The „exponential” torsion of superelliptic Jacobians

Jędrzej Garnek

UAM Poznań

SYMPAAN
Będlewo, 23.07.2025

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \quad \mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor$$

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor$$

Question

Find the determinant of the matrix:

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in (\mathbb{Z}/\ell)^\times}$$

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor$$

Question

Find the determinant of the matrix:

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in (\mathbb{Z}/\ell)^\times}$$

For any $i \in (\mathbb{Z}/\ell)^\times$:

$$n(i) + n(\ell - i) = r - 1$$

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \frac{1}{2}\mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}$$

Question

Find the determinant of the matrix:

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in (\mathbb{Z}/\ell)^\times}$$

For any $i \in (\mathbb{Z}/\ell)^\times$:

$$n(i) + n(\ell - i) = r - 1$$

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \frac{1}{2}\mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}$$

Question

Find the determinant of the matrix:

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in (\mathbb{Z}/\ell)^\times}$$

For any $i \in (\mathbb{Z}/\ell)^\times$:

$$n(i) + n(\ell - i) = 0 \qquad \text{(odd function)}$$

Let $\ell \in \mathbb{P}$, $\ell \nmid r$. Consider the function:

$$n : (\mathbb{Z}/\ell)^\times \to \frac{1}{2}\mathbb{Z}, \qquad n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}$$

Question

Find the determinant of the matrix:

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C}$$

where C – arbitrary set of representatives of $(\mathbb{Z}/\ell)^\times/\langle \pm 1 \rangle$.

For any $i \in (\mathbb{Z}/\ell)^\times$:

$$n(i) + n(\ell - i) = 0 \qquad \text{(odd function)}$$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

$$\det M_{\ell,r} =$$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

$$\det M_{\ell,r} = \begin{vmatrix} n(\frac{2}{2}) & n(\frac{2}{4}) & n(\frac{2}{5}) & n(\frac{2}{8}) & n(\frac{2}{10}) \\ n(\frac{4}{2}) & n(\frac{4}{4}) & n(\frac{4}{5}) & n(\frac{4}{8}) & n(\frac{4}{10}) \\ n(\frac{5}{2}) & n(\frac{5}{4}) & n(\frac{5}{5}) & n(\frac{5}{8}) & n(\frac{5}{10}) \\ n(\frac{8}{2}) & n(\frac{8}{4}) & n(\frac{8}{5}) & n(\frac{8}{8}) & n(\frac{8}{10}) \\ n(\frac{10}{2}) & n(\frac{10}{4}) & n(\frac{10}{5}) & n(\frac{10}{8}) & n(\frac{10}{10}) \end{vmatrix}$$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

$$\det M_{\ell,r} = \begin{vmatrix} n(1) & n(6) & n(7) & n(3) & n(9) \\ n(2) & n(1) & n(3) & n(6) & n(7) \\ n(8) & n(4) & n(1) & n(2) & n(6) \\ n(4) & n(2) & n(6) & n(1) & n(3) \\ n(5) & n(8) & n(2) & n(4) & n(1) \end{vmatrix}$$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

$$\det M_{\ell,r} = \begin{vmatrix} -1 & 0 & 0 & -1 & 1 \\ -1 & -1 & -1 & 0 & 0 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & -1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & -1 \end{vmatrix}$$

$$M_{\ell,r} := [n(i \cdot j^{-1})]_{i,j \in C},$$
$$n(j) := \left\lfloor \frac{j \cdot r}{\ell} \right\rfloor - \frac{r-1}{2}.$$

Example: $\ell = 11,\ r = 3,\ C = \{2, 4, 5, 8, 10\} \Rightarrow$

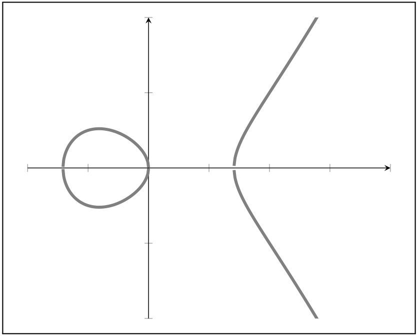
$$\det M_{\ell,r} = \begin{vmatrix} -1 & 0 & 0 & -1 & 1 \\ -1 & -1 & -1 & 0 & 0 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & -1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & -1 \end{vmatrix} = -11$$

An **abelian variety** is a projective algebraic group.

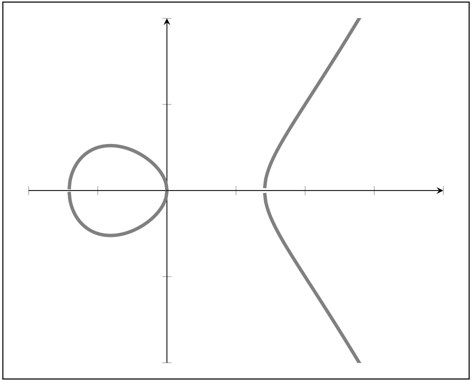
Example: E – elliptic curve, i.e. a smooth curve given by the equation

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Q}$$

along with a "point at infinity" $\mathcal{O}$.

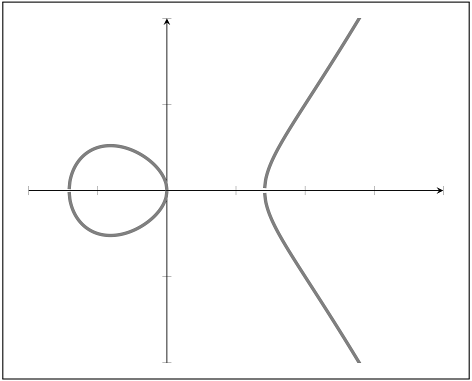


The set of real points on E, $E(\mathbb{R})$, (or complex, or rational, ...) on this curve has a structure of an abelian group:



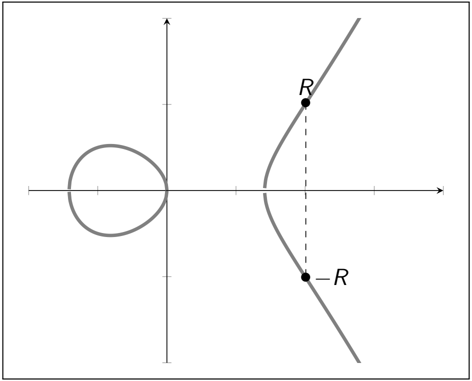
The set of real points on E, $E(\mathbb{R})$, (or complex, or rational, ...) on this curve has a structure of an abelian group:

- $\mathcal{O}$ – neutral element,



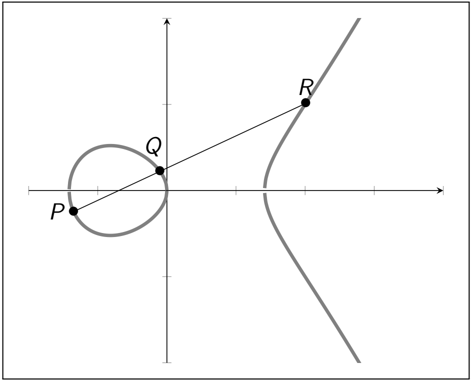
The set of real points on E, $E(\mathbb{R})$, (or complex, or rational, ...) on this curve has a structure of an abelian group:

- $\mathcal{O}$ – neutral element,
- the inverse point to $R = (x, y)$ is $-R := (x, -y)$,



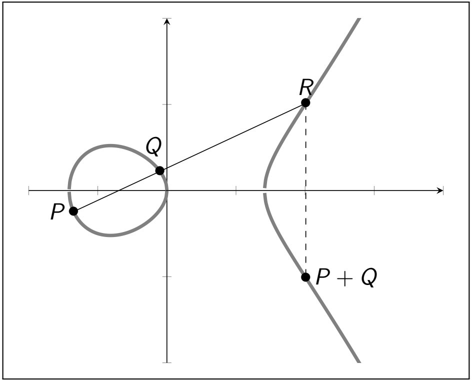
The set of real points on E, $E(\mathbb{R})$, (or complex, or rational, ...) on this curve has a structure of an abelian group:

- $\mathcal{O}$ – neutral element,
- the inverse point to $R = (x, y)$ is $\quad -R := (x, -y)$,
- $P + Q + R = \mathcal{O}$ iff P, Q, R are colinear.



The set of real points on E, $E(\mathbb{R})$, (or complex, or rational, ...) on this curve has a structure of an abelian group:

- $\mathcal{O}$ – neutral element,
- the inverse point to $R = (x, y)$ is $\quad -R := (x, -y)$,
- $P + Q + R = \mathcal{O}$ iff P, Q, R are colinear.



Algebraic formulas:

$$(x_1, y_1) + (x_2, y_2) := (x_3, y_3),$$

Algebraic formulas:

$$(x_1, y_1) + (x_2, y_2) := (x_3, y_3),$$

where:

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 &= \frac{y_2 - y_1}{x_2 - x_1} x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{aligned}$$

Is it possible to add points on other [a] curves?

[a] smooth projective

Is it possible to add points on other [a] curves?

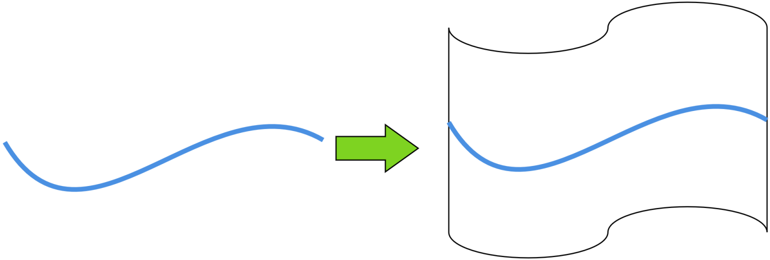
[a] smooth projective

Answer: No, ...

Is it possible to add points on other [a] curves?

[a] smooth projective

Answer: No, ... but any curve C can be embedded in an abelian variety $\mathrm{Jac}(C)$ (the **Jacobian** of C). The dimension of the Jacobian is the genus of the curve.



Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$a_0a_3 = a_1a_1 - a_5^2f_0 - a_3^2f_4 + 4a_4a_{13}f_0f_5 + a_5a_{10}f_1f_5 + 8a_4a_{10}f_1f_6 + a_3a_{10}(4f_2f_6 - f_3f_5) + 8a_4a_{11}f_0f_6 + 2a_{13}a_{15}f_0f_1f_5 + a_{10}a_{15}(4f_0f_2f_6 + 2f_0f_3f_5 + 3f_1^2f_6) + 4a_{11}a_{15}f_0f_1f_6 + 2a_{10}a_{13}(f_0f_5^2 + 3f_1f_3f_6) + 8a_{11}a_{13}f_0f_3f_6 + a_{10}^2(4f_1f_5f_6 + 4f_2f_4f_6 - f_2f_5^2 - f_3^2f_6) + a_{10}a_{11}(4f_0f_5f_6 + 4f_1f_4f_6 - f_1f_5^2) + a_{11}^2f_0(4f_4f_6 - f_5^2)$

$a_0a_4 = a_1a_2 + a_5a_{15}f_0f_3 + a_3a_{15}(9f_0f_5 + f_1f_4) + 2a_5a_{14}f_0f_4 + a_4a_{13}(20f_0f_6 + 3f_1f_5) + a_5a_{10}(7f_1f_6 + f_2f_5) + 4a_4a_{10}f_2f_6 + a_3a_{10}f_3f_6 + 4a_7a_9f_0f_5 + 4a_6a_9f_0f_6 - 4a_8^2f_0f_5 - 4a_7a_8f_0f_6 + 4a_6a_8f_1f_6 - 2a_7^2f_1f_6 + 4a_{15}^2f_0^2f_5 + 2a_{14}a_{15}f_0(2f_0f_6 + f_1f_5) + a_{13}a_{15}(14f_0f_1f_6 + 6f_0f_2f_5 + f_1^2f_5) + a_{13}a_{14}(8f_0f_2f_6 + 3f_0f_3f_5 - f_1^2f_6) + a_{10}a_{14}(8f_0f_4f_6 + f_0f_5^2 + 3f_1f_3f_6) + 2a_{13}^2(10f_0f_3f_6 + 2f_0f_4f_5 + 2f_1f_2f_6 + f_1f_3f_5) + a_{10}a_{13}(18f_0f_5f_6 + 6f_1f_4f_6 + f_1f_5^2 + 2f_2f_3f_6) + 4a_{12}a_{13}f_0f_3f_6 + 2a_{10}^2f_6(f_1f_6 + f_2f_5) + 2a_{10}a_{11}f_6(2f_0f_6 + f_1f_5) + 2a_{10}a_{12}f_0f_5f_6$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_0a_5 = a_2a_2 - a_5^2f_2 - a_3^2f_6 + a_5a_{15}(4f_0f_4 - f_1f_3) + a_3a_{15}f_1f_5 + 4a_5a_{14}f_0f_5 + 8a_4a_{14}f_0f_6 - 2a_3a_{14}f_1f_6 + 4a_4a_{12}f_1f_6 - 4a_6a_9f_1f_6 + 4a_7a_8f_1f_6 + a_{15}^2(4f_0f_2f_4 - f_0f_3^2 - f_1^2f_4) + a_{14}a_{15}f_5(4f_0f_2 - f_1^2) + 2a_{13}a_{15}(4f_0f_2f_6 + f_0f_3f_5 - 3f_1^2f_6) + a_{10}a_{15}(4f_0f_4f_6 - f_0f_5^2 - 4f_1f_3f_6) + 4a_{11}a_{15}f_6(2f_0f_3 - f_1f_2) + a_{12}a_{15}f_6(4f_0f_2 - f_1^2) + 4a_{10}a_{14}f_6(f_0f_5 - f_1f_4) - 4a_{10}a_{13}f_1f_5f_6 - 4a_{10}a_{11}f_1f_6^2$$

$$a_0a_6 = a_1a_3 - a_2a_{10}f_3 - a_3a_9f_1 + 4a_5a_8f_0 + 4a_4a_8f_1 + 2a_3a_8f_2 + 2a_3a_7f_3 + a_8a_{15}(4f_0f_2 + f_1^2) + 4a_7a_{15}f_0f_3 + 4a_6a_{15}f_0f_4 + 2a_8a_{13}(2f_0f_4 + f_1f_3) + 2a_7a_{13}(2f_0f_5 + f_1f_4) + 2a_6a_{13}(2f_0f_6 + f_1f_5) - 2a_9a_{10}f_0f_5 + 3a_8a_{10}f_1f_5 + 2a_6a_{11}f_1f_6 + 4a_7a_{12}f_0f_5 + 4a_6a_{12}f_0f_6$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_0a_7 = a_1a_4 + a_1a_{15}f_1 + a_5a_9f_0 - a_4a_6f_4 + a_7a_{14}(f_0f_5 - f_1f_4) - a_6a_{14}f_2f_4 + a_9a_{13}f_0f_4 + 2a_8a_{13}(-f_0f_5 + f_1f_4) + 2a_7a_{13}f_2f_4 + a_6a_{13}f_1f_6 - a_9a_{10}f_1f_5 + a_8a_{10}(-f_2f_5 + f_3f_4) + a_7a_{10}(-f_3f_5 + f_4^2) - a_6a_{10}f_3f_6 + a_9a_{12}f_0f_4 + a_8a_{12}(-f_0f_5 + f_1f_4) + a_7a_{12}f_2f_4$$

$$a_0a_8 = a_1a_5 + a_3a_7f_5 + 2a_3a_6f_6$$

$$a_0a_9 = a_2a_5 + a_4a_9f_3 + 3a_3a_8f_5 + 2a_5a_7f_4 + 4a_3a_7f_6 - a_8a_{15}f_2f_3 + a_7a_{15}(2f_1f_5 - f_3^2) + a_6a_{15}(2f_1f_6 - f_3f_4) + 4a_9a_{14}f_0f_5 - a_6a_{14}f_3f_5 - 4a_9a_{13}(-f_0f_6 - f_1f_5) + a_8a_{13}(4f_2f_5 - f_3f_4) + 2a_7a_{13}(2f_2f_6 + f_3f_5) + a_6a_{13}f_3f_6 + 4a_9a_{10}f_2f_6 + 4a_8a_{10}f_3f_6 + 2a_7a_{10}(2f_4f_6 - f_5^2) - 2a_6a_{10}f_5f_6 + 4a_9a_{11}f_1f_6 + 4a_9a_{12}f_0f_6 - a_6a_{12}f_3f_6$$

$$a_0a_{10} = a_3a_3$$

$$a_0a_{11} = 2a_3a_4 + a_3a_{15}f_1 + a_5a_{10}f_3 + a_3a_{10}f_5$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_0a_{12} = 2a_2a_7 + 2a_3a_{15}f_2 + a_5a_{14}f_1 + 2a_3a_{10}f_6 + 2a_4a_{12}f_3 - 2a_6a_9f_3 + 2a_7a_8f_3 + 4a_7^2f_4 + 4a_6a_7f_5 - a_{13}a_{15}f_1f_3 + a_{10}a_{15}(8f_0f_6 + f_1f_5 - 3f_3^2) + 2a_{11}a_{15}(f_0f_5 - f_2f_3) - 2a_{10}a_{13}f_3f_5 + 2a_{11}a_{13}(3f_1f_6 - f_3f_4) + 12a_{12}a_{13}f_0f_6 + a_{10}^2f_5^2 + 2a_{10}a_{11}f_3f_6 + 4a_{11}^2f_2f_6 + 4a_{11}a_{12}f_1f_6 + 4a_{12}^2f_0f_6$$

$$a_0a_{13} = a_3a_5$$

$$a_0a_{14} = 2a_4a_5 + a_5a_{15}f_1 + a_3a_{15}f_3 + a_5a_{10}f_5$$

$$a_0a_{15} = a_5a_5$$

$$a_2a_3 = a_0a_7 - 2a_5a_9f_0 - a_5a_8f_1$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_2a_4 = a_0a_8 - a_2a_{10}f_5 + a_4a_9f_2 - a_3a_6f_6 + a_9a_{15}f_0f_3 + a_8a_{15}(f_1f_3 - f_2^2) + a_7a_{15}(f_1f_4 - f_2f_3) + a_6a_{15}f_1f_5 - a_9a_{13}f_0f_5 - 2a_8a_{13}f_2f_4 + 2a_7a_{13}(f_1f_6 - f_2f_5) - a_6a_{13}f_2f_6 + a_9a_{11}f_2f_4 + a_8a_{11}(-f_1f_6 + f_2f_5) - a_8a_{12}f_2f_4 + a_7a_{12}(f_1f_6 - f_2f_5) - a_6a_{12}f_2f_6$$

$$a_2a_9 = a_0a_{15} + a_5a_{15}f_2 + a_4a_{15}f_3 + 2a_3a_{15}f_4 + 3a_4a_{13}f_5 + 3a_3a_{13}f_6 + a_3a_{12}f_6 + a_{15}^2f_1f_3 + a_{14}a_{15}f_1f_4 + a_{13}a_{15}(3f_1f_5 + 2f_2f_4) + 3a_{10}a_{15}f_3f_5 + a_{12}a_{15}f_1f_5 + a_{13}a_{14}(f_1f_6 + 2f_2f_5) + 2a_{11}a_{14}f_2f_6 + a_{12}a_{14}f_1f_6 + a_{10}a_{13}(2f_4f_6 + f_5^2) + 2a_{11}a_{13}f_3f_6$$

$$2a_2a_8 = a_0a_{14} - a_5a_{15}f_1 - a_5a_{13}f_3 + a_5a_{10}f_5 + 2a_3a_{11}f_6 - 2a_{15}^2f_0f_3 - 4a_{14}a_{15}f_0f_4 + 2a_{13}a_{15}(-3f_0f_5 - f_1f_4) - 4a_{11}a_{15}f_0f_6 - 4a_{12}a_{15}f_0f_5 - 2a_{13}a_{14}f_1f_5 - 4a_{12}a_{14}f_0f_6 - 4a_{13}^2f_1f_6 - 2a_{12}a_{13}f_1f_6$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$2a_2a_6 = a_0a_{11}+4a_5a_{14}f_0+3a_5a_{13}f_1+a_5a_{10}f_3-a_3a_{10}f_5+2a_5a_{11}f_2+a_5a_{12}f_1+a_{14}a_{15}(4f_0f_2-f_1^2)+6a_{13}a_{15}f_0f_3+a_{11}a_{15}(4f_0f_4+f_1f_3)+2a_{12}a_{15}f_0f_3+a_{10}a_{14}f_1f_5+2a_{13}^2(f_0f_5+f_1f_4)+2a_{12}a_{13}f_0f_5$

$a_1a_6 = a_0a_{10}+3a_5a_{13}f_0+3a_4a_{13}f_1+2a_5a_{10}f_2+a_4a_{10}f_3+a_3a_{10}f_4+a_5a_{12}f_0+a_{13}a_{15}(2f_0f_2+f_1^2)+3a_{10}a_{15}f_1f_3+2a_{13}a_{14}f_0f_3+2a_{11}a_{14}f_0f_4+a_{10}a_{13}(3f_1f_5+2f_2f_4)+a_{11}a_{13}(f_0f_5+2f_1f_4)+a_{10}^2f_3f_5+a_{10}a_{11}f_2f_5+a_{10}a_{12}f_1f_5+a_{11}a_{12}f_0f_5$

$2a_1a_7 = a_0a_{11}+a_3a_{15}f_1+2a_5a_{14}f_0-a_3a_{13}f_3-a_3a_{10}f_5-4a_{10}a_{14}f_0f_6-4a_{13}^2f_0f_5+2a_{10}a_{13}(-3f_1f_6-f_2f_5)-2a_{11}a_{13}f_1f_5-2a_{12}a_{13}f_0f_5-2a_{10}^2f_3f_6-4a_{10}a_{11}f_2f_6-4a_{10}a_{12}f_1f_6-4a_{11}a_{12}f_0f_6$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$2a_1a_8 = a_0a_{12} - 2a_5a_{15}f_0 - 2a_5a_{10}f_4 - a_3a_{11}f_5 - 2a_4a_{12}f_3 - 4a_8a_9f_1 + 2a_6a_9f_3 - 4a_8^2f_2 - 2a_7a_8f_3 - a_{15}^2f_1^2 - 2a_{14}a_{15}f_0f_3 + 2a_{13}a_{15}f_1f_3 + a_{10}a_{15}(-8f_0f_6 - f_1f_5 + 3f_3^2) - 4a_{14}^2f_0f_4 + 2a_{13}a_{14}(-3f_0f_5 + f_2f_3) + 2a_{10}a_{14}(-f_1f_6 + f_3f_4) - 4a_{12}a_{14}f_0f_5 + a_{10}a_{13}f_3f_5 - 12a_{12}a_{13}f_0f_6 - 4a_{12}^2f_0f_6$$

$$2a_1a_9 = a_0a_{14} - a_5a_{15}f_1 + a_3a_{15}f_3 + 2a_3a_{14}f_4 + 3a_3a_{13}f_5 + 4a_3a_{11}f_6 + a_3a_{12}f_5 + a_{11}a_{15}f_1f_5 + a_{10}a_{14}(4f_2f_6 + f_3f_5) + 2a_{13}^2(f_1f_6 + f_2f_5) + 6a_{10}a_{13}f_3f_6 + 2a_{12}a_{13}f_1f_6 + a_{10}a_{11}(4f_4f_6 - f_5^2) + 2a_{10}a_{12}f_3f_6$$

$$a_4a_4 = a_0a_{13} + a_5a_{13}f_2 + a_5a_{10}f_4 + a_3a_{10}f_6 + a_9^2f_0 + a_{13}a_{15}f_1f_3 + a_{10}a_{15}f_2f_4 + a_{11}a_{15}f_1f_4 + a_{10}a_{14}(f_1f_6 + f_2f_5) + a_{11}a_{14}f_1f_5 + a_{10}a_{13}(2f_2f_6 + f_3f_5) + a_{10}^2f_4f_6 + a_{10}a_{11}f_3f_6 + a_{10}a_{12}f_2f_6 + a_{11}a_{12}f_1f_6$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_0a_{12} = 2a_0a_{13} + 4a_5a_{15}f_0 + 2a_5a_{14}f_1 + 4a_5a_{13}f_2 + 4a_5a_{10}f_4 + 4a_4a_{10}f_5 + 4a_3a_{10}f_6 + 2a_5a_{11}f_3 + a_{15}^2(4f_0f_2 - f_1^2) + 4a_{14}a_{15}f_0f_3 + 2a_{13}a_{15}(4f_0f_4 + f_1f_3) + a_{10}a_{15}(4f_2f_4 - f_3^2) + 4a_{11}a_{15}f_1f_4 + 4a_{12}a_{15}f_0f_4 + 4a_{13}a_{14}f_0f_5 + 4a_{10}a_{14}(f_1f_6 + f_2f_5) + 4a_{12}a_{14}f_0f_5 + 4a_{13}^2(f_0f_6 + 2f_1f_5) + 4a_{10}a_{13}(2f_2f_6 + f_3f_5) + 4a_{12}a_{13}(2f_0f_6 + f_1f_5) + a_{10}^2(4f_4f_6 + f_5^2) + 4a_{10}a_{11}f_3f_6 + 4a_{10}a_{12}f_2f_6 + 4a_{11}a_{12}f_1f_6 + 4a_{12}^2f_0f_6$$

$$a_2a_{15} = a_5a_9 - a_8a_{15}f_3 - 2a_7a_{15}f_4 - 2a_6a_{15}f_5 - 2a_6a_{14}f_6 - a_8a_{13}f_5$$
$$a_2a_{14} = 2a_5a_8 + a_9a_{15}f_1 + 2a_8a_{15}f_2 + a_7a_{15}f_3 - a_7a_{13}f_5 - 2a_6a_{13}f_6$$

$$a_2a_{13} = a_5a_7 - 2a_9a_{15}f_0 - a_8a_{15}f_1$$

$$a_2a_{10} = a_3a_7 - 2a_9a_{13}f_0 - a_8a_{13}f_1$$

$$a_2a_{11} = 2a_3a_8 + a_9a_{13}f_1 + 2a_8a_{13}f_2 + a_7a_{13}f_3 - a_7a_{10}f_5 - 2a_6a_{10}f_6$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_2a_{12} = 2a_5a_7 + 2a_7a_{15}f_2 + a_6a_{15}f_3 + a_9a_{14}f_1 + 2a_9a_{13}f_2 + 3a_8a_{13}f_3 + 4a_7a_{13}f_4 + 3a_6a_{13}f_5 + a_8a_{10}f_5 + 2a_6a_{11}f_6$$

$$a_1a_{10} = a_3a_6 - a_7a_{13}f_1 - 2a_9a_{10}f_1 - 2a_8a_{10}f_2 - a_7a_{10}f_3 - 2a_9a_{11}f_0$$

$$a_1a_{11} = 2a_3a_7 - 2a_9a_{13}f_0 - a_8a_{13}f_1 + a_8a_{10}f_3 + 2a_7a_{10}f_4 + a_6a_{10}f_5$$

$$a_1a_{13} = a_3a_8 - a_7a_{10}f_5 - 2a_6a_{10}f_6$$

$$a_1a_{15} = a_5a_8 - a_7a_{13}f_5 - 2a_6a_{13}f_6$$

$$a_1a_{14} = 2a_5a_7 - 2a_9a_{15}f_0 - a_8a_{15}f_1 + a_8a_{13}f_3 + 2a_7a_{13}f_4 + a_6a_{13}f_5$$

$$a_1a_{12} = 2a_3a_8 + a_7a_{15}f_1 + 2a_9a_{14}f_0 + 3a_9a_{13}f_1 + 4a_8a_{13}f_2 + 3a_7a_{13}f_3 + 2a_6a_{13}f_4 + a_9a_{10}f_3 + 2a_8a_{10}f_4 + a_6a_{11}f_5$$

Example: Jacobian of the curve

$$Y^2 = f_6 X^6 + f_5 X^5 + f_4 X^4 + f_3 X^3 + f_2 X^2 + f_1 X + f_0$$

is given by an intersection of n quadratic forms:

$$a_5a_8 = a_4a_9 - a_8a_{15}f_2 - a_7a_{15}f_3 - a_6a_{15}f_4 - a_6a_{14}f_5 - a_8a_{13}f_4 - a_6a_{13}f_6 - a_6a_{12}f_6$$

$$a_5a_7 = a_4a_8 + a_9a_{15}f_0 + a_8a_{15}f_1 - a_7a_{13}f_4 - a_6a_{13}f_5 - a_6a_{11}f_6$$

$$a_5a_6 = a_4a_7 + a_7a_{15}f_1 + a_9a_{14}f_0 + a_9a_{13}f_1 + a_8a_{13}f_2 + a_7a_{13}f_3 - a_6a_{10}f_6$$

$$a_3a_7 = a_4a_6 - a_9a_{13}f_0 - a_7a_{13}f_2 - a_9a_{10}f_2 - a_8a_{10}f_3 - a_7a_{10}f_4 - a_9a_{11}f_1 - a_9a_{12}f_0$$

$$a_3a_8 = a_4a_7 - a_9a_{14}f_0 - a_9a_{13}f_1 - a_8a_{13}f_2 + a_7a_{10}f_5 + a_6a_{10}f_6$$

$$a_3a_9 = a_4a_8 - a_9a_{15}f_0 + a_8a_{13}f_3 + a_7a_{13}f_4 + a_6a_{13}f_5 + a_8a_{10}f_5 + a_6a_{11}f_6$$

$$a_5a_{15} = a_9^2 - a_{15}^2f_2 - a_{14}a_{15}f_3 - a_{10}a_{15}f_6 - a_{14}^2f_4 - a_{13}a_{14}f_5 - a_{12}a_{14}f_5 - 2a_{12}a_{13}f_6 - a_{12}^2f_6$$

$$a_5a_{14} = 2a_8a_9 + a_{15}^2f_1 - a_{13}a_{15}f_3 - 2a_{13}a_{14}f_4 - 2a_{10}a_{14}f_6 - 3a_{13}^2f_5 - 2a_{12}a_{13}f_5 - 2a_{11}a_{12}f_6$$

$$a_5a_{13} = a_8^2 - a_{15}^2f_0 - a_{13}^2f_4 - 2a_{10}a_{13}f_6 - a_{11}a_{13}f_5 - a_{10}a_{12}f_6$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_5a_{10} = a_7^2 - 2a_{13}a_{15}f_0 - a_{10}a_{15}f_2 - a_{11}a_{15}f_1 - a_{12}a_{15}f_0 - a_{10}^2f_6$$

$$a_5a_{11} = 2a_7a_8 - 2a_{14}a_{15}f_0 - a_{13}a_{15}f_1 + a_{10}a_{15}f_3 - a_{10}a_{13}f_5 - 2a_{10}a_{11}f_6$$

$$a_5a_{12} = 2a_7a_9 + a_{14}a_{15}f_1 + 2a_{13}a_{15}f_2 + a_{11}a_{15}f_3 - a_{10}a_{14}f_5 - 2a_{10}a_{13}f_6 - 2a_{10}a_{12}f_6$$

$$a_4a_{15} = a_8a_9 - a_{13}a_{15}f_3 - a_{11}a_{15}f_4 - a_{10}a_{14}f_6 - 2a_{13}^2f_5 - a_{12}a_{13}f_5 - a_{11}a_{12}f_6$$

$$a_4a_{14} = a_7a_9 + a_8^2 - a_{15}^2f_0 + a_{13}a_{15}f_2 - a_{10}a_{15}f_4 - 3a_{10}a_{13}f_6 - 2a_{11}a_{13}f_5 - 2a_{10}a_{12}f_6$$

$$a_4a_{13} = a_7a_8 - a_{14}a_{15}f_0 - a_{13}a_{15}f_1 - a_{10}a_{13}f_5 - a_{10}a_{11}f_6$$

$$a_3a_{10} = a_6^2 - a_{10}a_{15}f_0 - a_{11}a_{13}f_1 - 2a_{12}a_{13}f_0 - a_{10}^2f_4 - a_{10}a_{11}f_3 - a_{11}^2f_2 - a_{11}a_{12}f_1 - a_{12}^2f_0$$

$$a_3a_{11} = 2a_6a_7 - 2a_{11}a_{15}f_0 - 2a_{12}a_{14}f_0 - 3a_{13}^2f_1 - a_{10}a_{13}f_3 - 2a_{11}a_{13}f_2 - 2a_{12}a_{13}f_1 + a_{10}^2f_5$$

$$a_3a_{13} = a_7^2 - 2a_{13}a_{15}f_0 - a_{12}a_{15}f_0 - a_{13}a_{14}f_1 - a_{13}^2f_2 - a_{10}^2f_6$$

$$a_3a_{15} = a_8^2 - a_{15}^2f_0 - a_{10}a_{15}f_4 - a_{10}a_{14}f_5 - 2a_{10}a_{13}f_6 - a_{10}a_{12}f_6$$

$$a_3a_{14} = 2a_7a_8 - 2a_{14}a_{15}f_0 - a_{13}a_{15}f_1 + a_{10}a_{15}f_3 - a_{10}a_{13}f_5 - 2a_{10}a_{11}f_6$$

$$a_3a_{12} = 2a_6a_8 - 2a_{13}a_{15}f_0 - a_{11}a_{15}f_1 - 2a_{12}a_{15}f_0 + a_{10}a_{14}f_3 + 2a_{10}a_{13}f_4 + a_{10}a_{11}f_5$$

Example: Jacobian of the curve

$$Y^2 = f_6 X^6 + f_5 X^5 + f_4 X^4 + f_3 X^3 + f_2 X^2 + f_1 X + f_0$$

is given by an intersection of n quadratic forms:

$$a_4 a_{10} = a_6 a_7 - a_{11} a_{15} f_0 - a_{10} a_{14} f_2 - a_{12} a_{14} f_0 - 2a_{13}^2 f_1 - a_{10} a_{13} f_3 - a_{12} a_{13} f_1$$

$$a_4 a_{11} = a_6 a_8 + a_7^2 - 3a_{13} a_{15} f_0 - a_{10} a_{15} f_2 - 2a_{12} a_{15} f_0 - 2a_{13} a_{14} f_1 + a_{10} a_{13} f_4 - a_{10}^2 f_6$$

$$a_4 a_{12} = a_6 a_9 + a_7 a_8 - a_{14} a_{15} f_0 + 2a_{10} a_{15} f_3 + a_{11} a_{15} f_2 + a_{11} a_{13} f_4 - a_{10} a_{11} f_6$$

$$a_6 a_{14} = 2a_7 a_{13} - a_8 a_{11} + a_7 a_{12}$$

$$a_9 a_{11} = -a_7 a_{14} + 2a_8 a_{13} + a_8 a_{12}$$

$$a_9 a_{13} = -a_7 a_{15} + a_8 a_{14}$$

$$a_8 a_{13} = -a_6 a_{15} + a_7 a_{14}$$

$$a_7 a_{13} = -a_9 a_{10} + a_8 a_{11}$$

$$a_6 a_{13} = -a_8 a_{10} + a_7 a_{11}$$

$$a_{14} a_{14} = 2a_{13} a_{15} + a_{12} a_{15}$$

$$a_{13} a_{13} = a_{10} a_{15}$$

$$a_{11} a_{11} = 2a_{10} a_{13} + a_{10} a_{12}$$

$$a_{12} a_{13} = -2a_{10} a_{15} + a_{11} a_{14}$$

$$a_{11} a_{15} = a_{13} a_{14}$$

$$a_{10} a_{14} = a_{11} a_{13}.$$

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of n quadratic forms:

$$a_4a_{10} = a_6a_7 - a_{11}a_{15}f_0 - a_{10}a_{14}f_2 - a_{12}a_{14}f_0 - 2a_{13}^2f_1 - a_{10}a_{13}f_3 - a_{12}a_{13}f_1$$

$$a_4a_{11} = a_6a_8 + a_7^2 - 3a_{13}a_{15}f_0 - a_{10}a_{15}f_2 - 2a_{12}a_{15}f_0 - 2a_{13}a_{14}f_1 + a_{10}a_{13}f_4 - a_{10}^2f_6$$

$$a_4a_{12} = a_6a_9 + a_7a_8 - a_{14}a_{15}f_0 + 2a_{10}a_{15}f_3 + a_{11}a_{15}f_2 + a_{11}a_{13}f_4 - a_{10}a_{11}f_6$$

$$a_6a_{14} = 2a_7a_{13} - a_8a_{11} + a_7a_{12}$$

$$a_9a_{11} = -a_7a_{14} + 2a_8a_{13} + a_8a_{12}$$

$$a_9a_{13} = -a_7a_{15} + a_8a_{14}$$

$$a_8a_{13} = -a_6a_{15} + a_7a_{14}$$

$$a_7a_{13} = -a_9a_{10} + a_8a_{11}$$

$$a_6a_{13} = -a_8a_{10} + a_7a_{11}$$

$$a_{14}a_{14} = 2a_{13}a_{15} + a_{12}a_{15}$$

$$a_{13}a_{13} = a_{10}a_{15}$$

$$a_{11}a_{11} = 2a_{10}a_{13} + a_{10}a_{12}$$

$$a_{12}a_{13} = -2a_{10}a_{15} + a_{11}a_{14}$$

$$a_{11}a_{15} = a_{13}a_{14}$$

$$a_{10}a_{14} = a_{11}a_{13}.$$

where $n = 72$.

Example: Jacobian of the curve

$$Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$$

is given by an intersection of 72 quadratic forms.

How to work with Jacobians?

$$\mathrm{Jac}(C) \cong Pic^0(C) = \frac{\text{divisors (formal sums of points) of degree 0}}{\text{divisors of functions}}$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\mathrm{n}} = \mathcal{O}\}$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(A[n]) \cong \mathrm{Gl}_{2g}(\mathbb{Z}/n).$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \qquad \underbrace{P + P + \ldots + P}_{\mathrm{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

$$im\, \rho_{\ell^\infty} = ?$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

$$(im\, \rho_{\ell^\infty})^{Zar}$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\mathrm{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

$$(im\, \rho_{\ell^\infty})^{Zar,o}$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

$$(im\, \rho_{\ell^\infty})^{Zar,o} \cong MT(A) \otimes \mathbb{Q}_\ell.$$

n-torsion on an abelian variety A:

$$A[n] = \{P \in A(\overline{\mathbb{Q}}) : \quad \underbrace{P + P + \ldots + P}_{\text{n}} = \mathcal{O}\} \cong (\mathbb{Z}/n)^{2g}.$$

„Rationality" of torsion points is encoded by the Galois representation:

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{Gl}_{2g}(\mathbb{Z}_\ell).$$

Why study the torsion?

- interesting extensions (inverse Galois problem, class numbers),
- interesting representations (Last Fermat's Theorem, modularity).

What is the image of the representation?

Conjecture (Mumford–Tate)

$$(im\, \rho_{\ell^\infty})^{Zar,o} \cong MT(A) \otimes \mathbb{Q}_\ell.$$

– a bridge between the Hodge and Tate conjectures for abelian varieties.

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

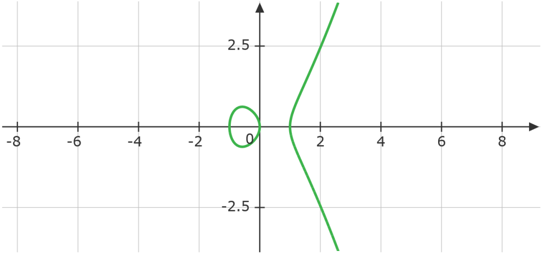
Example: $\ell = 2$, $f = x^3 + Ax + B$

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

Example: $\ell = 2,\ f = x^3 + Ax + B$

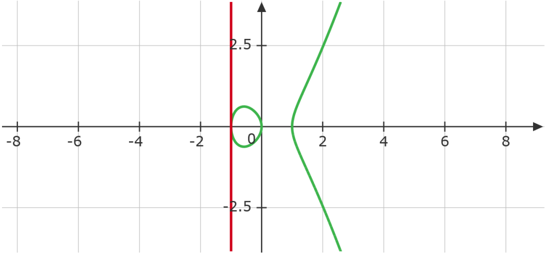


The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

Example: $\ell = 2$, $f = x^3 + Ax + B$

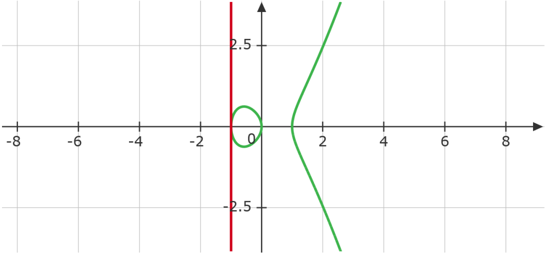


The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

Example: $\ell = 2,\ f = x^3 + Ax + B$



$$E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\},$$

where x_1, x_2, x_3 – zeroes of $x^3 + Ax + B$.

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

A more general case: Let $r := \deg f$, where $2\ell \nmid r$.
Then $\dim \mathrm{Jac}(C) = \frac{1}{2}(\ell - 1)(r - 1)$.

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

A more general case: Let $r := \deg f$, where $2\ell \nmid r$.
Then $\dim \mathrm{Jac}(C) = \frac{1}{2}(\ell - 1)(r - 1)$.

If $f(\alpha) = 0$, then in the group of the divisors:

$$\ell \cdot ((\alpha, 0) - \infty) = \mathrm{div}(x - \alpha),$$

The main question

What is the ℓ-torsion and the image of ρ_{ℓ^∞} for $\mathrm{Jac}(C)$, where

$$C : y^\ell = f(x) \quad ?$$

A more general case: Let $r := \deg f$, where $2\ell \nmid r$.
Then $\dim \mathrm{Jac}(C) = \frac{1}{2}(\ell - 1)(r - 1)$.

If $f(\alpha) = 0$, then in the group of the divisors:

$$\ell \cdot ((\alpha, 0) - \infty) = \mathrm{div}(x - \alpha),$$

so that

$$(\alpha, 0) - \infty \in \mathrm{Jac}(C)[\ell].$$

If $\ell = 2$, we obtain the whole ℓ-torsion. How about $\ell > 2$?

$$\mathrm{im}\, \rho_{\ell^\infty} \subset \mathrm{Gl}_{2g}(\mathbb{Z}_\ell)$$

What constraints does $\mathrm{im}\, \rho_{\ell^\infty}$ satisfy?

$$\operatorname{im} \rho_{\ell^\infty} \subset \mathrm{Gl}_{2(r-1)}(\mathcal{O}_\ell)$$

What constraints does $\operatorname{im} \rho_{\ell^\infty}$ satisfy?

- we have an action of μ_ℓ on $C : y^\ell = f(x)$ given by:

$$(x, y) \mapsto (x, \zeta_\ell \cdot y).$$

  Thus on $\mathrm{Jac}(C)$ we have an action of $\mathcal{O} := \mathbb{Z}[\zeta_\ell]$ and on ℓ^∞-torsion the action of $\mathcal{O}_\ell := \mathbb{Z}_\ell[\zeta_\ell]$.

$$\operatorname{im}\rho_{\ell^\infty} \subset \mathrm{GU}_{2(r-1)}(\mathcal{O}_\ell)$$

What constraints does $\operatorname{im}\rho_{\ell^\infty}$ satisfy?

- we have an action of μ_ℓ on $C : y^\ell = f(x)$ given by:

$$(x, y) \mapsto (x, \zeta_\ell \cdot y).$$

  Thus on $\mathrm{Jac}(C)$ we have an action of $\mathcal{O} := \mathbb{Z}[\zeta_\ell]$ and on ℓ^∞-torsion the action of $\mathcal{O}_\ell := \mathbb{Z}_\ell[\zeta_\ell]$.
- the action of the Galois group preserves a unitary form (Weil pairing),

$$\operatorname{im} \rho_{\ell^\infty} \subset \mathrm{GU}_{2(r-1)}(\mathcal{O}_\ell)^{\mathsf{Gal}(f)}$$

What constraints does $\operatorname{im} \rho_{\ell^\infty}$ satisfy?

- we have an action of μ_ℓ on $C : y^\ell = f(x)$ given by:

$$(x, y) \mapsto (x, \zeta_\ell \cdot y).$$

  Thus on $\mathsf{Jac}(C)$ we have an action of $\mathcal{O} := \mathbb{Z}[\zeta_\ell]$ and on ℓ^∞-torsion the action of $\mathcal{O}_\ell := \mathbb{Z}_\ell[\zeta_\ell]$.
- the action of the Galois group preserves a unitary form (Weil pairing),
- on λ-torsion (where $\lambda := 1 - \zeta_\ell$) the Galois group is $\mathsf{Gal}(f)$.

$$\operatorname{im} \rho_{\ell^\infty} \subset \mathrm{GU}_{2(r-1)}(\mathcal{O}_\ell)^{\mathsf{Gal}(f)}_{\mathsf{det} \in \mathcal{D}_J}$$

What constraints does $\operatorname{im} \rho_{\ell^\infty}$ satisfy?

- we have an action of μ_ℓ on $C : y^\ell = f(x)$ given by:

$$(x, y) \mapsto (x, \zeta_\ell \cdot y).$$

  Thus on Jac(C) we have an action of $\mathcal{O} := \mathbb{Z}[\zeta_\ell]$ and on ℓ^∞-torsion the action of $\mathcal{O}_\ell := \mathbb{Z}_\ell[\zeta_\ell]$.
- the action of the Galois group preserves a unitary form (Weil pairing),
- on λ-torsion (where $\lambda := 1 - \zeta_\ell$) the Galois group is Gal(f).
- condition on the determinants of ρ_{ℓ^∞}.

$$\operatorname{im} \rho_{\ell^\infty} \subset \mathrm{GU}_{2(r-1)}(\mathcal{O}_\ell)^{\mathsf{Gal}(f)}_{\det \in \mathcal{D}_J} \qquad (*)$$

What constraints does $\operatorname{im} \rho_{\ell^\infty}$ satisfy?

- we have an action of μ_ℓ on $C : y^\ell = f(x)$ given by:

$$(x, y) \mapsto (x, \zeta_\ell \cdot y).$$

  Thus on $\mathrm{Jac}(C)$ we have an action of $\mathcal{O} := \mathbb{Z}[\zeta_\ell]$ and on ℓ^∞-torsion the action of $\mathcal{O}_\ell := \mathbb{Z}_\ell[\zeta_\ell]$.
- the action of the Galois group preserves a unitary form (Weil pairing),
- on λ-torsion (where $\lambda := 1 - \zeta_\ell$) the Galois group is $\mathrm{Gal}(f)$.
- condition on the determinants of ρ_{ℓ^∞}.

Theorem (JG)

If $\mathrm{Gal}(f) = S_r$ and there exists a prime ideal $\mathfrak{p}$ in $\mathcal{O}$ such that $\mathrm{ord}_{\mathfrak{p}}(disc(f)) = 1$, then $(*)$ is an equality!

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{O}_\ell^\times$?

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{O}_\ell^\times$?

- the „natural candidate” for the image:

$$\{d \in \mathcal{O}_\ell^\times : d \cdot \overline{d} \in 1 + \ell \cdot (r-1)\mathbb{Z}_\ell\}$$

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} \to \mathcal{O}_\ell^\times$?

- the „natural candidate" for the image:

$$\{d \in \mathcal{O}_\ell^\times : d \cdot \overline{d} \in 1 + \ell \cdot (r-1)\mathbb{Z}_\ell\}$$

- class field theory:
  - $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} \approx \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times$, where $\mathbb{I}_{\mathbb{Q}} := \prod'_{p \le \infty} \mathbb{Q}_p^\times$,
  - $\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ comes from the Hecke character

$$\chi : \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times \to \mathbb{Q}(\zeta_\ell)^\times,$$

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

- the „natural candidate" for the image:

$$\{d \in \mathcal{O}_\ell^\times : d \cdot \overline{d} \in 1 + \ell \cdot (r-1)\mathbb{Z}_\ell\}$$

- class field theory:
  - $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell)) \approx \mathbb{I}_{\mathbb{Q}(\zeta_\ell)}/\mathbb{Q}(\zeta_\ell)^\times$, where $\mathbb{I}_{\mathbb{Q}(\zeta_\ell)} := \prod'_{\mathfrak{p} \leq \infty} \mathbb{Q}(\zeta_\ell)_{\mathfrak{p}}^\times$,
  - $\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ comes from the Hecke character

$$\chi : \mathbb{I}_{\mathbb{Q}(\zeta_\ell)}/\mathbb{Q}(\zeta_\ell)^\times \to \mathbb{Q}(\zeta_\ell)^\times,$$

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

- the „natural candidate" for the image:

$$\{d \in \mathcal{O}_\ell^\times : d \cdot \overline{d} \in 1 + \ell \cdot (r-1)\mathbb{Z}_\ell\}$$

- class field theory:
  - $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell)) \approx \mathbb{I}_{\mathbb{Q}(\zeta_\ell)}/\mathbb{Q}(\zeta_\ell)^\times$, where $\mathbb{I}_{\mathbb{Q}(\zeta_\ell)} := \prod'_{\mathfrak{p} \le \infty} \mathbb{Q}(\zeta_\ell)_{\mathfrak{p}}^\times$,
  - $\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ comes from the Hecke character

$$\chi : \mathbb{I}_{\mathbb{Q}(\zeta_\ell)}/\mathbb{Q}(\zeta_\ell)^\times \to \mathbb{Q}(\zeta_\ell)^\times,$$

- the „infinity type" χ is determined by $\mu_\ell \circlearrowleft H^0(\Omega_C)$, and equal to:

$$\prod_{j=1}^{\ell-1} \sigma_j^{\lfloor \frac{r \cdot j}{\ell} \rfloor}$$

where $\sigma_j(\zeta_\ell) := \zeta_\ell^j$.

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

- „linear algebra”:

$\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ has a finite index in the "natural candidate" iff $\det M_{\ell,r} \neq 0$.

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

- „linear algebra":

$\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ has a finite index in the "natural candidate" iff $\det M_{\ell,r} \neq 0$.

- Hirabayashi formula for the determinant of $M_{\ell,r}$ (Demjanenko, '98)

$$\det M_{\ell,r} = \frac{(-1)^{\frac{\ell-1}{2}} \cdot h_\ell^-}{2\ell} \cdot (r^{r_\ell} - 1)^{\frac{\ell-1}{2r_\ell}},$$

where:

- h_ℓ^- is the relative class number of $\mathbb{Q}(\zeta_\ell)$,
- r_ℓ is the multiplicative order of r mod ℓ.

Question

What can be said about the image of $\det_{\mathcal{O}} \circ \rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))^{ab} \to \mathcal{O}_\ell^\times$?

- „linear algebra":

$\det_{\mathcal{O}} \circ \rho_{\ell^\infty}$ has a finite index in the "natural candidate" iff $\det M_{\ell,r} \neq 0$.

- Hirabayashi formula for the determinant of $M_{\ell,r}$ (Demjanenko, '98)

$$\det M_{\ell,r} = \frac{(-1)^{\frac{\ell-1}{2}} \cdot h_\ell^-}{2\ell} \cdot (r^{r_\ell} - 1)^{\frac{\ell-1}{2r_\ell}},$$

where:

- h_ℓ^- is the relative class number of $\mathbb{Q}(\zeta_\ell)$,
- r_ℓ is the multiplicative order of r mod ℓ.

Corollary (JG)

Under the assumptions of the Theorem, the MT conjecture (and Hodge and Tate's) holds for $\mathrm{Jac}(C)$*!*

About the proof

About the proof

- a lifting result:

  (Serre, ...) if $G \subset \mathrm{Gl}_r(\mathbb{Z}_\ell)$ is a closed subgroup and

  $$G \pmod{\ell} = \mathrm{Gl}_r(\mathbb{Z}/\ell),$$

  then $G = \mathrm{Gl}_r(\mathbb{Z}_\ell)$.

About the proof

- a lifting result:

  (JG) if $G \subset \mathrm{GU}_r(\mathcal{O}_\ell)$ is a closed subgroup and

$$G \pmod{\ell} = \mathrm{GU}_r(\mathcal{O}_\ell/\ell),$$

  then $G = \mathrm{GU}_r(\mathcal{O}_\ell)$.

About the proof

- a lifting result:

  (JG) if $G \subset \mathrm{GU}_r(\mathcal{O}_\ell)$ is a closed subgroup and

  $$G \pmod{\lambda} = \mathrm{GU}_r(\mathcal{O}_\ell/\lambda),$$

  to $G = \mathrm{GU}_r(\mathcal{O}_\ell)$.

About the proof

- a lifting result:

  (JG) if $G \subset \mathrm{GU}_r(\mathcal{O}_\ell)$ is a closed subgroup and

  $$G \pmod{\lambda^2} = \mathrm{GU}_r(\mathcal{O}_\ell/\lambda^2),$$

  to $G = \mathrm{GU}_r(\mathcal{O}_\ell)$.

About the proof

- a lifting result:

  (JG) if $G \subset \mathrm{GU}_r(\mathcal{O}_\ell)$ is a closed subgroup and
  $$G \pmod{\lambda^2} = \mathrm{GU}_r(\mathcal{O}_\ell/\lambda^2),$$
  to $G = \mathrm{GU}_r(\mathcal{O}_\ell)$.

- „descent theory": the description of $\mathbb{Q}(\mathrm{Jac}(C)[\lambda^2])$, i.e.
  $$\mathbb{Q}(\zeta_\ell, \mathrm{Jac}(C)[\lambda^2]) = \mathbb{Q}(\zeta_\ell, \alpha_1, \ldots, \alpha_r, \sqrt[\ell]{\alpha_i - \alpha_j} : i \neq j),$$
  where $\alpha_1, \ldots, \alpha_r$ – roots of f.

Thank you for your attention!

Other remarks

Other remarks

- Hodge group (the special Mumford–Tate group):

$$U(H_1(\mathrm{Jac}(C), \mathbb{Q}), \Psi)$$

Other remarks

- Hodge group (the special Mumford–Tate group):

$$U(H_1(\mathrm{Jac}(C), \mathbb{Q}), \Psi)$$

- from the proof of the MT conjecture in this case it follows that

$$\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}[\zeta_\ell],$$

Other remarks

- Hodge group (the special Mumford–Tate group):

$$U(H_1(\mathrm{Jac}(C), \mathbb{Q}), \Psi)$$

- from the proof of the MT conjecture in this case it follows that

$$\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}[\zeta_\ell],$$

- Hodge conjecture:

Theorem (Ribet)

If $E := \mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q}$ *is a commutative field and*

$$MT(\mathrm{Jac}(C)) = U(H_1(\mathrm{Jac}(C), \mathbb{Q}), \Psi),$$

then $\mathrm{Jac}(C)$ *satisfies criterion (1,1) (i.e. all classes Hodge's are derived from divisors). In particular, it satisfies the Hodge conjecture!*