Today: *j*-invariant, § 2.7 p 86
- captures the property of 2 curves being isomorphic.
- endomorphism of an EC, § 2.9 p 50
- GLV scalar multiplication and multi-scalar multi. algorithm.
- Sage Math demo

What does it mean for two curves to be isomorphic?

There is an invertible change of variables between the two equations.

\[ K(C) \text{ is a function field of degree of transcendence } 1, \text{ that is there is one free variable } \]

\[ K(C) = \frac{K[X,Y]}{(f(X,Y))} \text{ where } f: F(X,Y) = 0 \text{ and } F \text{ is irreducible.} \]

\[ K(C) \text{ is a function field of degree of transcendence } 1, \text{ that is there is one free variable } \]

\[ K(C) = \frac{Q[X,Y]}{(f(X,Y))} \text{ where } f: y^2 - x^3 - ax - b = 0. \]

They are isomorphic of curves \( C_1, C_2 \) if there is a variable \( x \) that can take any degree.

Isomorphism of curves \( C_1, C_2 \) isomorphic of function fields.

That's all for the math algebraic point of view.

ISO MORPHISM.

Two elliptic curves \( E_1 \) and \( E_2 \) defined over \( K \) and given by (long) Weierstrass equations

\[ E_1: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]
\[ E_2: y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6' \]

are said to be isomorphic over \( K \) if there exist \( u, v, s, t \in K, u \neq 0, s.t. \)

the change of variables \( (x, y) \mapsto (u^3 x + v, u^3 y + u^2 s x + t) \)

transforms the equation of \( E_1 \) into the equation of \( E_2 \) (up to multi. by \( \pm 1 \) scalar).

If \( E_2 = E_1 \) this is an automorphism.

In short Weierstrass form \( \bar{E}_1: y^2 = x^3 + ax + b \) and \( \bar{E}_2: y^2 = x^3 + a' x + b \)

\( E_1 \) and \( E_2 \) are isomorphic \( \iff (x, y) \mapsto (u^2 x, u^3 y) \).

Sage Math: - isomorphism to return \((u, v, s, t)\) above.
The $j$-invariant is invariant under automorphisms.

**Definition.** $E/K: y^2 = x^3 + ax + b$ an elliptic curve.

Its $j$-invariant is

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}$$

- **well-defined as the denominator is $-\Delta = 4a^3 + 27b^2 \neq 0$**

⚠️ Two elliptic curves of the same order are not isomorphic. But isogenous: They don't necessarily have the same group structure. They don't have the same $j$-invariant.

⚠️ Two E.C. of the same $j$-invariant have the same number of points in $\bar{K}$ (algebraic closure).

**Example of non-isogenous curves:** $E_1: y^2 = x^3 - 6x + 4$ has a 2-torsion point $(2, 0)$

1. 2-torsion is \((x, y) \rightarrow \left( \frac{x^2 - 2x + 6}{x-2}, \frac{(x^2 - 4x - 2)y}{x-2} \right)
2. \(j(E_1) = 3456\)
3. \(j(E_2) = 23328\)

$$x: E_2 \sim E_1, (x, y) \rightarrow \left( \frac{x^2/4 + x + 3}{x+4}, \frac{x^3/8 + x + 1/2}{(x+4)^2} y \right)$$

### 2 special cases:

- **$j = 1728$ or $a_4 = 0$, $a_6$ any $\neq 0$ in $K$, all curves $y^2 = x^3 + a_4 x + a_6$ are isomorphic.**

- **$j = 0$ or $a_4 = 9$, $a_6 \neq 0$ any value of $K$. All curves $y^2 = x^3 + a_6$ are isomorphic over $K_{alg.}$ closure.**

**Theorem 2.19.** Let $E_1: y^2 = x^3 + a_4 x + a_6$ and $E_2: y^2 = x^3 + a_2 x + b_2$ be two elliptic curves with $j$-invariant $j_1$ and $j_2$ resp.

If $j_1 = j_2$ then there exists $\mu \neq 0$ in $\bar{K}$ s.t. $a_4 = \mu^4 a_2$, $b_2 = \mu^6 b_1$.

The transformation is $(x, y) = (\mu^2 x, \mu^3 y)$ and changes $E_1$ to $E_2$ (equivalence).

**Proof.**

$$j_1 = 1728 \cdot \frac{4a_4^3}{4a_4^3 + 27b_4^2}$$

$$j_2 = 1728 \cdot \frac{4a_2^3}{4a_2^3 + 27b_2^2}$$

Assume $a_2 \neq 0$ and $a_4 \neq 0$.

$$j_1 = j_2 \text{ and } a_2 a_4 \neq 0 \Rightarrow \frac{4a_4^3 + 27b_4^2}{4a_4^3} = \frac{4a_2^3 + 27b_2^2}{4a_2^3}$$

Let $\frac{a_4}{a_2} = \mu^4$ for some $\mu \neq 0$ in $K$, then $(\frac{a_4}{a_2})^3 = \mu^6$.

And $\frac{b_2}{b_4} = \frac{a_4}{a_2} = \pm \mu^6 = \frac{b_2}{b_4}$.

If $\frac{b_4}{b_2} = -\mu^6$, change $\mu$ into $\mu' = \mu / b_2$ to get $\frac{b_4}{b_2} = \mu' i$ and $\frac{a_4}{a_2} = \mu'^4$.

$$i^2 = -1, i^6 = 1 \text{ and } i^4 = 1.$$
\[ y^2 = x^3 + a_1 x + b_1 \quad \text{with} \quad a_1 = a \mu^4 \text{ and } b_1 = b \mu^6. \]

- The isomorphism is in an extension of \( K \) containing \( \mu. \)

**Special cases:**
- \( j = -1728, \ a_6 = 0 \quad y = x^3 + ax \) are all isomorphic. with \( \mu^4 = a, \) then
  \[ \frac{\partial y}{\partial \mu} = \frac{x^3}{\mu^6} + \frac{a}{\mu^4} x \quad \Rightarrow \quad (\frac{\partial y}{\partial \mu})^2 = (\frac{x}{\mu^2})^3 + \frac{a}{\mu^4} \frac{x}{\mu^2}. \]
- \( j = 0, \ a_4 = 0 \quad y = x^3 + bx \) are all isomorphic. with \( \mu^6 = b, \) then
  \[ \frac{\partial y}{\partial \mu} = \frac{x^3}{\mu^6} + \frac{b}{\mu^4} \quad \Rightarrow \quad (\frac{\partial y}{\partial \mu})^2 = (\frac{x}{\mu^2})^3 + (\frac{b}{\mu^4}, \frac{x}{\mu^2}). \]

Given \( j; \) there always exists a elliptic curve over \( K \) of \( j \)-invariant; namely

\[ \mathcal{E}: \quad y^2 = x^3 + \frac{3j}{1728-j} x + \frac{2j}{1728-j}. \]

**Exercise:** can we always change \( \mathcal{E}, \) \( y^2 = x^3 + ax + b \) into \( \mathcal{E}', \) \( y^2 = x^3 + bx' \) over \( K, \) \( a = -3? \)

We need \( a_4 = a \) and \( \frac{a_4}{a_2} = \mu^6 \in K. \) We need \( a_4 \) to be a 4-th power.

**Exercise:** simplify the coefficients of \( y^2 - 108x + 1512. \)

a) \( \text{gcd}(108, 1512) = 108 = 3 \cdot 3 \cdot 3, \quad 1512 = 7 \cdot 3 \cdot 3. \)

One finds \( y^2 = x^3 - 3x + 7 \) but the map is defined over \( \mathbb{Q}(\sqrt{169}). \)

SageMath example:
\[ y^2 = x^3 - 25x + 111, \quad y^2 = x^3 + 14x + 4. \]

\[ \frac{a_4}{a_2} = \frac{-25}{4} = \left(\frac{5}{2}\right)^2 \text{ but is not a 4-th power in } \mathbb{Q}. \] 101 is in \( \mathbb{Q}(\sqrt{169}). \) \( j = -1728. \)

If \( F_1 \) and \( F_2 \) have the same \( j \)-invariant; \( j(F_1) = j(F_2) \) but \( \mu \notin K \) but in some extension of \( K, \) \( F_1 \) and \( F_2 \) are TWIST of each other.
On certain curves, there are endomorphisms other than just the multiplication-by-\( m \) \([m]\) map, and Billet, Petit and Vaudene in 2001 published a paper to accelerate \([m]\) P thanks to an endomorphism.

- If an endomorphism of curves is \( (x, y) \mapsto (x, \frac{2}{y}, \frac{1}{y}) \), what is an endomorphism? (in term of rational function of \( x, y \)).
- What is the degree?

**Lemma**

\[ \alpha(x, y) = (r_1(x), r_2(x) - y) \] for two rational functions \( r_1(x), r_2(x) \).

**Proof.** Assume that \( \alpha \) is an endomorphism of \( E \) given by rational functions

\[ \alpha(x, y) = (R_1(x, y), R_2(x, y))^T \] for all \((x, y) \in E(\mathbb{K}) \).

- \( \alpha \) is a homomorphism: \( \alpha(P_0) = P_0 \).
- Assume that \( \alpha \) is non-trivial: \( \alpha(x, y) \neq P_0 \) for some \( x, y \).
- The identity map is \( \text{Id}: (x, y) \mapsto (x, y) \).
- \( y^d \) for any \( d > 1 \) can be replaced by \( y^{(d \mod 2)} \).

\[ d = (d \mod 2) + 2 \frac{d}{2} \]

\[ y^d = y^{(d \mod 2)} \cdot y^{2 \frac{d}{2}} = y^{(d \mod 2)} \cdot (x^2 + Ax + b)^{\frac{d}{2}} \]

\[ m \neq 0 \implies d \mod 2 = \begin{cases} 0 & \text{if } d \quad \text{is even} \\ 1 & \text{if } d \quad \text{is odd} \end{cases} \]

Any even power of \( y \) can be replaced by a function in \( x \), any odd power of \( y \) by \( y \) times any even power of \( x \).

\[ R_1(x, y) = \frac{P_1(x) + P_2(x) y}{P_3(x) + P_4(x) y}, \quad R_2(x, y) = \frac{P_3(x) - P_4(x) y}{P_5(x) - P_6(x) y} \]

\[ \alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2), \]

Now, \( \alpha(x, y) = -\alpha(x, -y) \) if

\[ \begin{pmatrix} q_1(x) - q_2(x) y \\ q_3(x) \end{pmatrix} = \begin{pmatrix} q_4(x) - q_5(x) y \\ q_6(x) \end{pmatrix} \]

\[ R_1(x, y) = R_1(x, -y) \quad \text{and} \quad R_2(x, -y) = -R_2(x, y) \]

\[ \begin{pmatrix} q_1(x) \\ q_3(x) \end{pmatrix}, \quad \begin{pmatrix} q_4(x) \\ q_6(x) \end{pmatrix} \cdot y \begin{pmatrix} r_1(x), \ r_2(x) y \end{pmatrix} \]

\[ \square \]
Exercise 2.19 shows that if \( r_1(x) = \frac{\Phi(x)}{q(x)} \) and \( q(x) \) is defined (\( \neq 0 \)),
then \( r_2(x) = \frac{r(x)}{q(x)} \) is defined: \( r(x) \neq 0 \).

If \( q(x_0) = 0 \), then \( \alpha(x_0, y_0) = \infty \).

Definition. The degree of \( \alpha \) is \( \deg(\alpha) = \max(\deg(p(x)), \deg(q(x))) \).

Let \( \alpha: (x, y) \rightarrow (r_1(x), r_2(x), y) \) and \( r_1(x) = \frac{p(x)}{q(x)} \).

\( \alpha \) is SEPARABLE if the derivative \( r_4'(x) \) is not 0.

(Ex. 2.2, remember that \( \frac{p(x)}{q(x)}' = \frac{p'(x)q(x) - p(x)q'(x)}{q^2(x)} \).

In characteristic \( p \): if \( p = 0 \) in \( \mathbb{F}_p \), \( f(x) = \sum_{i=0}^{\infty} a_i x^i \) \( f'(x) = \sum_{i=2}^{\infty} a_i i x^{i-1} \).

\( f'(x) \) is identically 0 if \( a_i i = 0 \) for all \( 1 \leq i \leq n \), but since \( a_i \) are not all 0, then \( p \mid i \) for all \( i \), and \( f(x) = \sum_{j=0}^{\infty} a_j x^{p^j} \) \( = g(x^p) \).

Example: The multiplication by 2 is an endomorphism of degree 2. Read p. 52.

The Frobenius endomorphism. Let \( E \) be an elliptic curve defined over a field \( \mathbb{F}_p \).

Definition. The Frobenius map is \( \text{Frob}: E(\mathbb{F}_p) \rightarrow E(\mathbb{F}_p) \)
\( (x, y) \rightarrow (x^p, y^p) \) where \( p = \text{char}(\mathbb{F}_p) \).

Ferdinand Georg Frobenius 1849-1917.

Proposition. \( \text{Frob} \) is an endomorphism.

\( \text{Frob} \) is inseparable of degree \( p \).

Proof of \( \text{Frob} \) being an endomorphism. Check that \( \text{Frob}(P + Q) = \text{Frob}(P) + \text{Frob}(Q) \), \( \text{Frob}(P) = 2P \).

i.e. \( \text{Frob} \) commutes with addition and doubling.

Takes the addition formulas (p. 14):
\[
\lambda = \begin{pmatrix}
\lambda_1 - \lambda_2 \\
\lambda_1 - \lambda_2 \\
3 \lambda_1^2 + A \\
2 y_1
\end{pmatrix}
\]
\( x_3 = \lambda^2 - x_1 - x_2 \)
\( y_3 = \lambda(x_1 - x_3) - y_1 \)

\( \text{Frob}(P + Q) = (x_3^p, y_3^p) = \left( (\lambda^2 - x_1 - x_2)^p, (\lambda(x_1 - x_3)^p - y_1)^p \right) \).

Remember that \( (a + b)^p = a^p + b^p \) in \( \mathbb{F}_p \).

Indeed, \( (a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i C_i^p \) where \( C_i^p = \frac{p!}{i!(p-i)!} \).

Hence, \( \text{Frob}(P + Q) = \text{Frob}(P) + \text{Frob}(Q) \) for \( P \neq Q \).

Doubling:
\[
\left( \frac{3 x_1^2 + A}{2 y_1} \right)^p = \left( \frac{3 x_1^2 + A}{2^p y_1^p} \right) = \frac{3 x_1^2 + A}{2 y_1^p}
\]
\( 2^p \).

Important point is \( A^p = A \) because \( A \in \mathbb{F}_p \), the field of definition of \( E \).

We proved that \( \text{Frob} \) is an endomorphism.

\( \text{Frob} \) is of degree \( p \) because it is given by \( p \) polynomials of degree \( p \).

\( \text{Frob} \) is not separable: \( f'(x) = x^p, f'(x) = p x^{p-1} = 0 \) in \( \mathbb{F}_p[x] \), hence not separable.
Proposition 2.24.

Let \( \alpha \neq 0 \) be an separable endomorphism of an elliptic curve \( E \). Then

\[
\deg(\alpha) = \# \text{Ker}(\alpha)
\]

where \( \text{Ker}(\alpha) \) is the kernel of the homomorphism \( \alpha : E(K) \to E(K) \). (That is, the preimage of \( \text{ker} \).)

If \( \alpha \neq 0 \) is not separable, then \( \deg(\alpha) > \# \text{Ker}(\alpha) \).