

Elliptic Curves: j -Invariant

Talk 09

Michael Lindner

Oct. 8, 2026

Contents

1	From Legendre equations to degree-two maps	3
2	Degree-two maps and the group action	4
3	Construction of the invariant	6
4	The main result	8

Setup. We use the following notation and definitions throughout.

- The letter K denotes an algebraically closed field with $\text{char } K \neq 2$.
- We write $\mathbb{P}^n := \mathbb{P}_K^n$ and identify $\mathbb{P}^1$ with $K \cup \{\infty\}$ where $\infty := [1 : 0]$.
- A *curve* is an integral smooth projective scheme over K of dimension one.
- An *elliptic* curve is a curve of genus one.
- The letter E denotes an elliptic curve.

Introduction

Recall that any elliptic curve E can be embedded into $\mathbb{P}^2$ via a Legendre equation, i.e. there is a morphism $g : E \rightarrow \mathbb{P}^2$ such that $E \cong \text{Im } g =: W$, where W is given by the projectivization of

$$y^2 = x(x-1)(x-\lambda),$$

with $\lambda \in K \setminus \{0, 1\}$. The explicit equation might vary under weaker assumptions on K , but in our setup we see that all elliptic curves arise from equations differing only by this single parameter λ . One may hope for the following conclusion:

Dream: The assignment $E \mapsto \lambda$ yields a well-defined one-to-one correspondence between elliptic curves up to isomorphism and elements of $K \setminus \{0, 1\}$.

A quick reality check shows that this is not true: The assignment $E \mapsto \lambda$ is not even well-defined, since it depends on our choice of g . If $W' \subseteq \mathbb{P}^2$ is given by

$$y^2 = x(x-1)(x-(1-\lambda)),$$

and $i \in K$ with $i^2 = -1$, then

$$W \xrightarrow{\sim} W', (x, y) \mapsto (1-x, iy)$$

is an isomorphism. Thus, E can be mapped to both λ and $1-\lambda$.

However, one can repair this defect by constructing a map $j : K \setminus \{0, 1\} \rightarrow K$ such that the composite $E \mapsto \lambda \mapsto j(\lambda)$ is well-defined and induces the desired one-to-one correspondence

$$j : \{\text{isomorphism classes of elliptic curves}\} \leftrightarrow K$$

called the *j-invariant*. To this end we will proceed by proving the following:

- 1) The map g induces a degree-two map $E \rightarrow \mathbb{P}^1$ with branch points $0, 1, \infty, \lambda$.
- 2) If $f_i : E \rightarrow \mathbb{P}^1$ is a degree-two map with branch points $0, 1, \infty, \lambda_i$, then $\lambda_1 \in S_3 \lambda_2$, where the group action $S_3 \curvearrowright (K \setminus \{0, 1\})$ is defined below.
- 3) There is $j : K \setminus \{0, 1\} \rightarrow K$, such that $j(\lambda_1) = j(\lambda_2)$, if and only if $\lambda_1 \in S_3 \lambda_2$. In particular, $j(E)$ is well-defined.
- 4) We have $E_1 \cong E_2$ if and only if $j(E_1) = j(E_2)$, and every $\mu \in K$ appears as the j -invariant of some elliptic curve E .

This approach loosely follows [Har77, Ch. 4.4]. For a slightly different approach using the uniqueness of double covers, see [Vak25, Ch. 19.9].

1 From Legendre equations to degree-two maps

1.1 Reminder (Hurwitz). Let $f : X \rightarrow Y$ be a finite separable morphism of curves, such that f has only tame ramification, i.e. $\text{char } K \nmid e_P(f)$ for all $P \in X$. Then the equation

$$2g(X) - 2 = \deg(f)(2g(Y) - 2) + \sum_{P \in X} (e_P(f) - 1)$$

holds. In particular, any degree-two map $h : E \rightarrow \mathbb{P}^1$ satisfies

$$0 = 2 \cdot 1 - 2 = 2(2 \cdot 0 - 2) + \sum_{P \in E} (e_P(h) - 1) = \sum_{P \in E} (e_P(h) - 1) - 4$$

where $e_P(h) \in \{1, 2\}$, so h has exactly four ramification points. Moreover,

$$2 = \deg h = \sum_{Q \in h^{-1}(P)} e_Q(h)$$

for all $P \in \mathbb{P}^1$ implies that their images are distinct. Hence, h has exactly four branch points.

1.2 Lemma. Let $g : E \rightarrow \mathbb{P}^2$ be a morphism such that $E \cong \text{Im } g =: W$, where W is given by

$$y^2 = x(x - 1)(x - \lambda)$$

where $\lambda \neq 0, 1$. Then there is a degree-two map $f : E \rightarrow \mathbb{P}^1$ with branch points $0, 1, \infty, \lambda$.

Proof. Since $E \cong W$ is smooth (and thus regular), we can extend

$$W \setminus \{[0 : 1 : 0]\} \rightarrow \mathbb{P}^1, [x : y : z] \mapsto [x : z]$$

to a morphism $f : W \rightarrow \mathbb{P}^1$. Then

$$\begin{aligned} K(W) &= \text{Frac}(K[x, y]/(y^2 - x(x - 1)(x - \lambda))) \\ &= \text{Frac}(K(x)[y]/(y^2 - x(x - 1)(x - \lambda))) \end{aligned}$$

and $K(\mathbb{P}^1) = K(x)$ imply

$$\deg f = [K(W) : K(\mathbb{P}^1)] = 2.$$

Hence, f has exactly four branch points and

$$2 = \deg f = \sum_{Q \in f^{-1}(P)} e_Q(f)$$

implies that a point $P \in \mathbb{P}^1$ is a branch point if and only if we have $\#(f^{-1}(P)) = 1$. Given $P := [x : 1] \in \mathbb{P}^1 \setminus \{\infty, 0, 1, \lambda\}$, we have

$$f^{-1}(\{P\}) = \{[x : y : 1] \mid y^2 = x(x-1)(x-\lambda)\}.$$

Hence, $\text{char}(K) \neq 2$ and $x(x-1)(x-\lambda) \neq 0$ yield $\#(f^{-1}(P)) = 2$. Hence, the branch points must be the remaining points $0, 1, \lambda, \infty$. $\square$

2 Degree-two maps and the group action

2.1 Lemma. Let $f : X \rightarrow Y$ be a finite map of curves such that $K(X)/K(Y)$ is Galois. Then $\text{Aut}_Y(X)$ acts transitively on each fiber.

Proof. We reduce to the following algebra claim:

Let B be an integrally closed domain, $F := \text{Frac}(B)$, L/F a finite Galois extension, $G := \text{Gal}(L/F)$ and A the integral closure of B in L . Then G acts transitively on the set of prime ideals over any given prime ideal $\mathfrak{p}$. (For a proof of this fact see [Lan02, Ch. 5 Prop. 2.1].)

To this end, recall the equivalence of categories

$$(\text{curves with finite maps})^{\text{op}} \rightarrow (\text{Field}_K^{\text{trdeg}=1}), X \mapsto K(X).$$

In fact, for our purposes, full faithfulness suffices. In particular, we get an isomorphism $\text{Aut}_Y(X) \cong \text{Aut}_{K(Y)}(K(X))$. Moreover, if $X = \text{Spec}(R)$, $Y = \text{Spec}(S)$, $\mathfrak{p} \subseteq R$ is a prime ideal and $f \in \text{Aut}_Y(X)$ corresponds to $\sigma \in \text{Aut}_{K(Y)}(K(X))$, then $f(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p})$. Thus, the $\text{Aut}_Y(X)$ -action can be locally described by the Galois group.

This leads to the following reduction: Let $y \in Y$ with affine open neighborhood $\text{Spec } B =: V \subseteq Y$. Since f is finite (and thus affine), we obtain $f^{-1}(V) = \text{Spec } A =: U$ and $(f|_U : U \rightarrow V) = \text{Spec}(\varphi)$ for some finite (and thus integral) ring map $\varphi : B \rightarrow A$. Moreover, A and B are integrally closed, since curves are smooth and hence normal. Additionally, the equalities $L := K(X) = K(\text{Spec } A) = \text{Frac}(A)$ and $F := K(Y) = \text{Frac}(B)$ hold. Hence, if L_B (respectively L_A) denotes the integral closure of B (respectively A) in L , we get

$$A \subseteq L_B \subseteq L_A = A.$$

This concludes the desired reduction. $\square$

2.2 Reminder (Linear Systems). For degree-two maps on elliptic curves the correspondence of divisors and maps to projective space using linear systems boils down to the following:

- Let $D \in \text{Div}(E)$ be effective with $\deg D = 2$. Then the linear system $|D| \neq \emptyset$ is base-point free and induces a map $E \rightarrow \mathbb{P}(H^0(E, \mathcal{L}(D)))$ whose fibers correspond to the divisors in $|D|$. Using $\deg D > 2g - 2$, the Riemann-Roch theorem yields

$$\dim_K(H^0(E, \mathcal{L}(D))) = \ell(D) = \deg D - g + 1 = 2.$$

Hence, by a choice of basis of $H^0(E, \mathcal{L}(D)) \cong K^2$ we get a map $f : E \rightarrow \mathbb{P}^1$ such that

$$D \in |D| = \left\{ \sum_{Q \in f^{-1}(P)} e_Q(f)Q \mid P \in \mathbb{P}^1 \right\} =: \text{Div}_f$$

holds.

- Conversely, if $f_i : E \rightarrow \mathbb{P}^1$ are finite morphisms with $D \in \text{Div}_{f_1} \cap \text{Div}_{f_2}$, then both correspond to $|D|$, i.e. they only differ by an automorphism of $\mathbb{P}^1$.

2.3 Lemma. Let $f_i : E \rightarrow \mathbb{P}^1$ be a degree-two map ramified at $P_i \in E$. Then there are automorphisms $\sigma \in \text{Aut}(E)$ and $\tau \in \text{Aut}(\mathbb{P}^1)$, such that $f_2 \circ \sigma = \tau \circ f_1$ and $\sigma(P_1) = P_2$ hold.

Proof. The linear system $|P_1 + P_2|$ induces a degree-two map $g : E \rightarrow \mathbb{P}^1$ with $\{P_1, P_2\}$ as one of its fibers. Moreover, the degree-two field extension $K(E)/K(\mathbb{P}^1)$

is Galois as $\text{char } K \neq 2$. Then Lemma 2.1 yields $\sigma \in \text{Aut}(E)$ with $\sigma(P_1) = P_2$. Hence, f_1 and $f_2 \circ \sigma$ are both degree-two maps ramified at P_1 , i.e. both correspond to $|2P_1|$, and hence differ only by an automorphism $\tau \in \text{Aut}(\mathbb{P}^1)$. $\square$

2.4 Construction (S_3 acts on $K \setminus \{0, 1\}$). Recall that the group $\text{Aut}(\mathbb{P}^1)$ acts sharply three-transitively on $\mathbb{P}^1$. This motivates the following group action. For $\lambda \in K \setminus \{0, 1\}$ and $\alpha \in S_3$ define $\alpha \cdot \lambda$ by:

- 1) Permute the triple $(0, 1, \lambda)$ according to α . Let (x_1, x_2, x_3) denote this permuted triple.
- 2) Let $\tau \in \text{Aut}(\mathbb{P}^1)$ be the automorphism uniquely determined by $\tau(\infty) = \infty$, $\tau(x_1) = 0$ and $\tau(x_2) = 1$.
- 3) Define $\alpha \cdot \lambda := \tau(x_3)$.

One checks easily that this indeed defines a group action.

2.5 Lemma. Assume in the situation of Lemma 2.3 that f_i has branch points $0, 1, \infty, \lambda_i$ and that $f_1(P_1) = \infty = f_2(P_2)$. Then $\lambda_1 \in S_3\lambda_2$ holds.

Proof. Consider $\sigma \in \text{Aut}(E)$ and $\tau \in \text{Aut}(\mathbb{P}^1)$ as in Lemma 2.3. In particular,

$$\tau(\infty) = (\tau \circ f_1)(P_1) = (f_2 \circ \sigma)(P_1) = f_2(P_2) = \infty$$

holds. Since automorphisms send branch points to branch points, we obtain $\tau(\{0, 1, \lambda_1\}) = \{0, 1, \lambda_2\}$, i.e. $(\tau(0), \tau(1), \tau(\lambda_1)) =: (x_1, x_2, x_3)$ is a permutation of $(0, 1, \lambda_2)$, obtained by applying some $\alpha \in S_3$. Then

$$\lambda_1 = \tau^{-1}(x_3) = \alpha \cdot \lambda_2 \in S_3\lambda_2$$

holds by construction. $\square$

3 Construction of the invariant

3.1 Remark. We want to construct $j : K \setminus \{0, 1\} \rightarrow K$ such that $j(\lambda_1) = j(\lambda_2)$ holds if and only if $\lambda_1 \in S_3\lambda_2$. Observe that $x \mapsto (x - a)/(b - a)$ is the unique

automorphism $\tau \in \text{Aut}(\mathbb{P}^1)$ given by $\tau(\infty) = \infty$, $\tau(a) = 0$ and $\tau(b) = 1$. Hence,

$$\begin{aligned} S_3\lambda &= \left\{ \frac{c-a}{b-a} \mid a, b, c \in \{0, 1, \lambda\} \text{ distinct} \right\} \\ &= \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\} \end{aligned} \quad (3.1)$$

holds. In particular, $\#(S_3\lambda) = 6$ for almost all $\lambda \in K \setminus \{0, 1\}$. If j is given by f/g for some polynomials $f, g \in K[X]$ with $g(\mu) \neq 0$ for all $\mu \in K \setminus \{0, 1\}$, then the roots of $f - j(\lambda)g$ are given by $S_3\lambda$. Hence, it is reasonable to consider the case $\deg f = 6 > \deg g$. In fact, these conditions are sufficient:

3.2 Lemma. Let $f, g \in K[X]$ such that:

- $g(\mu) \neq 0$ for all $\mu \in K \setminus \{0, 1\}$
- $j : K \setminus \{0, 1\} \rightarrow K$ given by f/g is S_3 -invariant
- $\deg f = 6 > \deg g$, f is monic

Then $j(\lambda_1) = j(\lambda_2)$ if and only if $\lambda_1 \in S_3\lambda_2$.

Proof. Consider the subgroup

$$G := \left\{ X \mapsto \frac{c-a}{b-a} \mid a, b, c \in \{0, 1, X\} \text{ distinct} \right\} \subseteq \text{Aut}_K(K(X))$$

generalizing S_3 -invariance to $K(X)$. Since the algebraically closed field K is infinite, the identity $(f/g)(\lambda) = (\sigma(f/g))(\lambda)$ for all $\lambda \in K \setminus \{0, 1\}$ and $\sigma \in G$ implies $f/g \in K(X)^G$. Next, observe that Artin's fixed field theorem yields

$$[K(X) : K(X)^G] = \#G = 6.$$

Moreover, $K(X)/K(X)^G$ is a Galois extension with Galois group G . (For a proof of this theorem, consider [Lan02, Ch. 6 Thm. 1.8].) In particular, the minimal polynomial of X over $K(X)^G$ is given by the monic degree-six polynomial

$$f(T) - \frac{f(X)}{g(X)}g(T) = \text{mipo}_{X, K(X)^G} = \prod_{\sigma \in G} (T - \sigma(X)) \in K(X)[T]$$

Hence, any $\lambda_1, \lambda_2 \in K \setminus \{0, 1\}$ with $j(\lambda_1) = j(\lambda_2)$ satisfy

$$\begin{aligned} 0 &= f(\lambda_1) - j(\lambda_1)g(\lambda_1) = f(\lambda_1) - j(\lambda_2)g(\lambda_1) \\ &= \prod_{\sigma \in G} (\lambda_1 - \sigma(X)(\lambda_2)) = \prod_{\alpha \in S_3} (\lambda_1 - \alpha \cdot \lambda_2) \end{aligned}$$

i.e. $\lambda_1 \in S_3\lambda_2$ holds. The other implication holds by the S_3 -invariance of j . $\square$

3.3 Remark. Naive ideas for S_3 -invariant formulas might be

$$\lambda \mapsto \sum_{\mu \in S_3 \lambda} \mu \quad \text{or} \quad \lambda \mapsto \prod_{\mu \in S_3 \lambda} \mu.$$

However, these are constant functions, so they fail to classify orbits. Valid choices are

$$\lambda \mapsto \sum_{\mu \in S_3 \lambda} \mu^2 \quad \text{or} \quad \lambda \mapsto \text{sym}_6^2(S_3 \lambda),$$

where sym_6^2 denotes the second elementary symmetric polynomial in six variables. Another such function is the j -invariant:

3.4 Definition (j -invariant). Let E be an elliptic curve. Then there is a degree-two map $f : E \rightarrow \mathbb{P}^1$ (e.g. by Lemma 1.2) with branch points $0, 1, \infty, \lambda$. Finally, we define the j -invariant by

$$j(E) := 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

3.5 Remark. Using eq. (3.1), one easily checks that j is S_3 -invariant as a function of λ . Hence, $j(E)$ does not depend on the choice of f by Lemma 2.5 and Lemma 3.2. Moreover, the equation

$$j(\lambda) = 2^7 \left(\left(\sum_{\mu \in S_3 \lambda} \mu^2 \right) + 3 \right)$$

holds and the coefficient 2^8 above resolves issues arising in characteristic two. However, we explicitly excluded this case, so one should not worry about it here.

4 The main result

4.1 Theorem. Let E_1 and E_2 be elliptic curves. Then $E_1 \cong E_2$ holds if and only if $j(E_1) = j(E_2)$.

Proof. The forward implication is clear. Conversely, assume $j(E_1) = j(E_2)$. By Lemma 1.2 and Lemma 3.2, we have $E_i \cong W_i \subseteq \mathbb{P}^2$, where W_i is given by

$$y^2 = x(x - 1)(x - \lambda_i)$$

and $\lambda_1 \in S_3\lambda_2$. Hence, $\{0, 1, \lambda_1\} = \sigma(\{0, 1, \lambda_2\})$ for some $\sigma \in \text{Aut}(\mathbb{P}^1)$ fixing ∞ , i.e. we have

$$\{0, 1, \lambda_1\} = \{at + b \mid t \in \{0, 1, \lambda_2\}\}$$

for some $a, b \in K$ with $a \neq 0$. Next, observe that we can choose $c \in K$ with $c^2 = a^3$ as K is algebraically closed. Then

$$W_2 \rightarrow W_1, (x, y) \mapsto (ax + b, cy) =: (x', y')$$

is the desired isomorphism. This follows from $x = (x' - b)/a$ and

$$\begin{aligned} a^{-3}(y')^2 &= y^2 = x(x-1)(x-\lambda_2) \\ &= a^{-3}(x'-b)(x'-b-a)(x'-b-a\lambda_2) \\ &= a^{-3}(x'-\sigma(0))(x'-\sigma(1))(x'-\sigma(\lambda_2)) \\ &= a^{-3}x'(x'-1)(x'-\lambda_1). \end{aligned} \quad \square$$

4.2 Proposition. Let $\mu \in K$. Then there exists an elliptic curve such that $\mu = j(E)$.

Proof. Observe that K is algebraically closed. Hence, there is $\lambda \in K$ such that

$$2^8(\lambda^2 - \lambda + 1)^3 = \mu\lambda^2(\lambda - 1)^2$$

holds. In particular, $\text{char } K \neq 2$ yields $\lambda \neq 0, 1$. Hence, the Legendre equation $y^2 = x(x-1)(x-\lambda)$ defines an elliptic curve $E \subseteq \mathbb{P}^2$. Finally,

$$j(E) = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = \frac{\mu\lambda^2(\lambda - 1)^2}{\lambda^2(\lambda - 1)^2} = \mu$$

concludes the proof. $\square$

References

- [Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics 52. Springer New York, 1977.
- [Lan02] Serge Lang. *Algebraic Geometry*. 3rd ed. Graduate Texts in Mathematics 211. Springer-Verlag New York, 2002.
- [Vak25] Ravi Vakil. *The Rising Sea - Foundations of Algebraic Geometry*. Princeton University Press, 2025.