mathrm{End}(J) = \{T \in M_g(k) \mid T\Lambda \subset \Lambda\}$$

Hence, if Π is a period matrix for C, i.e., $\Lambda = \Pi\mathbb{Z}^{2g}$, then we are reduced to finding a $\mathbb{Z}$-basis of the solutions (T, R) to

$$T\Pi = \Pi R, \qquad T \in M_g(k^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z}).$$

Heuristically, via lattice reduction algorithms, we can find such a $\mathbb{Z}$-basis.

Heuristic solution

By picking a k-basis for $H^0(C, \Omega_C)$, we have

$$\mathrm{End}(J) = \{T \in M_g(k) \mid T\Lambda \subset \Lambda\}$$

Hence, if Π is a period matrix for C, i.e., $\Lambda = \Pi\mathbb{Z}^{2g}$, then we are reduced to finding a $\mathbb{Z}$-basis of the solutions (T, R) to

$$T\Pi = \Pi R, \qquad T \in M_g(k^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z}).$$

Heuristically, via lattice reduction algorithms, we can find such a $\mathbb{Z}$-basis.

There is no obvious way to prove that our guesses are actually correct.

Representing endomorphisms via correspondences

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \mapsto \{Q_1, \ldots, Q_g\} \iff \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

Representing endomorphisms via correspondences

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \mapsto \{Q_1, \ldots, Q_g\} \iff \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

The equations of this divisor is a certificate of containment $\boxed{\alpha}$ for $\alpha \in \mathrm{End}\, J^{\mathrm{al}}$.

Representing endomorphisms via correspondences

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \mapsto \{Q_1, \ldots, Q_g\} \iff \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

The equations of this divisor is a certificate of containment 

for $\alpha \in \mathrm{End}\, J^{\mathrm{al}}$.

Theorem (C–Mascot–Sijsling–Voight)

We give an algorithm for

$$\mathrm{M}_g(k^{\mathrm{al}}) \ni \alpha \mapsto \begin{cases} \texttt{true} & \text{if } \alpha \in \mathrm{End}\, J^{\mathrm{al}}, \text{ and a certificate} \\ \texttt{false} & \text{if } \alpha \notin \mathrm{End}\, J^{\mathrm{al}} \end{cases}$$

By interpolation via α_C or by locally solving a differential equation on $C \times C$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\mathrm{End}\, J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \mathrm{End}\, J^{\mathrm{al}}$.

$$\mathrm{M}_g(k^{\mathrm{al}}) \ni \alpha \mapsto \begin{cases} \texttt{true} & \text{if } \alpha \in \mathrm{End}\, J^{\mathrm{al}}, \text{ and a certificate } \\ \texttt{false} & \text{if } \alpha \notin \mathrm{End}\, J^{\mathrm{al}} \end{cases}$$

- By night, we search for evidence that $\mathrm{End}\, J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* ✓.

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.
  - Studying $J_{\mathbb{F}_p}$ for several p. Under the Mumford–Tate conjecture its structure will be as random as $\operatorname{End} J^{\mathrm{al}}$ allows it, and we get a sharp upperbound.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.
  - Studying $J_{\mathbb{F}_p}$ for several p. Under the Mumford–Tate conjecture its structure will be as random as $\operatorname{End} J^{\mathrm{al}}$ allows it, and we get a sharp upperbound.
  - Studying what Hodge cycles lift from $\mathbb{Z}/p^n\mathbb{Z}$ to the limit $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Examples

- We have verified, decomposed and matched the 66 158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* `LMFDB.org`

Examples

- We have verified, decomposed and matched the 66 158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* LMFDB.org
- The algorithm verifies that the following genus 4 curve over $\mathbb{Q}(\sqrt{3})$

$$\begin{aligned}
0 &= -8x^2 + 8xy + 17y^2 - 34xz - 2yz - 28z^2 - 10xw - 9yw - 18zw + 2w^2, \\
0 &= 4x^3 - 6x^2y - 6xy^2 + 12x^2z + 6xyz + 24y^2z - 12xz^2 - 24z^3 + 2x^2w + 7xyw \\
&\qquad + 4y^2w + 4xzw - 13yzw - 8z^2w - 20xw^2 - 3zw^2 - 12w^3
\end{aligned}$$

has real multiplication by the maximal order of $\mathbb{Q}(x)/(x^4 - x^3 - 3x^2 + x + 1)$.

Examples

- We have verified, decomposed and matched the 66 158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* `LMFDB.org`
- The algorithm verifies that the following genus 4 curve over $\mathbb{Q}(\sqrt{3})$

$$
\begin{aligned}
0 &= -8x^2 + 8xy + 17y^2 - 34xz - 2yz - 28z^2 - 10xw - 9yw - 18zw + 2w^2, \\
0 &= 4x^3 - 6x^2y - 6xy^2 + 12x^2z + 6xyz + 24y^2z - 12xz^2 - 24z^3 + 2x^2w + 7xyw \\
&\qquad + 4y^2w + 4xzw - 13yzw - 8z^2w - 20xw^2 - 3zw^2 - 12w^3
\end{aligned}
$$

has real multiplication by the maximal order of $\mathbb{Q}(x)/(x^4 - x^3 - 3x^2 + x + 1)$. We used this in a recent project, where we show that the 2-isogeny field of A_f solves the inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes C_2 \simeq$ **17T7**. 32 MB .

Examples

- We have verified, decomposed and matched the 66 158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* `LMFDB.org`
- The algorithm verifies that the following genus 4 curve over $\mathbb{Q}(\sqrt{3})$

$$
\begin{aligned}
0 &= -8x^2 + 8xy + 17y^2 - 34xz - 2yz - 28z^2 - 10xw - 9yw - 18zw + 2w^2,\\
0 &= 4x^3 - 6x^2y - 6xy^2 + 12x^2z + 6xyz + 24y^2z - 12xz^2 - 24z^3 + 2x^2w + 7xyw\\
&\qquad + 4y^2w + 4xzw - 13yzw - 8z^2w - 20xw^2 - 3zw^2 - 12w^3
\end{aligned}
$$

  has real multiplication by the maximal order of $\mathbb{Q}(x)/(x^4 - x^3 - 3x^2 + x + 1)$.
  We used this in a recent project, where we show that the 2-isogeny field of A_f solves the inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes C_2 \simeq$ **17T7**. 32 MB .
- Code available: `https://github.com/edgarcosta/endomorphisms`

What is a K3 surface?

K3 surfaces are one of the natural generalizations of elliptic curves.

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

What is a K3 surface?

K3 surfaces are one of the natural generalizations of elliptic curves.

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

e.g. Fermat quartic surface $x^4 + y^4 + z^4 + w^4 = 0$.

What is a K3 surface?

K3 surfaces are one of the natural generalizations of elliptic curves.

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

e.g. Fermat like surface $w^2 = x^6 + y^6 + z^6$.

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\operatorname{Pic} X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z})$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\mathrm{NS}\, X^{\mathrm{al}} \simeq \mathrm{Pic}\, X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\mathrm{Pic}\, X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z}) \subsetneq H^2(X, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle\text{algebraic curves in } X\rangle / \langle\text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\operatorname{Pic} X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z}) \subsetneq H^2(X, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

Thus, $1 \leq \operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} \leq 20 = \dim H^{1,1}(X)$.

A generic K3 surface has $\operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} = 1$.

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle\text{algebraic curves in } X\rangle/\langle\text{linear equivalences}\rangle \subset H_2(X,\mathbb{Z})$$

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\operatorname{Pic} X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X,\mathbb{Z}) \subsetneq H^2(X,\mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

Thus, $1 \leq \operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} \leq 20 = \dim H^{1,1}(X)$.

A generic K3 surface has $\operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} = 1$.

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

"The evaluation of ρ for a given surface presents in general grave difficulties." — Zariski

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

"The evaluation of ρ for a given surface presents in general grave difficulties." — Zariski

"New and interesting" Galois representations arise from $T(X)$:

$$H^2(X, \mathbb{Q}) \simeq Pic(X^{\mathrm{al}})_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

"The evaluation of ρ for a given surface presents in general grave difficulties." — Zariski

"New and interesting" Galois representations arise from $T(X)$:

$$H^2(X, \mathbb{Q}) \simeq Pic(X^{\mathrm{al}})_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}$$

Useful for studying rational points, via a potential Brauer–Manin obstruction:

$$H^1(\operatorname{Gal}(k^{\mathrm{al}}/k), \operatorname{Pic} X^{\mathrm{al}}) \simeq \mathrm{Br}_1(X)/Br_0(X)$$

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$$

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\text{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a (saturated) lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a (saturated) lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

- Unlike for curves, effective algorithms to compute Π have only become available very recently.
- Heuristically, via lattice reduction algorithms, we can find $\Lambda \subset H_2(X, \mathbb{Z})$.
- There is no obvious way to prove that our guesses are actually correct.

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a (saturated) lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

- Unlike for curves, effective algorithms to compute Π have only become available very recently.
- Heuristically, via lattice reduction algorithms, we can find $\Lambda \subset H_2(X, \mathbb{Z})$.
- There is no obvious way to prove that our guesses are actually correct.
- Nonetheless, given Π as a ball, one can compute $B \gg 0$ such that such that

$$\operatorname{Pic}(X^{\mathrm{al}})_{|B} := \mathbb{Z}\langle \gamma \in \operatorname{Pic} X^{\mathrm{al}} \mid -\gamma_{\mathrm{prim}}^2 < B \rangle \subseteq \Lambda \qquad \text{(Lairez–Sertöz)}.$$

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} \geq 19$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3 z + yw^3 + z^3 w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3 z + yw^3 + z^3 w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut}\Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut} \Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.
- No small rational curves: There are no lines, no conics, no twisted cubics.
- The “smallest” non-trivial curves that appear are smooth rational quartics.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk} \operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut} \Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.
- No small rational curves: There are no lines, no conics, no twisted cubics.
- The “smallest” non-trivial curves that appear are smooth rational quartics.
- Lattice computations with Λ predict that there are

  133056

  smooth rational quartics spanning Λ.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon \mathrm{H}_2(X,\mathbb{Z}) \times \mathrm{H}^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1\,\mathrm{H}^2_{\mathrm{dR}}(X/k)$.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon \mathrm{H}_2(X,\mathbb{Z}) \times \mathrm{H}^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1\,\mathrm{H}^2_{\mathrm{dR}}(X/k)$.

Theorem (Movasati–Sertöz)

If $\gamma = [C] \in \mathrm{H}_2(X,\mathbb{Z})$ for a curve $C \subset X$ then from $\frac{1}{2\pi i}(\int_\gamma \omega)_{\omega\in F^1}$ one can construct an ideal I_γ such that $I(C) \subsetneq I_\gamma$.

In favorable circumstances we expect low order equations in I_γ to span $I(C)$.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon \mathrm{H}_2(X,\mathbb{Z}) \times \mathrm{H}^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1\,\mathrm{H}^2_{\mathrm{dR}}(X/k)$.

Theorem (Movasati–Sertöz)

If $\gamma = [C] \in \mathrm{H}_2(X,\mathbb{Z})$ for a curve $C \subset X$ then from $\frac{1}{2\pi i}(\int_\gamma \omega)_{\omega\in F^1}$ one can construct an ideal I_γ such that $I(C) \subsetneq I_\gamma$.

In favorable circumstances we expect low order equations in I_γ to span $I(C)$.

Theorem (Cifani–Pirola–Schlesinger)

For a smooth rational quartic curve $C \subset X$ we have that the equation of the quadric surface containing C generates $I_{[C],2}$, i.e., $I(C)_2 = I_{[C],2}$.

Reconstructing quadric surfaces

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

$$\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

Reconstructing quadric surfaces

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

$$\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

- Fortunately, there is a small **Aut(Λ)** orbit of size 336:
  $133056 = 336 + 1008 + 1176 + 3528 \cdot 3 + 4704 \cdot 3 + 7056 \cdot 9 + 14112 \cdot 3$

Reconstructing quadric surfaces

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

- Fortunately, there is a small $\mathbf{Aut}(\Lambda)$ orbit of size 336:
  $133056 = 336 + 1008 + 1176 + 3528 \cdot 3 + 4704 \cdot 3 + 7056 \cdot 9 + 14112 \cdot 3$
- For each quartic curve $C \subset X$, we can compute

$$I_{[C],2} = \langle a_0 x^2 + \cdots + a_9 w^2 \rangle_{\mathbb{C}}$$

  that defines a quadric surface Q, such that $Q \cap X = C \cup \overline{C}$.
  Hence, we expect an orbit of 168 quadrics each containing a pair of quartics.
- We aim reconstruct the ten (algebraic!) coefficients of these quadrics.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.
- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 10014013832542203812872613924739x^{161}$$
$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$
$$-1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$
$$+23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313\cdots$$

- Every computation must be done extremely selectively!

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.
- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 1001401383254220381287261392 4739x^{161}$$
$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$
$$- 1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$
$$+ 23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313 \cdots$$

- Every computation must be done extremely selectively!
- We are presented with the same 168 degree field L in 9 different ways.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 1001401383254220381287261392 4739x^{161}$$

$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$

$$- 1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$

$$+ 23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313 \cdots$$

- Every computation must be done extremely selectively!
- We are presented with the same 168 degree field L in 9 different ways. The abstract isomorphism problem is hopeless.

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \ldots, a_9) = \mathbb{Q}(a_0)$.

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \ldots, a_9) = \mathbb{Q}(a_0)$.

In our case, we have all the compatible embeddings

$$\sigma_i : \mathbb{Q}(a_k) \hookrightarrow L \hookrightarrow \mathbb{C}$$

Thus the isomorphisms is given is the solution of the following linear system

$$\{\sigma_i(a_k)^j\}_{i,j} \cdot v = \{\sigma_i(a_0)\}_i, \qquad v \in \mathbb{Q}^{168}$$

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \dots, a_9) = \mathbb{Q}(a_0)$.

In our case, we have all the compatible embeddings

$$\sigma_i : \mathbb{Q}(a_k) \hookrightarrow L \hookrightarrow \mathbb{C}$$

Thus the isomorphisms is given is the solution of the following linear system

$$\{\sigma_i(a_k)^j\}_{i,j} \cdot v = \{\sigma_i(a_0)\}_i, \qquad v \in \mathbb{Q}^{168}$$

This is numerically stable, as $\{\sigma_i(a_k)^j\}_{i,j}$ is a Vandermonde matrix, and one can verify the solution once found.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive! Linear algebra 😰

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive! Linear algebra 😰 Gröbner basis 😱

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0 x^2 + a_1 xy + \cdots + a_9 w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!
  Linear algebra 😰 Gröbner basis 😱
- Working over $\mathbb{F}_p$ we find 10 distinct points.
  Hence, S is zero-dimensional and reduced, and $\deg S \leq 10$.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!
  Linear algebra 😰 Gröbner basis 😱
- Working over $\mathbb{F}_p$ we find 10 distinct points.
  Hence, S is zero-dimensional and reduced, and $\deg S \leq 10$.
- We conclude $\deg S = 10$ via Gotzmann regularity theorem, by checking that $\dim L[x, y, z, w]_\bullet / I_\bullet = 10$ for $\bullet = 6, 7$, where $V(I) = S$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Certifying $\operatorname{Pic} X^{\text{al}} = \Lambda$

$$Q : a_0 x^2 + a_1 xy + \cdots + a_9 w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\text{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\text{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\text{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0 x^2 + a_1 xy + \cdots + a_9 w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.
- Certify that these correspond to the original classes.
  Showing that there are at most 66528 distinct quadrics. Can be done over $\mathbb{C}$.
  This establishes a bijection between these quadric surfaces and the 168 pairs of quartic curve classes that they correspond to.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.
- Certify that these correspond to the original classes.
  Showing that there are at most 66528 distinct quadrics. Can be done over $\mathbb{C}$.
  This establishes a bijection between these quadric surfaces and the 168 pairs of quartic curve classes that they correspond to.

$$\operatorname{Pic} X^{\mathrm{al}} = \Lambda \quad \checkmark$$

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega \in F^1} \in K^{21}$.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega \in F^1} \in K^{21}$.

These can be reconstructed in the same fashion as we reconstructed a_i.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega \in F^1} \in K^{21}$.

These can be reconstructed in the same fashion as we reconstructed a_i.

Unclear how to certify this step! What are the denominators of $\frac{1}{2\pi i}\int_C \omega$?

Can one certifiable K using geometry instead of Gröbner basis?

Summary

Today we saw how solving for

$$T\Pi_X = \Pi_X R, \qquad T \in M_n(k^{\mathrm{al}}), \quad R \in M_m(\mathbb{Z})$$

heuristically reveals both arithmetic and the geometry X.

And how convert these heuristic insights into rigorous mathematical statements:

- If $X = \mathrm{Jac}(C)$, we give an algorithm to compute $\mathrm{End}\, J^{\mathrm{al}}$.
- If X is a K3 surface, we give an algorithm to compute the saturation of the lattice generated by rational curves of degree up to 4.

Theorem (C–Sertöz)

The K3 surface $X : x^4 + xyzw + y^3 z + yw^3 + z^3 w = 0 \subset \mathbb{P}^3$ has $\mathrm{Pic}\, X^{\mathrm{al}} = \Lambda$, generated by quartics over a quadratic extension of $L := \mathbb{Q}(\{a_i\}_i)$.