# Nontrivial Sha for curves of genus 2 arising from K3 surfaces

Ronald van Luijk
MSRI, Berkeley

Joint work with

Adam Logan
Waterloo, Canada

May 4, 2006
San Diego

## The entire talk on one page

**Theorem 1.** *Let $S$ be the set of primes that split completely in*

$$F = \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{-3(1+\sqrt{2})}, \sqrt{6(1+\sqrt{5})}\right).$$

*Then for all $n$ that are products of elements in $S$, the 2-part of the Tate-Shafarevich group of the Jacobian of the curve*

$$C_n\colon\ y^2 = -6n(x^2+1)(x^2-2x-1)(x^2+x-1)$$

*is nontrivial.*

**Proof in short:**
We take a specific principal homogeneous space of the Jacobian of $C_n$ that is everywhere locally solvable and show that it does not have any rational points by viewing it as a double cover of a K3 surface on which rational points do not exist due to a Brauer-Manin obstruction.

## Goal of this talk:

Understand previous page and why we care.

## Main ingredients:

(a) 2-descent on Jacobians

(b) Brauer-Manin obstruction to the existence of rational points

Let $C$ be a smooth, geom. irred. curve of genus 2 over a #-field $K$.

**Faltings:** The set $C(K)$ of rational points is finite.

Let $C$ be a smooth, geom. irred. curve of genus 2 over a #-field $K$.

**Faltings:** The set $C(K)$ of rational points is finite.

Many known methods to find $C(K)$ (in special cases) require knowing the Mordell-Weil group $J(K)$ of rational points on the Jacobian $J$ of $C$.

**Mordell-Weil Theorem:**
$J(K)$ is finitely generated, i.e., $J(K) \cong J(K)_{\mathsf{tors}} \oplus \mathbb{Z}^r$.

Let $C$ be a smooth, geom. irred. curve of genus 2 over a #-field $K$.

**Faltings:** The set $C(K)$ of rational points is finite.

Many known methods to find $C(K)$ (in special cases) require knowing the Mordell-Weil group $J(K)$ of rational points on the Jacobian $J$ of $C$.

**Mordell-Weil Theorem:**
$J(K)$ is finitely generated, i.e., $J(K) \cong J(K)_{\text{tors}} \oplus \mathbb{Z}^r$.

$$\boxed{\begin{array}{l} J(K)_{\text{tors}} \\ J(K)/2J(K) \end{array}} \Longrightarrow \boxed{\begin{array}{l} J(K)_{\text{tors}} \\ r = \text{rank}\, J(K) \end{array}} \Longrightarrow \boxed{\begin{array}{l} J(K) \\ \text{computable} \end{array}}$$

$J(K)_{\text{tors}}$ is easy to find, so what remains is computing $J(K)/2J(K)$.

There are cohomologically defined finite groups

$$\begin{array}{ll} \mathrm{Sel}^{(2)}(K,J), & \text{the 2-Selmer group,} \\ Ш(K,J), & \text{the Shafarevich-Tate group,} \end{array}$$

with

$$0 \to J(K)/2J(K) \to \mathrm{Sel}^{(2)}(K,J) \to Ш(K,J)[2] \to 0.$$

**2-descent:** compute $\mathrm{Sel}^{(2)}(K,J)$ and decide which of its elements come from $J(K)/2J(K)$ (i.e., map to 0).

There are cohomologically defined finite groups

$$\begin{array}{ll} \mathrm{Sel}^{(2)}(K,J), & \text{the 2-Selmer group,} \\ Ш(K,J), & \text{the Shafarevich-Tate group,} \end{array}$$

with

$$0 \to J(K)/2J(K) \to \mathrm{Sel}^{(2)}(K,J) \to Ш(K,J)[2] \to 0.$$

**2-descent:** compute $\mathrm{Sel}^{(2)}(K,J)$ and decide which of its elements come from $J(K)/2J(K)$ (i.e., map to 0).

**Assumption:** We can compute $\mathrm{Sel}^{(2)}(K,J)$.

**Remaining goal:** Which elements of $\mathrm{Sel}^{(2)}(K,J)$ map to 0?

**Element of** $\text{Sel}^{(2)}(K, J)$: a twist $\pi\colon Y \to J$ of the map $[2]\colon J \to J$ (over $\overline{K}$ there is an isomorphism $\sigma$ such that

$$\begin{array}{ccc} Y_{\overline{K}} & \overset{\cong}{\underset{\sigma}{\dashrightarrow}} & J_{\overline{K}} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle [2]} \\ J_{\overline{K}} & = & J_{\overline{K}} \end{array}$$

commutes), where $Y$ is locally soluble everywhere.

The element $Y \to J$ maps to 0 in $Ш(K, J)[2]$ iff $Y(K) \neq \emptyset$.

**Element of** $\text{Sel}^{(2)}(K, J)$: a twist $\pi\colon Y \to J$ of the map $[2]\colon J \to J$ (over $\overline{K}$ there is an isomorphism $\sigma$ such that

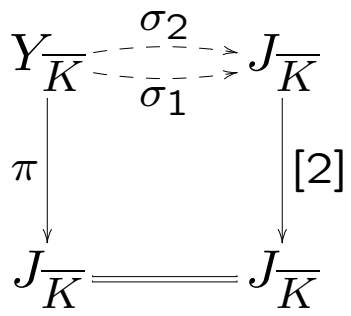
$$\begin{array}{ccc} Y_{\overline{K}} & \overset{\cong}{\underset{\sigma}{\dashrightarrow}} & J_{\overline{K}} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle [2]} \\ J_{\overline{K}} & = & J_{\overline{K}} \end{array}$$

commutes), where $Y$ is locally soluble everywhere.

The element $Y \to J$ maps to 0 in $Ш(K, J)[2]$ iff $Y(K) \neq \emptyset$.

**Problem:** The surfaces $Y$ are described by 72 quadrics in $\mathbb{P}^{15}$ ...

## Solution: A quotient of $Y$.




Two isomorphisms $\sigma_1$ and $\sigma_2$ differ by translation by a 2-torsion point, as the morphism

$$Y_{\overline{K}} \xrightarrow{(\sigma_1,\sigma_2)} J_{\overline{K}} \times J_{\overline{K}} \xrightarrow{(P,Q)\mapsto P-Q} J_{\overline{K}}$$

has connected domain and finite image.

$[-1]$ on $J$ commutes with translation by 2-torsion points $\Rightarrow$
it induces a unique involution $\iota$ of $Y_{\overline{K}}$, defined over $K$. Set $X = Y/\iota$.

## Solution: A quotient of $Y$

$[-1]$ on $J$ commutes with translation by 2-torsion points $\Rightarrow$
it induces a unique involution $\iota$ of $Y_{\overline{K}}$, defined over $K$. Set $X = Y/\iota$.

**Advantages:**

- $X$ is a complete intersection of 3 quadrics in $\mathbb{P}^5$.
- $X(K) = \emptyset \;\Rightarrow\; Y(K) = \emptyset$

**Disadvantage:**

- This only gives sufficient conditions for $Y(K) = \emptyset$.

## Solution: A quotient of $Y$

$[-1]$ on $J$ commutes with translation by 2-torsion points $\Rightarrow$
it induces a unique involution $\iota$ of $Y_{\overline{K}}$, defined over $K$. Set $X = Y/\iota$.

**Advantages:**

- $X$ is a complete intersection of 3 quadrics in $\mathbb{P}^5$.
- $X(K) = \emptyset \;\Rightarrow\; Y(K) = \emptyset$

**Disadvantage:**

- This only gives sufficient conditions for $Y(K) = \emptyset$.

**Situation:** Such K3 surfaces are everywhere locally soluble, but may still satisfy $X(K) = \emptyset$. Do they?

## Tool: Brauer-Manin obstruction.

## Tool: Brauer-Manin obstruction.

For any scheme $Z$ we set $\operatorname{Br} Z = H^2_{\text{ét}}(Z, \mathbb{G}_m)$.

For any $K$-algebra $S$ and any $S$-point $x\colon \operatorname{Spec} S \to X$, we get a homomorphism $x^*\colon \operatorname{Br} X \to \operatorname{Br} S$, yielding a map

$$\rho_S\colon X(S) \to \operatorname{Hom}(\operatorname{Br} X, \operatorname{Br} S).$$

## Tool: Brauer-Manin obstruction.

For any scheme $Z$ we set $\operatorname{Br} Z = H^2_{\text{ét}}(Z, \mathbb{G}_m)$.

For any $K$-algebra $S$ and any $S$-point $x\colon \operatorname{Spec} S \to X$, we get a homomorphism $x^*\colon \operatorname{Br} X \to \operatorname{Br} S$, yielding a map

$$\rho_S\colon X(S) \to \operatorname{Hom}(\operatorname{Br} X, \operatorname{Br} S).$$

Apply this to $K$ and to the ring of adèles

$$\mathbb{A}_K = \prod_{v \in M_K}{}' K_v \qquad \text{(almost all coordinates are integral).}$$

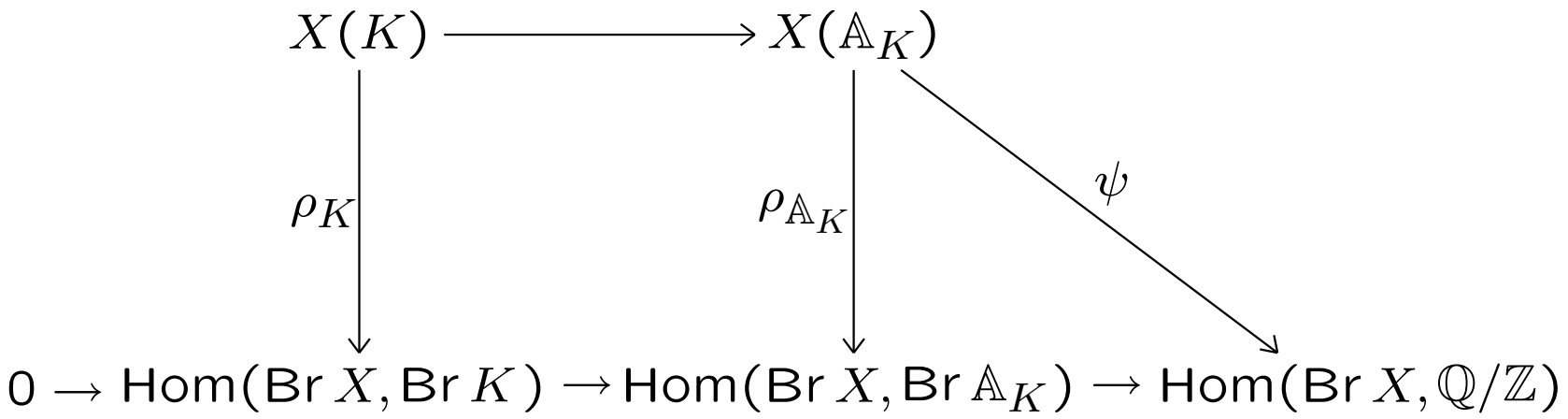
From class field theory (and comparison theorems) we have

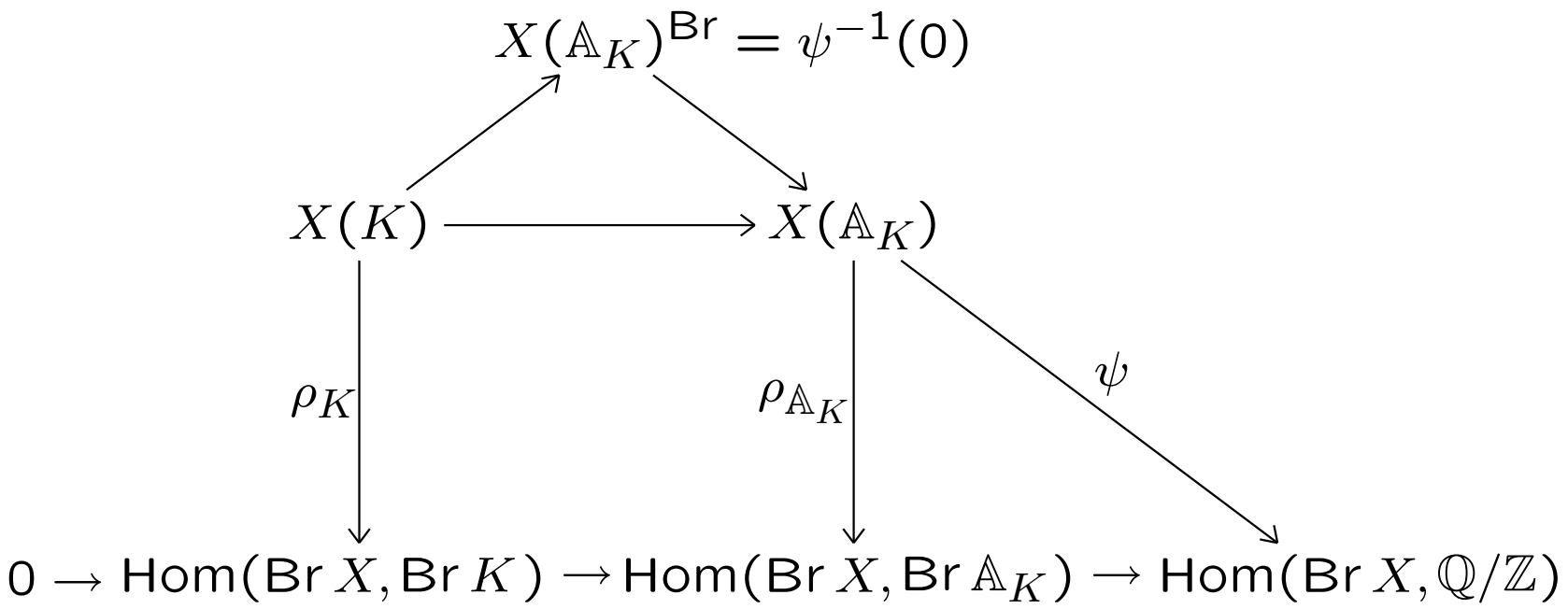
$$0 \to \qquad \operatorname{Br} K \quad \to \qquad \operatorname{Br} \mathbb{A}_K \quad \to \qquad \mathbb{Q}/\mathbb{Z}$$

Applying $\operatorname{Hom}(\operatorname{Br} X, \_\,)$ we find ...

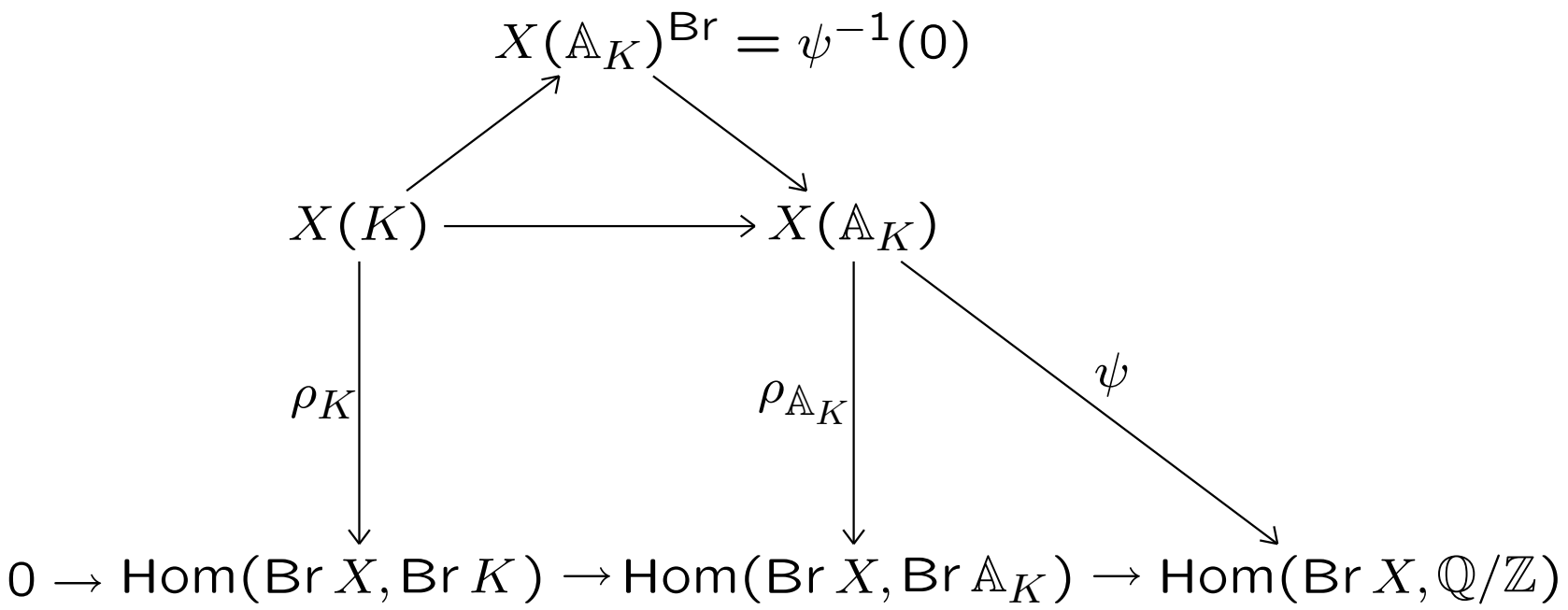
$$0 \to \mathrm{Hom}(\mathrm{Br}\, X, \mathrm{Br}\, K) \to \mathrm{Hom}(\mathrm{Br}\, X, \mathrm{Br}\, \mathbb{A}_K) \to \mathrm{Hom}(\mathrm{Br}\, X, \mathbb{Q}/\mathbb{Z})$$

$$
\begin{array}{ccccccc}
 & & X(K) & & X(\mathbb{A}_K) & & \\
 & & \downarrow{\scriptstyle \rho_K} & & \downarrow{\scriptstyle \rho_{\mathbb{A}_K}} & & \\
0 & \to & \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, K) & \to & \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, \mathbb{A}_K) & \to & \mathsf{Hom}(\mathsf{Br}\, X, \mathbb{Q}/\mathbb{Z})
\end{array}
$$

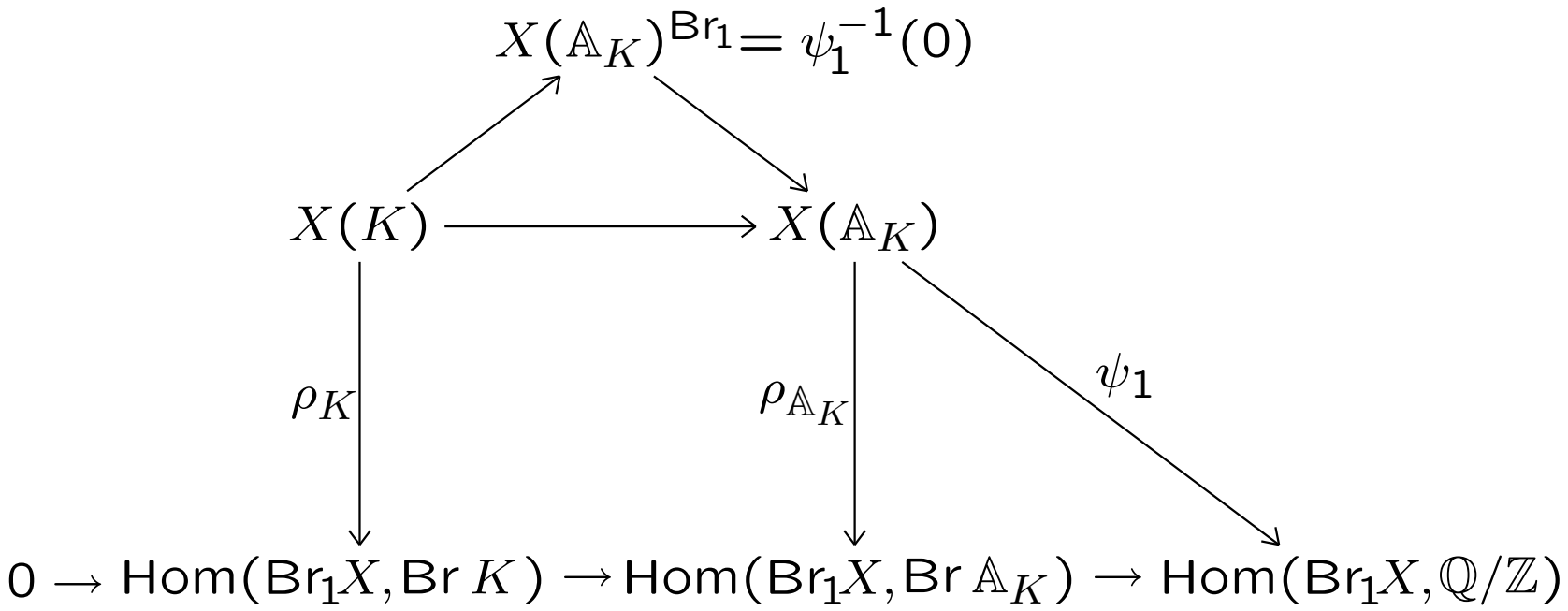

$X(K)$
$X(\mathbb{A}_K)$
$\rho_K$
$\rho_{\mathbb{A}_K}$
$\psi$
$0 \to \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, K) \to \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, \mathbb{A}_K) \to \mathsf{Hom}(\mathsf{Br}\, X, \mathbb{Q}/\mathbb{Z})$


$X(\mathbb{A}_K)^{\mathsf{Br}} = \psi^{-1}(0)$
$X(K)$
$X(\mathbb{A}_K)$
$\rho_K$
$\rho_{\mathbb{A}_K}$
$\psi$
$0 \to \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, K) \to \mathsf{Hom}(\mathsf{Br}\, X, \mathsf{Br}\, \mathbb{A}_K) \to \mathsf{Hom}(\mathsf{Br}\, X, \mathbb{Q}/\mathbb{Z})$

$$X(\mathbb{A}_K)^{\mathsf{Br}} = \emptyset \quad \Rightarrow \quad X(K) = \emptyset$$



$$X(\mathbb{A}_K)^{\mathrm{Br}_1} = \emptyset \quad \Rightarrow \quad X(K) = \emptyset$$




$\mathrm{Br}_1\, X = \ker(\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X})$

$$X(\mathbb{A}_K)^{\mathrm{Br}_1} = \emptyset \quad \Rightarrow \quad X(K) = \emptyset.$$

**Two steps:**

- Compute $\mathrm{Br}_1 Z/\mathrm{Br}\, K$ for the desingularization(!) $Z$ of $X = Y/\iota$.

The Hochschild-Serre spectral sequence gives

$$\mathrm{Br}_1 Z/\mathrm{Br}\, K \;\cong\; H^1(G_K, \mathrm{Pic}\,\overline{Z}).$$

$$X(\mathbb{A}_K)^{\mathrm{Br}_1} = \emptyset \quad \Rightarrow \quad X(K) = \emptyset.$$

**Two steps:**

- Compute $\mathrm{Br}_1 Z/\mathrm{Br}\, K$ for the desingularization(!) $Z$ of $X = Y/\iota$.

The Hochschild-Serre spectral sequence gives

$$\mathrm{Br}_1 Z/\mathrm{Br}\, K \;\cong\; H^1(G_K, \mathrm{Pic}\,\overline{Z}).$$

- Compute $Z(\mathbb{A}_K)^{\mathrm{Br}_1}$.

$$X(\mathbb{A}_K)^{\mathrm{Br}_1} = \emptyset \quad \Rightarrow \quad X(K) = \emptyset.$$

**Two steps:**

- Compute $\mathrm{Br}_1 Z/\mathrm{Br}\, K$ for the desingularization(!) $Z$ of $X = Y/\iota$.

The Hochschild-Serre spectral sequence gives

$$\mathrm{Br}_1 Z/\mathrm{Br}\, K \;\cong\; H^1(G_K, \mathrm{Pic}\,\overline{Z}).$$

- Compute $Z(\mathbb{A}_K)^{\mathrm{Br}_1}$.

Things will turn out easier when we have an elliptic fibration.

## Making the theory and the ideas explicit

Consider $C\colon\ y^2 = f$, with $f \in K[X]$ separable of degree 6.

Set $A = K[\theta] = K[X]/f$, a product of fields.

$$(P, Q) \longmapsto (x_P - \theta)(x_Q - \theta)$$

$$J(K)/2J(K) \xhookrightarrow[\phi]{} A^*/K^*A^{*2}$$

## Making the theory and the ideas explicit

Consider $C\colon\ y^2 = f$, with $f \in K[X]$ separable of degree 6.

Set $A = K[\theta] = K[X]/f$, a product of fields.

$$(P, Q) \longmapsto (x_P - \theta)(x_Q - \theta)$$

$$\begin{array}{ccc} J(K)/2J(K) & \xrightarrow[\phi]{} & A^*/K^*A^{*2} \\ \downarrow & & \downarrow \\ J(K_v)/2J(K_v) & \xrightarrow[\phi_v]{} & A_v^*/K_v^*A_v^{*2} \end{array}$$

We consider the computable **fake Selmer group**

$$\mathrm{Sel}_f^{(2)}(K, J) = \{x \in A^*/K^*A^{*2}\ :\ x \in \mathrm{im}\,\phi_v \text{ for all } v\}.$$

For $\delta \in \mathrm{Sel}_f^{(2)}(K, J) \subset A^*/K^*A^{*2}$ we set

$$\mathcal{X}_\delta = \{\alpha \in A^* \ : \ \delta\alpha^2 = c_2\theta^2 + c_1\theta + c_0\} \subset A^*.$$

Then the corresponding

$$X_\delta \subset \mathbb{P}(A)$$

is a complete intersection of three quadrics $C_3 = C_4 = C_5 = 0$.

For $\delta \in \mathrm{Sel}_f^{(2)}(K, J) \subset A^*/K^*A^{*2}$ we set

$$\mathcal{X}_\delta = \{\alpha \in A^* \ : \ \delta\alpha^2 = c_2\theta^2 + c_1\theta + c_0\} \subset A^*.$$

Then the corresponding

$$X_\delta \subset \mathbb{P}(A)$$

is a complete intersection of three quadrics $C_3 = C_4 = C_5 = 0$.

**Fact:** The K3 surface $X_\delta$ is the quotient $Y_\delta/\langle\iota\rangle$.

For every $\xi \in A_{\overline{K}}$ with $\xi^2 = \delta$, the set

$$\{\xi^{-1}(s\theta + t) \ : \ s, t \in K\}$$

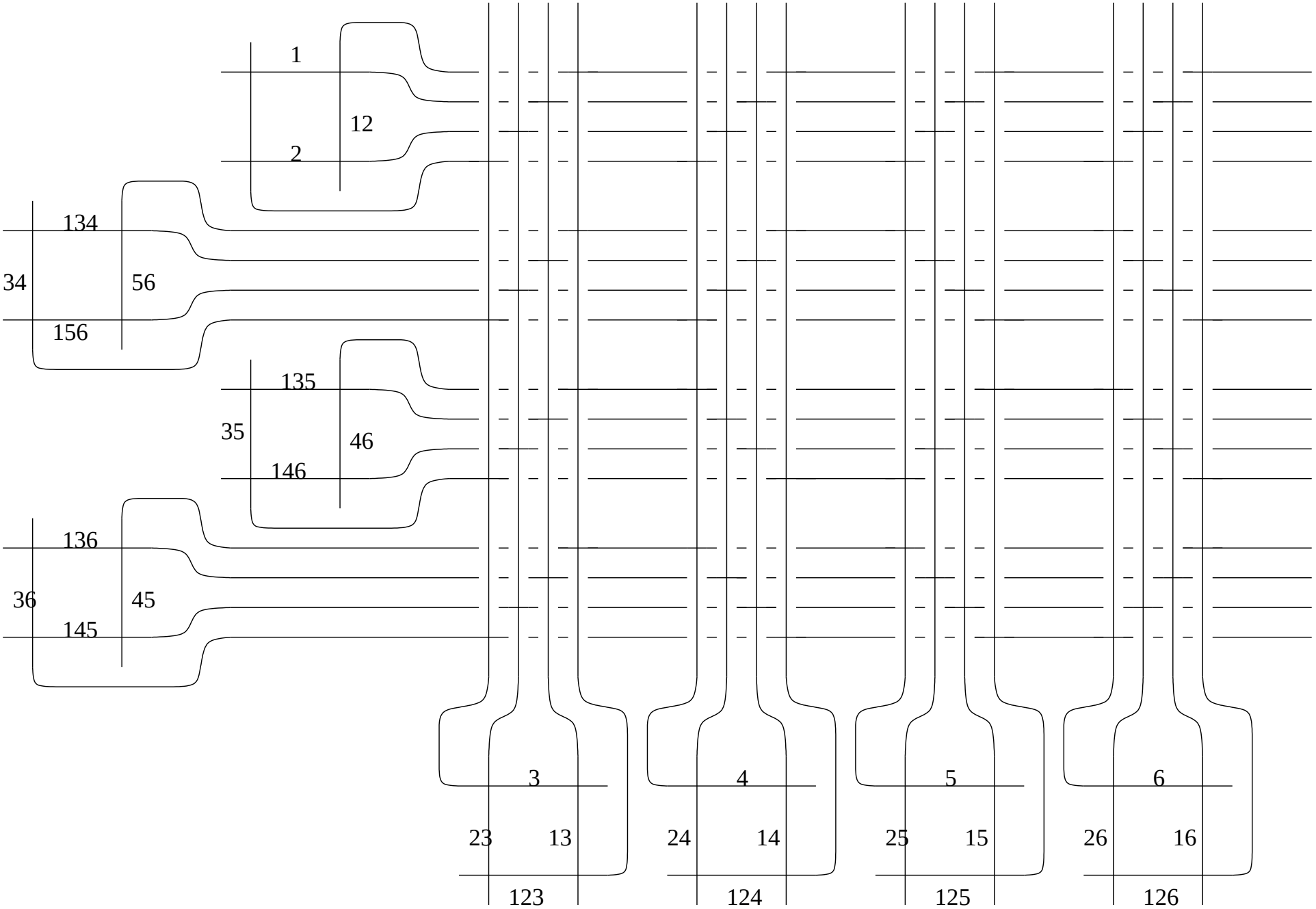
corresponds to a line on $X_\delta$.

After fixing one square root $\xi$ of $\delta$ in $A_{\overline{K}}$, the remaining square roots of $\delta$ are parametrized by $\mu_2(A_{\overline{K}})$ and the lines by $\mu_2(A_{\overline{K}})/\{\pm 1\}$.

Since we have $A_{\overline{K}} \cong \bigoplus_{\omega, f(\omega)=0} \overline{K}$, the lines are parametrized by partitions of the roots of $f$ into two parts.

Two lines intersect if and only if their partitions differ by one element.

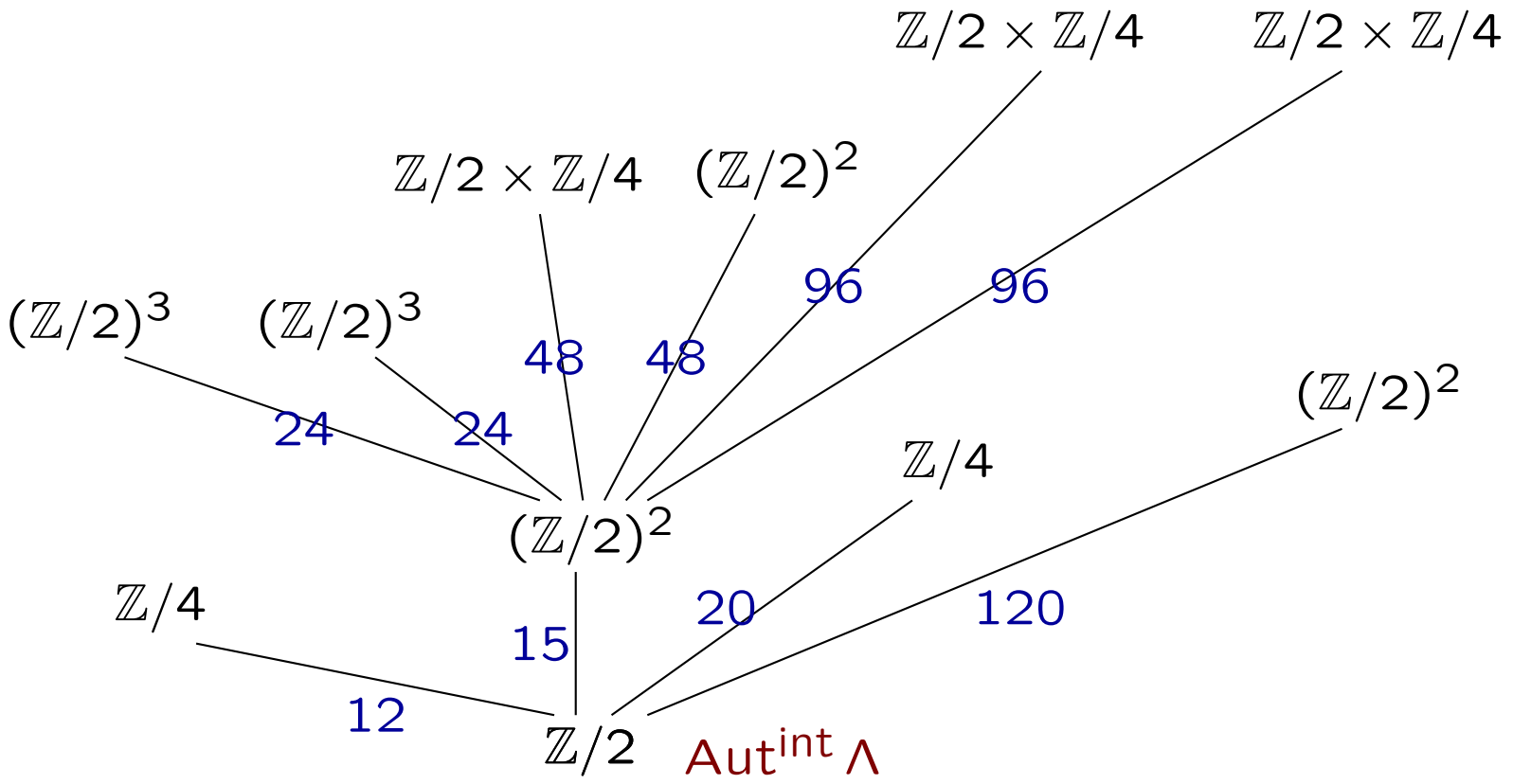
# Intersection among 32 lines on $\overline{Z}$



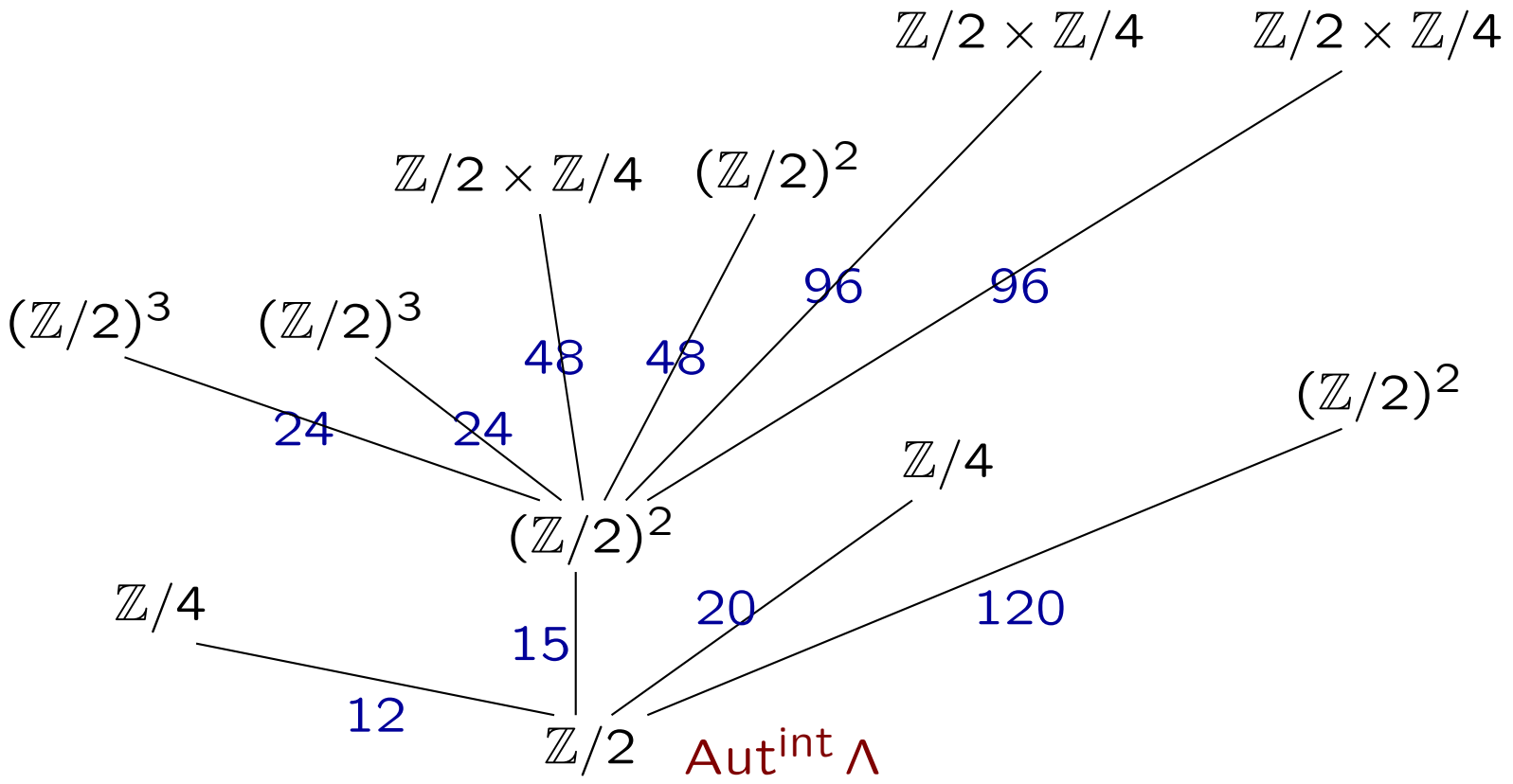
**Proposition:** Generically the group $\operatorname{Pic}\overline{Z}$ has rank 17, generated by the set $\Lambda$ of 32 lines.

**Corollary:** $G_K$ acts on $\operatorname{Pic}\overline{Z}$ through a subgroup of $\operatorname{Aut}^{\mathsf{int}}\Lambda$ (which has size 23040).

We can compute $H^1(G, \operatorname{Pic}\overline{Z})$ for all 2455 possible subgroups $G$ of $\operatorname{Aut}^{\mathsf{int}}\Lambda$ (up to conjugacy).

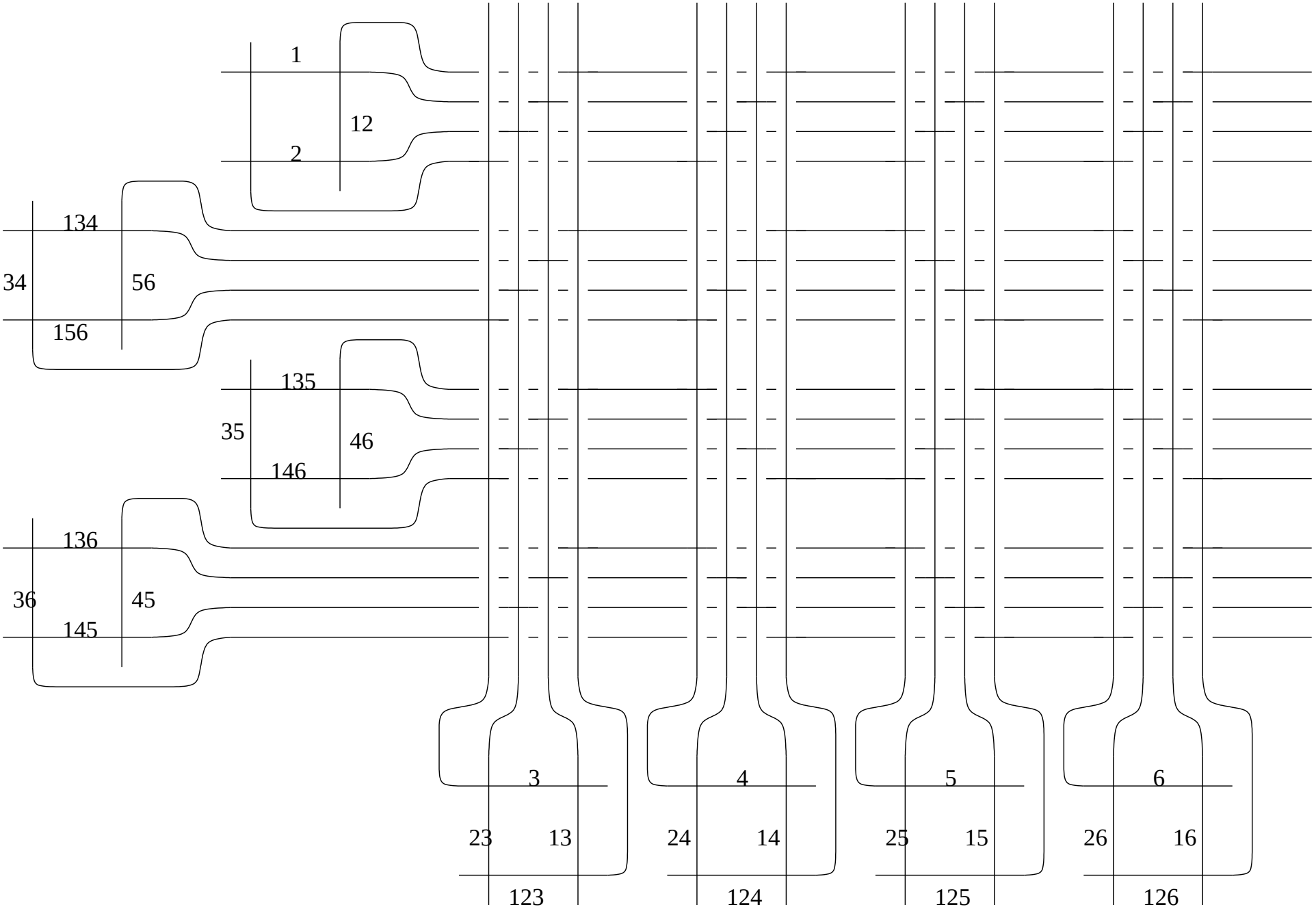



These 11 subgroups, including $\mathrm{Aut}^{\mathrm{int}}\,\Lambda$, induce all nontrivial Brauer elements.

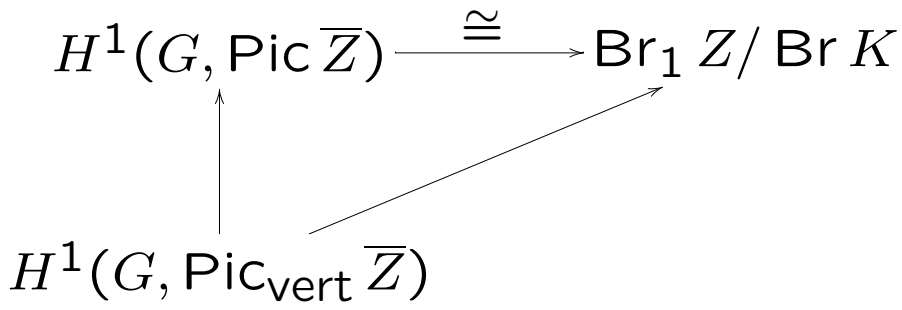



Step 2, Computing $Z(\mathbb{A}_K)^{\mathrm{Br}_1}$, is difficult

# An elliptic fibration



There is a group $E$ of order 384 such that if the Galois action factors through $E$, then $Z$ has an elliptic fibration over $K$, where four of the fibers consist of four lines intersecting in a cycle.




We need to express a nonzero element of $\mathrm{Br}_1\, Z/\,\mathrm{Br}\, K$ as an Azumaya algebra...

**Definition:** A **central simple algebra** over $K$ is a simple $K$-algebra with center equal to $K$.

**"Definition":** An **Azumaya algebra** is to a central simple algebra, as a sheaf is to a vectorspace.

For $a, b \in K$, let $(a, b)$ denote the central simple algebra over $K$, generated by $1, i, j, ij$ with $i^2 = a$, $j^2 = b$, and $ji = -ij$.

**Proposition 2.** *Let $\phi : V \to \mathbb{P}^1$ be an elliptic fibration, and suppose that $V$ has bad fibers of type $I_4$ over $P = (\alpha : 1)$, where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Suppose further that the field of definition of the components of the fiber at $P$ is $\mathbb{Q}(\alpha, \sqrt{c})$, where $c \in \mathbb{Q}(\alpha)$ is of square norm. Then the pullback of the algebra $\mathrm{cores}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c, t - \alpha) \in \mathrm{Br}\,\mathbb{Q}(t)$ to $V$ (where $t$ is the coordinate on the standard affine patch of $\mathbb{P}^1$) is an element of $\mathrm{Br}_\phi V$.*

**Theorem 3.** *Let $f$ factor as the product of three quadratic polynomials $f_1, f_2, f_3$, let $\delta_i$ be the images of $\delta$ in $\mathbb{Q}[x]/(f_i)$, and let $V$ be the K3 surface constructed from $f, \delta$. Suppose further that the splitting field of $f$ is of degree 8; that the norm of $\delta_1$ is a square; that the norms of $\delta_2$ and $\delta_3$ multiplied by the discriminant of $f_1$ are squares; and that the $\delta_i$ are otherwise generic, so that the field of definition of the lines of $V$ has degree 32. Then both elliptic fibrations associated to the factorization $f = (f_1)(f_2 f_3)$ satisfy the conditions of Proposition 2, and the elements of the vertical Brauer group constructed in that proposition map to the same (nontrivial) element of $H^1(\mathbb{Q}, \operatorname{Pic} V)$ and hence to the same element of $\operatorname{Br} V / \operatorname{Br} K$.*

**Theorem 4.** *Let $f$ factor as the product of three quadratic polynomials $f_1, f_2, f_3$, let $\delta_i$ be the images of $\delta$ in $\mathbb{Q}[x]/(f_i)$, and let $V$ be the K3 surface constructed from $f, \delta$. Suppose further that the splitting field of $f$ is of degree 8; that the norm of $\delta_1$ is a square; that the norms of $\delta_2$ and $\delta_3$ multiplied by the discriminant of $f_1$ are squares; and that the $\delta_i$ are otherwise generic, so that the field of definition of the lines of $V$ has degree 32. Then both elliptic fibrations associated to the factorization $f = (f_1)(f_2 f_3)$ satisfy the conditions of Proposition 2, and the elements of the vertical Brauer group constructed in that proposition map to the same (nontrivial) element of $H^1(\mathbb{Q}, \operatorname{Pic} V)$ and hence to the same element of $\operatorname{Br} V / \operatorname{Br} K$.*

$$C_n \colon\ y^2 = -6n f_1 f_2 f_3$$

$$f_1 = x^2 + 1, \quad f_2 = x^2 - 2x - 1, \quad f_3 = x^2 + x - 1,$$

$$\delta = \left(3, -(1+\sqrt{2}), (1+\sqrt{5})/2\right) \in K[x]/f_1 \times K[x]/f_2 \times K[x]/f_3.$$

I will spare you the details of actually evaluating the Azumaya algebra on the rational points.

The local invariants are constant at every prime. It is $\frac{1}{2}$ at 2 and it equals 0 everywhere else. This does not sum to 0...

We conclude that $X_\delta$ does not have any rational points, so neither does the homogeneous space $Y_\delta$ that covers $X_\delta$.

I will spare you the details of actually evaluating the Azumaya algebra on the rational points.

The local invariants are constant at every prime. It is $\frac{1}{2}$ at 2 and it equals 0 everywhere else. This does not sum to 0...

We conclude that $X_\delta$ does not have any rational points, so neither does the homogeneous space $Y_\delta$ that covers $X_\delta$.

It remains to check that $Y_\delta$ is locally solvable everywhere...

$$S = \left\{ p : p \text{ split in } \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{-3(1+\sqrt{2})}, \sqrt{6(1+\sqrt{5})}\right)\right\}.$$

$$C_n \colon\ y^2 = -6n(x^2+1)(x^2-2x-1)(x^2+x-1).$$

$$\delta = \left(3, -(1+\sqrt{2}), (1+\sqrt{5})/2\right)$$

A standard (but slightly tedious) computation:
$\delta$ is in the Selmer group, i.e., $Y_\delta$ is locally solvable everywhere.

$$S = \left\{ p : p \text{ split in } \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{-3(1+\sqrt{2})}, \sqrt{6(1+\sqrt{5})}\right)\right\}.$$

$$C_n \colon\ y^2 = -6n(x^2+1)(x^2-2x-1)(x^2+x-1).$$

$$\delta = \left(3, -(1+\sqrt{2}), (1+\sqrt{5})/2\right)$$

A standard (but slightly tedious) computation:
$\delta$ is in the Selmer group, i.e., $Y_\delta$ is locally solvable everywhere.

We reduce to the case of primes of bad reduction for $C_n$, namely $\infty, 2, 3, 5$, and primes dividing $n$.

At primes dividing $n$ we have $\delta = (3, 3\alpha^2, 3\beta^2) = 1$ in $A^*/K^*A^{*2}$.
The primes $\infty, 2, 3, 5$ we do by brute force.