Arithmetic Information of Rational Elliptic Surfaces and Shioda's Rank 68 Surface

Blair Butler, Andreas-Stephan Elsenhans

University of Sydney

ANTS XVII, July 2026

Elliptic Surfaces

An **elliptic surface** with base $\mathbb{P}^1$ can be given in a globally minimal Weierstrass form:

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where $a_i(t) \in k(t)$ for all i.

Elliptic Surfaces

Elliptic Surfaces

An **elliptic surface** with base $\mathbb{P}^1$ can be given in a globally minimal Weierstrass form:

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where $a_i(t) \in k(t)$ for all i.

Mordell-Weil Theorem for Function Fields

Let $E/k(t)$ be an elliptic surface with base $\mathbb{P}^1$. Then $E(\overline{k}(t))$ is a finitely generated group.

Elliptic Surfaces

Elliptic Surfaces

An **elliptic surface** with base $\mathbb{P}^1$ can be given in a globally minimal Weierstrass form:

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where $a_i(t) \in k(t)$ for all i.

Mordell-Weil Theorem for Function Fields

Let $E/k(t)$ be an elliptic surface with base $\mathbb{P}^1$. Then $E(\overline{k}(t))$ is a finitely generated group.

If $\deg a_i(t) \leq i$ for all i, the surface is rational.

If $\deg a_i(t) \leq 2i$ for all i, and there exists at least one i such that $\deg a_i(t) > i$, the surface is $K3$.

The Field of Definition

Let E be an elliptic surface, then there exists a number field k of finite degree such that

$$E(\overline{\mathbb{Q}}(t)) = E(k(t)).$$

Field of Definition

Consider an elliptic surface E. Let k be the smallest number field such that $E(k(t)) = E(\overline{\mathbb{Q}}(t))$. We call k the **field of definition** of the geometric Mordell-Weil group.

The Field of Definition

Let E be an elliptic surface, then there exists a number field k of finite degree such that

$$E(\overline{\mathbb{Q}}(t)) = E(k(t)).$$

Field of Definition

Consider an elliptic surface E. Let k be the smallest number field such that $E(k(t)) = E(\overline{\mathbb{Q}}(t))$. We call k the **field of definition** of the geometric Mordell-Weil group.

Silverman's Specialization Theorem

Let $\mathcal{E}(k)$ be an elliptic surface. Then the specialization map $\sigma_t : E(k(t)) \to \mathcal{E}_t(k)$ is injective for all but finitely many points of $t \in \mathbb{P}^1$.

Elliptic Delsarte Surfaces

Delsarte surface

A Delsarte surface is an irreducible, two-dimensional subvariety in $\mathbb{P}^3$ defined by a polynomial containing exactly four monomials with an invertible exponent matrix.

Delsarte surface

A Delsarte surface is an irreducible, two-dimensional subvariety in $\mathbb{P}^3$ defined by a polynomial containing exactly four monomials with an invertible exponent matrix.

Surface	Maximal Rank	Occurring for n
$y^2 = x^3 + t^n + 1$	68	360
$y^2 = x^3 + t^n x + 1$	56	840
$y^2 = x^3 + t^n x^2 + 1$	9	20
$y^2 = x^3 + (t^n + 1)^2$	18	60
$y^2 = x^3 + (1 + t^n)^3$	4	6
$y^2 = x^3 + (1 + t^n)x$	24	24
$y^2 = x^3 + t^n x - x^2$	3	6
$y^2 = x^3 + (1 + t^n)^2 x$	6	12
$y^2 + -t^n xy + y = x^3$	1	2
$y^2 = x^3 - 3t^{40} x + t^n + 1$	18	120
$t^n + x^2 + y^2 + x^2 y^2$	0	1

An Elliptic Surface of Rank 68

Shioda's Rank 68 Elliptic Surface

The elliptic surface given by

$$y^2 = x^3 + t^{360} + 1$$

has rank 68 over $E(\overline{\mathbb{Q}}(t))$.

An Elliptic Surface of Rank 68

Shioda's Rank 68 Elliptic Surface

The elliptic surface given by

$$y^2 = x^3 + t^{360} + 1$$

has rank 68 over $E(\overline{\mathbb{Q}}(t))$.

- Jasbir Chahal, Matthijs Meijer, and Jaap Top gave a decomposition of this surface into "simpler" pieces
- Bas Heijne found points for each of these smaller surfaces
- Sven Bootsma was able to determine polynomials requiring roots in order to have rank 68
- Jennifer Pearson showed it has rank 2 over $\mathbb{Q}(t)$
- Sajad Salami determined the field of definition was a compositum of number fields of degree 1728 and 5760.

Decomposing the Rank 68 Surface

Let $K = (t)$, where k is a number field with $\zeta_6 \in k$. We have an order-6 automorphism,

$$\rho(x, y) = (\zeta_6^2 x, \, -y).$$

Pass to $L = K(s)$ with $s^6 = t$: cyclic of degree 6, with $\mathrm{Gal}(L/K) = \langle \sigma \rangle, \;\; \sigma : s \mapsto \zeta_6 s$.

Set $V := E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$. It carries two commuting actions:

- a $\mathbb{Q}(\zeta_6)$-structure, $\zeta_6 \cdot (P \otimes r) := \rho(P) \otimes r$;
- the Galois map $\sigma_V(P \otimes r) := P^\sigma \otimes r$.

Since ρ is defined over K it commutes with σ_V, so σ_V is in fact $\mathbb{Q}(\zeta_6)$-*linear*. With $\sigma_V^6 = \mathrm{id}$, its eigenvalues are 6th roots of unity, all in $\mathbb{Q}(\zeta_6)$, hence

$$V = \bigoplus_{\lambda^6 = 1} V_\lambda \qquad \text{as } \mathbb{Q}(\zeta_6)\text{-vector spaces.}$$

Decomposing into Smaller Elliptic Surfaces

Using that process, we can instead consider the elliptic surfaces given by

$$y^2 = x^3 + t^i(t^{60} + 1), \quad 0 \le i \le 5.$$

By repeating this process, we can decompose to 11 elliptic surfaces:

$$\begin{array}{cc}
y^2 = x^3 + t^2(t+1), & y^2 = x^3 + t^3(t+1), \\
y^2 = x^3 + t(t^2+1), & y^2 = x^3 + t^2(t^2+1), \\
y^2 = x^3 + t^3(t^2+1), & y^2 = x^3 + t(t^3+1), \\
y^2 = x^3 + t^2(t^3+1), & y^2 = x^3 + t^5 + 1, \\
y^2 = x^3 + t(t^5+1), & y^2 = x^3 + t(t^4+1),
\end{array}$$

$$y^2 = x^3 + t^5 + t^{-5}.$$

Rational Elliptic Surfaces

Shioda-Tate Formula for Rational Elliptic Surfaces

For a rational surface, the Picard Number is 10.

$$\operatorname{rank} E(\overline{\mathbb{Q}}(t)) = 8 - \sum_{v \in \mathbb{P}^1} (m_v - 1),$$

Key fact: Every rational elliptic surface defined by a minimal Weierstrass equation has ≤ 240 points of the form $(x(t), y(t))$:

$$x(t) = c_1 t^2 + c_2 t + c_3, \quad y(t) = c_4 t^3 + c_5 t^2 + c_6 t + c_7.$$

These generate the Mordell-Weil group.

The action of the Galois group on $E(\overline{\mathbb{Q}}(t))$ preserves the height pairing and so gives a Galois representation:

$$\rho : G \to \mathrm{Aut}(E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tor}}, \langle \cdot, \cdot \rangle).$$

Now the field of definition k is the Galois extension of $\mathbb{Q}$ corresponding to $\mathrm{Ker}(\rho)$ in the sense of Galois theory, and we have $\mathrm{Gal}(k/\mathbb{Q}) = \mathrm{Im}(\rho)$.

Algorithm (`RatESSolve`): A globally minimal Weierstrass form of a rational elliptic surface, defined over a number field

- The Rank
- The field of definition of the geometric Mordell-Weil Group
- The Automorphism Group of the above
- The generating sections of the Mordell-Weil Group
- The torsion points
- The Galois representation
- The characters of the irreducible components of the Galois representation

1. Take sections of the elliptic surface of the form $(c_1t^2 + c_2t + c_3, c_4t^3 + c_5t^2 + c_6t + c_7)$, and substitute these into the Weierstrass equation for the elliptic surface, forming an ideal over $\mathbb{Q}[c_1, \ldots, c_7]$.
2. Compute the primary decomposition of this ideal, and extract the polynomials needed to define the number fields.

SplitAutGrp: Computing Splitting Fields

Input: Polynomials $f_1, \ldots, f_r \in \mathbb{Q}[x]$ with squarefree product.

Step 1 — Galois group: `GaloisGroup` computes $G \subset S_n$ acting on the roots $r_1, \ldots, r_n$ (represented p-adically).

Step 2 — Splitting field: $\texttt{GaloisSubgroup}(S, \texttt{sub} < G| >)$ produces an invariant I and resolvent polynomial g with root $-I(r_1, \ldots, r_n)$. This defines $K = \mathbb{Q}[X]/(g)$.

Step 3 — Automorphisms: For each $\sigma \in G$ find $h \in \mathbb{Q}[X]$ satisfying

$$h\big(-I(r_1, \ldots, r_n)\big) = -I(r_{1^\sigma}, \ldots, r_{n^\sigma})$$

by interpolation mod p, then Newton lift: $h_{n+1} = h_n - g(h_n(\bar{X}))/g'(h_n(\bar{X}))$.

Output: K, $\mathrm{Aut}(K/\mathbb{Q})$, explicit roots of each f_i in K.

Example of SplitAutGrp:

Let K be the degree 54 splitting field of the polynomial $x^9 + 6x^3 - 2$.

$$
\begin{tikzcd}
K = \mathbb{Q}(\zeta_3, r)(\sqrt[3]{r^2}) \\
\mathbb{Q}(\zeta_3)(r) \arrow[u] \\
\mathbb{Q}(\zeta_3) \arrow[u] \\
\mathbb{Q} \arrow[u] \arrow[uuu, bend right]
\end{tikzcd}
$$

`AutomorphismGroup(K)` takes about 23 minutes.

Example of SplitAutGrp:

Let K be the degree 54 splitting field of the polynomial $x^9 + 6x^3 - 2$.

$$
\begin{tikzcd}
K = \mathbb{Q}(\zeta_3, r)(\sqrt[3]{r^2}) \\
\mathbb{Q}(\zeta_3)(r) \arrow[u] \\
\mathbb{Q}(\zeta_3) \arrow[u] \\
\mathbb{Q} \arrow[u] \arrow[uuu, bend right]
\end{tikzcd}
$$

`AutomorphismGroup(K)` takes about 23 minutes.

Instead take a polynomial for each of the generating elements of the extensions:

- f the minimal polynomial of ζ_3
- g the minimal polynomial of r
- h the minimal polynomial of $\sqrt[3]{r^2}$

Then `SplitAutGrp([f,g,h])` takes about 0.5s.

Implementation: RatESSolve

Example: $y^2 = x^3 - 3t(t^2-1)x + (t^2-1)^2$

```
> F<t> := FunctionField(RationalField());
> E := EllipticCurve([-3*t*(t^2-1),(t^2-1)^2]);
> rk, K, Aut, secs, tors, reps, chars:= RatESSolve(E);
```

We find that this has:

- Rank: 5
- Torsion Points: None
- $[k : \mathbb{Q}] : 48$
- $Gal(K/\mathbb{Q}) : C_2 \times S_4$
- Galois representations: Irreducible components have characters $[1, 1, 3]$

Runtime: ≈ 15 minutes

Surface	Rank	$[k : \mathbb{Q}]$	$\mathrm{Gal}(k/\mathbb{Q})$
$y^2 = x^3 + t^2(t+1)$	2	2	C_2
$y^2 = x^3 + t^3(t+1)$	2	2	C_2
$y^2 = x^3 + t(t^2+1)$	4	16	QD_{16}
$y^2 = x^3 + t^2(t^2+1)$	4	6	S_3
$y^2 = x^3 + t^3(t^2+1)$	4	16	QD_{16}
$y^2 = x^3 + t(t^3+1)$	6	54	$C_9 \rtimes C_6$
$y^2 = x^3 + t^2(t^3+1)$	6	54	$C_9 \rtimes C_6$
$y^2 = x^3 + t(t^5+1)$	8	240	$(C_5 \rtimes C_8) \rtimes S_3$
$y^2 = x^3 + t^5 + 1$	8	240	$(C_5 \rtimes C_8) \rtimes S_3$
$y^2 = x^3 + t(t^4+1)$	8	48	$C_2 \times D_{12}$
Total	**52**		

The K3 Sub-Surface

The remaining surface is the K3 elliptic surface:

$$y^2 = x^3 + t^5 + t^{-5}, \qquad \text{with rank } E(\bar{\mathbb{Q}}(t)) = 16.$$

Consider points of the form: $P = (x(t), y(t))$, where:

$$x(t) = \frac{c_1 t^4 + c_2 t^3 + c_3 t^2 + c_4 t + c_5}{t^2},$$
$$y(t) = \frac{d_1 t^6 + d_2 t^5 + d_3 t^4 + d_4 t^3 + d_5 t^2 + d_6 t + d_7}{t^3}.$$

We can use this to find 16 independent points over a number field of degree 192. We have the representation:

$$\bar{\rho}\colon Gal(k/\mathbb{Q}) \to Aut\big(E(\overline{k}(t)), \langle\cdot,\cdot\rangle\big),$$

and $|Im(\rho)| = 192 = [k : \mathbb{Q}]$.

Main Theorem

Theorem

The field of definition of the Mordell-Weil group of Shioda's rank 68 surface

$$y^2 = x^3 + t^{360} + 1$$

is the splitting field of the polynomials:

$$\begin{array}{cc}
x^2 - x + 1, & x^8 - 6x^4 - 3, \\
x^6 - 3x^5 + 5x^3 - 3x + 1, & x^9 + 6x^3 - 2, \\
x^5 - x^4 + 4x^3 + 4x^2 - x + 13, & x^3 - x^2 - 3x - 3, \\
x^{12} - 4x^9 + 22x^6 - 12x^3 + 2, & x^{12} + 4x^6 + 54, \\
x^4 - x^3 + x^2 - x + 1, & x^4 - 2x^3 + 4x^2 + 12x + 6, \\
x^3 - 5, & x^{16} - 60x^{12} - 370x^8 - 300x^4 + 25,
\end{array}$$

$$x^8 - x^7 + 2x^6 + 2x^5 - 5x^4 + 13x^3 - 13x^2 + x + 1,$$

which is a number field of degree $829\,440 = 2^{11} \cdot 3^4 \cdot 5$.

Elliptic Delsarte Surfaces

Surface	Rank	Field of Definition Degree
$y^2 = x^3 + t^{360} + 1$	68	829 440
$y^2 = x^3 + t^{840}x + 1$	56	?
$y^2 = x^3 + t^{20}x^2 + 1$	9	1280
$y^2 = x^3 + (t^{60} + 1)^2$	18	288
$y^2 = x^3 + (1 + t^6)^3$	4	2
$y^2 = x^3 + (1 + t^{24})x$	24	128
$y^2 = x^3 + t^6x - x^2$	3	12
$y^2 = x^3 + (1 + t^{12})^2x$	6	8
$y^2 - t^2xy + y = x^3$	1	1
$y^2 = x^3 - 3t^{40}x + t^{120} + 1$	18	16
$t + x^2 + y^2 + x^2y^2$	0	1