Today: • j-invariant, § 2.7 p 46
→ captures the property of 2 curves being isomorphic.
• endomorphism of an EC, § 2.9 p 50
• GLV scalar multiplication and multi-scalar mult. algorithm.
• Sage Math demos
• exercices in Washington's book : 2.13, 2.17, 2.19, 2.23.

What does it mean for two curves to be isomorphic?
→ there is an invertible change of variables between the two equations.

$K(\mathcal{C})$ is a function field of degree of transcendance 1, that is there is one "free variable"
$K(\mathcal{C}) = \text{Frac}(K[X,Y]/(F(X,Y)))$ where $\mathcal{C}$: $F(X,Y)=0$ and F is irreducible.
(Frac = field of fractions of the quotient ring)

like for $K(t)$ where t is a variable. Notation: $K[t]$ is a polynomial ring, $K(t)$ is a function field, like $\mathbb{Q}[i]$ versus $\mathbb{Q}(i)$. ← with inversion and here moreover it's with $i^2=-1$.
↑ without considering inversion (or a field of fractions...)

$K(x,y)/(f(x,y))$ where f: $y^2-x^3-ax-b=0$.

it's like $K(x)[Y]/(Y^2-x^3-ax-b)$ one variable x that can take any degree.

isomorphism of curves $\mathcal{C}_1, \mathcal{C}_2$ ⟷ isomorphism of their function fields.

that's all for the math / algebraic point of view.

ISOMORPHISM of curves of $\mathbb{P}^2(K)$.

Two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ defined over K and given by (long) Weierstraß equations

$\mathcal{E}_1$: $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$

$\mathcal{E}_2$: $y^2+a_1'xy+a_3'y = x^3+a_2'x^2+a_4'x+a_6'$

are said to be isomorphic over K if there exist $u, r, s, t \in K$, $u \neq 0$, s.t.
the change of variables $(x,y) \longmapsto (u^2x+r,\ u^3y+u^2sx+t)$
transforms the equation of $\mathcal{E}_1$ into the equation of $\mathcal{E}_2$ (up to mult. by $\neq 0$ scalar).
if $E_2 = E_1$ this is an automorphism.

In short Weierstraß form $\mathcal{E}_1$: $y^2=x^3+ax+b$ and $\mathcal{E}_2$: $y^2=x^3+a'x+b$,
$\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic $\Leftrightarrow$ $(x,y) \mapsto (u^2x, u^3y)$.

+ Sage Math : .isomorphism_to returns (u,r,s,t) above.

The j-invariant is invariant under isomorphisms.

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

Its j-invariant is $$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- 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 have necessarily 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 $\overline{K}$ (algebraic closure).

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

a 2-isogeny is $(x,y) \mapsto \left(\frac{x^2-2x+6}{x-2}, \frac{(x^2-4x-2)}{(x^2-4x+4)} y \right) = \left(\frac{(x-2)^2 + 2x + 2}{x-2}, \frac{x^2-4x-2}{(x-2)^2} \right)$

$= (x-2)^2$

$j(E_1) = 3456$

$j(E_2) = 23328$

$\hat{\imath} : E_2 \to E_1, \quad (x,y) \mapsto \left(\frac{x^2/4 + x + 3}{x+4}, \frac{x^2/8 + x + 1/2}{(x+4)^2} y \right)$

2 special cases:
- $j = 1728 \iff a_6 = 0$, a_4 any $\neq 0$ in K. all curves $y^2 = x^3 + a_4 x$ are isomorphic.
- $j = 0 \iff a_4 = 0$, $a_6 \neq 0$ any value of K. All curves $y^2 = x^3 + a_6$ are isomorphic over $\overline{K}$ alg. closure.

Theorem 2.19. Let $E_1 : y_1^2 = x_1^3 + a_1 x_1 + b_1$ and $E_2 : y_2^2 = x_2^3 + a_2 x_2 + b_2$ be two elliptic curves with j-invariants j_1 and j_2 resp.
If $j_1 = j_2$ then there exists $\mu \neq 0$ in $\overline{K}$ s.t. $a_2 = \mu^4 a_1$, $b_2 = \mu^6 b_1$.
The transformation is $(x_2, y_2) = (\mu^2 x_1, \mu^3 y_1)$ and changes E_1 to E_2. (equation).

PROOF.

$$j_1 = 1728 \frac{4a_1^3}{4a_1^3 + 27b_1^2} \qquad j_2 = 1728 \frac{4a_2^3}{4a_2^3 + 27b_2^2}$$

assume $a_2 \neq 0$ and $a_1 \neq 0$.

$$j_1 = j_2 \text{ and } a_1 a_2 \neq 0 \iff \frac{4a_1^3 + 27b_1^2}{4a_1^3} = \frac{4a_2^3 + 27b_2^2}{4a_2^3} \iff 1 + \frac{27b_1^2}{4a_1^3} = 1 + \frac{27b_2^2}{a_2^3}$$

$$\iff \boxed{\frac{b_1^2}{b_2^2} = \frac{a_1^3}{a_2^3}}$$

Let $\frac{a_1}{a_2} = \mu^4$ for some $\mu \neq 0 \in \overline{K}$, then $\left(\frac{a_1}{a_2}\right)^3 = \mu^{12}$

and $\mu^{12} = \frac{b_1^2}{b_2^2} \Rightarrow \pm \mu^6 = \frac{b_1}{b_2}$.

if $\frac{b_1}{b_2} = -\mu^6$, change μ into $\mu' = i\mu$ to get $\frac{b_1}{b_2} = \mu'^6$ and $\frac{a_1}{a_2} = \mu'^4$.

$i^2 = -1$, $i^6 = -1$ and $i^4 = 1$.

note that: $\mathcal{E}_1 : y_1^2 = x_1^3 + a_1 x_1 + b_1 \quad \times \mu^6$:

$$y_1^2 \mu^6 = x_1^3 \mu^6 + a_1 x_1 \mu^6 + b_1 \mu^6$$

$$\Leftrightarrow (y_1 \mu^3)^2 = (x_1 \mu^2)^3 + a_1 \mu^4 (x_1 \mu^2) + b_1 \mu^6$$

$$(x_1, y_1) \longmapsto (x_1 \mu^2, y_1 \mu^3)$$

$$\mathcal{E}_1 \longrightarrow y_2^2 = x_2^3 + a_2 x_2 + b_2 \quad \text{with } a_2 = a_1 \mu^4 \text{ and } b_2 = b_1 \mu^6$$

⚠ the isomorphism is in an extension of K containing μ.

special cases: $j = 1728$, $a_6 = 0$ $y = x^3 + ax$ are all isomorphic. with $\mu^4 = a$, then

$$\frac{y^2}{\mu^6} = \frac{x^3}{\mu^6} + \frac{a}{\mu^4}\frac{x}{\mu^2} \Leftrightarrow \left(\frac{y}{\mu^3}\right)^2 = \left(\frac{x}{\mu^2}\right)^3 + \frac{a}{\mu^4}\frac{x}{\mu^2} \Leftrightarrow y'^2 = x'^3 + x'$$

$j = 0$, $a_4 = 0$ $y = x^3 + b$ are all isomorphic. with $\mu^6 = b$, then

$$\frac{y^2}{\mu^6} = \frac{x^3}{\mu^6} + \frac{b}{\mu^6} \Leftrightarrow y'^2 = x'^3 + 1, \quad (x, y) \mapsto \left(\frac{x}{\mu^2}, \frac{y}{\mu^3}\right).$$

Given j, there always exists $\mathcal{E}$ elliptic curve over K of j-invariant j, 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 $\mathcal{E}': y'^2 = x'^3 + \underbrace{-3}_{a_1 = a}x' + b'$? over K $a = -3$?

We need $\frac{a_1}{a_2} = \mu^4 \in K$. We need $\frac{a_1}{a_2}$ to be a 4-th power.

Exercice: simplify the coefficients of $y^2 = x^3 - 108x + 1512$.

a) $\gcd(-108, 1512) = 108 = -3 \cdot 6^2$. $1512 = 7 \cdot 6^3$.

one find $y^2 = x^3 - 3x + 7$ but the map is defined over $\mathbb{Q}(\sqrt{6})$.

SageMath example: $y^2 = x^3 - 25x$ / $\mathbb{Q}$, $y^2 = x^3 - 4x$ / $\mathbb{Q}$.

$\frac{a_1}{a_2} = \frac{-25}{-4} = \left(\frac{5}{2}\right)^2$ but is not a 4-th power in $\mathbb{Q}$. is is in $\mathbb{Q}(\sqrt{10})$. $j = 1728$.

If $\mathcal{E}_1$ and $\mathcal{E}_2$ have the same j-invariant: $j(E_1) = j(E_2)$ but $\mu \notin K$ but in some extension of K, $\mathcal{E}_1$ and $\mathcal{E}_2$ are TWIST of each other.

ENDOMORPHISMS. Washington p. 51.

On certain curves, there are endomorphisms other than just the multiplication-by-m $[m]$ map, and Ballard, Lambert and Vanhove in 2001 published a paper to accelerate $[m]P$ thanks to an endomorphism.

- if an isomorphism of curves is $(x,y) \mapsto (x\mu^2, y\mu^3)$, what is an endomorphism? (in term of rational function of x, y).
- what is the degree?

Lemma $\alpha(x,y) = (r_1(x), r_2(x)\cdot y)$ for two rational functions $r_1(x), r_2(x)$.

Proof. Assume that α is an endomorphism of E given by rational function

$$\alpha(x,y) = \left(R_1(x,y), R_2(x,y)\right) \text{ for all } (x,y) \in E(\bar{K}).$$

- α is a homomorphism: $\alpha(P_\infty) = P_\infty$
- assume that α is non-trivial: $\alpha(x,y) \neq P_\infty$ for some x,y.
- the identity map is $Id: (x,y) \mapsto (x,y)$.
- y^d for any $d > 1$ can be replaced by $y^{(d \bmod 2)} \cdot$ [illegible]$^{\lfloor d/2 \rfloor}$

$$d = (d \bmod 2) + 2\cdot\lfloor d/2 \rfloor.$$

$$y^d = y^{d \bmod 2} \cdot y^{2\cdot\lfloor d/2 \rfloor} = y^{d \bmod 2} \cdot (x^3 + Ax + b)^{\lfloor d/2 \rfloor}$$

where $d \bmod 2 = \begin{cases} 0 \\ 1 \end{cases}$.

$\Rightarrow$ any even power of y can be replaced by a function in x, any odd power of y by y times a function in x.

$$\Rightarrow R_1(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} \cdot \frac{p_3(x) - p_4(x)y}{p_3(x) - p_4(x)y} = \frac{p_1p_3(x) - p_2p_4(x^3+ax+b) + (p_2p_3 - p_1p_4)y}{p_3^2(x) - p_4^2(x)(x^3+ax+b)}$$

$$\alpha(P_1+P_2) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

$\alpha(P_1) + \alpha(P_2)$,

Now, $\alpha(x,y) = -\alpha(x,y) \iff \left(\frac{q_1(x)(-q_2(x)y)}{q_3(x)}, \frac{q_4(x) - q_5(x)y}{q_6(x)}\right) = \left(\frac{q_1 + q_2 y}{q_3}, \frac{-q_4}{q_6}\right)$

$R_1(x,y) = R_1(x,-y)$ and $R_2(x,-y) = -R_2(x,y)$

$$\Rightarrow \left(\frac{q_1(x)}{q_3(x)}, \frac{q_5(x)}{q_6(x)}y\right) = \left(r_1(x), r_2(x)y\right) \qquad \square.$$

Exercice 2.19 shows that if $r_1(x) = \frac{p(x)}{q(x)}$ and $q(x_0)$ is defined ($\neq 0$),
then $r_2(x) = \frac{r(x)}{s(x)}$ is defined: $s(x_0) \neq 0$.

- if $q(x_0) = 0$, then $\alpha(x_0, y_0) = P_\infty$.

Definition. The degree of α is $\deg(\alpha) = \text{Max}\left(\deg(p(x)), \deg(q(x))\right)$.
where $\alpha: (x,y) \mapsto (r_1(x), r_2(x)\,y)$ and $r_1(x) = \frac{p(x)}{q(x)}$.

α is SEPARABLE if the derivative $r_1'(x)$ is not 0.

(ex 2.2, remember that $\left(\frac{p(x)}{q(x)}\right)' = \frac{p'(x)q(x) - p(x)q'(x)}{q^2(x)}$.)

in characteristic p: that is, $p = 0$ in $\mathbb{F}_p$: $f(x) = \sum_{i=0}^{n} a_i x^i$ $\quad f'(x) = \sum_{i=1}^{n} a_i \cdot i \cdot x^{i-1}$

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

Example: the multiplication by 2 is an endomorphism of degree 2. read p. 52.

The Frobenius endomorphism. Let E an elliptic curve defined over a finite field $\mathbb{F}_p$.

Definition. The Frobenius map is $\pi_p : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$
$(x,y) \mapsto (x^p, y^p)$ where $p = \text{order}(\mathbb{F}_p)$.
p can be a prime power.
Useful in characteristic 2.

Ferdinand Georg Frobenius. 1849-1917.

Proposition. • π_p is an endomorphism.
• π_p is inseparable of degree p.

Proof of π_p being an endomorphism. check that $\pi_p(P+Q) = \pi_p(P) + \pi_p(Q)$, $\pi_p(2P) = 2\pi_p(P)$.
i.e. π_p commutes with addition and doubling.

take the addition formulas: (p14)

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} \\ \frac{3x_1^2 + A}{2y_1} \end{cases}$$

$x_3 = \lambda^2 - x_1 - x_2$
$y_3 = \lambda(x_1 - x_3) - y_1$

$\pi_p(P+Q) = (x_3^p, y_3^p) = \left((\lambda^2 - x_1 - x_2)^p, (\lambda(x_1 - x_3) - y_1)^p\right)$

remember that $(a+b)^p = a^p + b^p$ in $\mathbb{F}_{p^k}$.

indeed, $(a+b)^p = \sum_{i=0}^{p} a^{p-i} b^i C_p^i$ where $C_n^p = \frac{p!}{n!(p-n)!} = \binom{p}{n}$

hence, $\pi_p(P+Q) = \pi_p(P) + \pi_p(Q)$ for $P \neq Q$.

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

the important point is $A^p = A$ because $A \in \mathbb{F}_p$ the field of definition of E.

We proved that π_p is an endomorphism.
π_p is of degree p because is it given by polynomials of degree p.
π_p is not separable: $f(x) = x^p$, $f'(x) = p\,x^{p-1} = 0$ in $\mathbb{F}_p[X]$, hence not separable. □

Proposition 2.21.

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

$$\deg(\alpha) = \#\ker(\alpha)$$

where $\ker(\alpha) = \{P \in E(\bar{K}),\ \alpha(P) = P_\infty\}$. (that is, the preimage of P_∞).

if $\alpha \neq 0$ is not separable, then $\deg \alpha > \#\ker(\alpha)$.