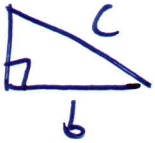
Elliptic Curves: Lecture 1 — 19/01/2024

§1: Fermat's method of Infinite Descent.

DEF Δ (right-angled) 

is • rational if $a,b,c \in \mathbb{Q}$

• Primitive if $a,b,c \in \mathbb{Z}$ coprime ($\Leftrightarrow$ pairwise coprime)

Lemma 1.1 Every primitive Δ is of form: $(2uv, u^2-v^2, u^2+v^2)$

for $u,v \in \mathbb{N}$, $u>v>0$.

Proof WLOG a odd, b even $\Rightarrow$ c odd

$\Rightarrow \left(\frac{b}{2}\right)^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$. RHS is product of coprime integers.

$\Rightarrow$ By unique fact. of $\mathbb{Z}$: both factors on RHS squares,

so $\frac{c-a}{2} = v^2$, $\frac{c+a}{2} = u^2$. Rearrange ✓

DEF $D \in \mathbb{Q}_{>0}$ congruent number $\Leftrightarrow \exists$ rational Δ with area $(\Delta) = D$. (Only care about D squarefree integer)

E.g. 6 is congruent ($(3,4,5)$-triangle)

Lemma 1.2 D congruent $\Leftrightarrow Dy^2 = x^3 - x$ for some $x,y \in \mathbb{Q}$ $(y \neq 0)$.

Proof By Lemma 1.1: D congruent

$\Leftrightarrow Dw^2 = uv(u^2-v^2)$. Then $(x,y) = \left(\frac{u}{v}, \frac{w}{v^2}\right)$. ✓

Fermat showed: 1 not congruent number.

Theorem 1.3 $\nexists$ solution to: $w^2 = uv(u+v)(u-v)$, $u,v \in \mathbb{Z}$, $w \neq 0$.

Proof WLOG u,v coprime. & $u,w>0$.

If $v<0$: replace $(u,v,w) \mapsto (-v,u,w)$, so WLOG $v>0$.
If u,v both odd: replace $(u,v,w) \mapsto \left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$
so WLOG u,v not both odd.

$\Rightarrow$ $u, v, u+v, u-v$ pairwise coprime integers (positive), with product square. So, all squares. $u=a^2$, $v=b^2$, $u+v=c^2$, $u-v=d^2$

Since $u \not\equiv v \bmod 2$: $\Rightarrow$ c,d both <u>odd</u>.

$\Rightarrow \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = u = a^2$.

So, $\left(\frac{c-d}{2}, \frac{c+d}{2}, a\right)$ is Pythagorean, and furthermore: <u>primitive</u>

With area: $\frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b}{2}\right)^2$.

If $w_1 \equiv \frac{b}{2}$, then by <u>lemma 1.1</u>: $w_1^2 = u_1 v_1 (u_1+v_1)(u_1-v_1)$

for some $u_1, v_1 \in \mathbb{Z}$, hence: new solution.

But: $w_1 = \frac{b}{2}$, so $4w_1^2 = b^2 = v \leq w^2$ $\Rightarrow w_1 \leq \frac{1}{2}w$

$\Rightarrow$ Contradiction by Infinite Descent ✓

<u>Variant for Polynomials.</u>

<u>Let</u>: K field, $\mathrm{char}(K) \neq 2$ & $\bar{K}$ algebraic closure of K.

<u>lemma 1.4</u> $u, v \in K[t]$ coprime. If $\alpha u + \beta v$ is square for 4 distinct choices $(\alpha,\beta) \in \mathbb{P}^1_K$, then u,v constant polys.

<u>Proof</u> WLOG $K = \bar{K}$. & Find change of coords of $\mathbb{P}^1_K$

so WLOG the (α,β)'s are: $(1:0)$, $(0:1)$, $(1:-1)$, $(1:-\lambda)$.

$\lambda \in K \setminus \{0,1\}$.

So: $u=a^2$, $v=b^2$, $u-v=(a+b)(a-b)$,

$u-\lambda v=(a+\mu b)(a-\mu b)$, $\mu^2=\lambda$.

By UFD of $k[t]$: $a+b$, $a-b$ squares of polynomials.

$\Rightarrow a+b$, $a-b$, $a+\mu b$, $a-\mu b$ are all squares.

But: $\max(\deg a, \deg b) \leq \frac{1}{2}\max(\deg u, \deg v)$.

$\Rightarrow$ By Fermat's method: $u, v \in k$ ✓

DEF 1.5 (i) An elliptic curve E/K is: projective closure of plane affine curve: $y^2=f(x)$, where $f \in K[X]$ is monic + cubic poly, distinct roots. (in $\bar{K}$)

(ii) $\forall$ L/K field ext: $E(L)=\{(x,y)\in L^2 : y^2=f(x)\} \cup \{0\}$

Fact: $E(L)$ is: Abelian group, identity O.

In this course: study $E(K)$ for K finite field / local field / number field.

By lemma 1.2 + Thm 1.3: if E determined by $y^2=x^3-x$ then $E(\mathbb{Q})=\{0,(0,0),(\pm 1,0)\} \cong C_2 \times C_2$.

Corollary 1.6 E/K elliptic curve. Then: $E(K(t))=E(K)$.

Proof WLOG $K=\bar{K}$. By change of coords: WLOG assume $y^2=x(x-1)(x-\lambda)$, $\lambda \in K\setminus\{0,1\}$.

If $(x,y)\in E(K(t))$, write: $x=\frac{u}{v}$, $u,v\in K[t]$ coprime.

$\Rightarrow \omega^2 = uv(u-v)(u-\lambda v)$. $u, v \in K[t]$. $\Rightarrow \omega \in K[t]$

By unique fact. of $K[t]$: all 4 terms on RHS squares.

$\Rightarrow$ By lemma 1.4: u, v constant, so x, y constant.

Elliptic Curves: lecture 2 22/01/2024.

§2: Remarks on Algebraic Curves. (over $k=\bar{k}$)

DEF 2.1 Plane curve $C=\{f(x,y)=0\}\subseteq \mathbb{A}^2$ (for $f\in k[x,y]$ irred) is: rational $\Leftrightarrow$ has rational parametrisation, i.e.

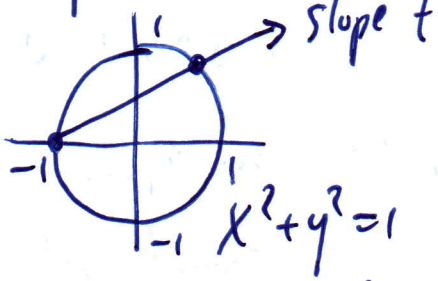
$\exists\ \phi,\psi\in k(t)$ s.t.

i) $\mathbb{A}^1 \longrightarrow \mathbb{A}^2$, $t\longmapsto(\phi(t),\psi(t))$ injective on $\mathbb{A}^1-\{\text{finite \# of pts}\}$

ii) $f(\phi(t),\psi(t))=0\ \ \forall t\in\mathbb{A}^1$

Example 2.2 a) Any nonsingular conic is rational.

Example: circle.



$y=t(x+1)$ & $x^2+y^2=1$.

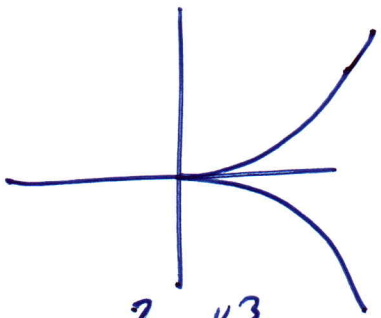
$\Rightarrow x^2+t^2(x+1)^2=1$

$\Rightarrow (x+1)(x-1+t^2(x+1))=0$

$\Rightarrow x=-1$ or $x=\frac{1-t^2}{1+t^2}$.

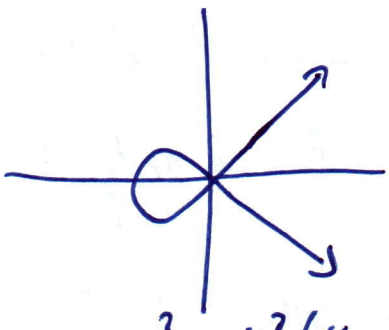
So, get param $(x,y)=\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$.

b) Any nonsingular Cubic is rational.



$y^2=x^3$

$\Rightarrow (x,y)=(t^2,t^3)$



$y^2=x^2(x+1)$ (example sheet)

c) Corollary 1.6 $\Rightarrow$ Elliptic curves are not rational.

Remark 2.3 Genus $g(C) \in \mathbb{Z}_{\geq 0}$ an invariant of smooth projective curve C.

(i) If $k = \mathbb{C}$ $\Rightarrow$ genus = genus of corresponding Riemann surf.

(ii) A smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus $\frac{(d-1)(d-2)}{2}$

Prop 2.4 (still assuming $k = \bar{k}$): let C smooth proj curve.

(i) C rational (def 2.1) $\Leftrightarrow g(C) = 0$

(ii) C is elliptic curve (def 1.5) $\Leftrightarrow g(C) = 1$

Proof (i) omitted

(ii) $\Rightarrow$: Check C is smooth proj curve in $\mathbb{P}^2$ (example sheet) & use Remark 2.3

$\Leftarrow$: Later!

Order of Vanishing C algebraic curve & $P \in C$ smooth pt.

Write: $\mathrm{ord}_P(f) \equiv$ order of vanishing of $f \in k(C)$ at P (is negative, if f has pole here).

Fact: $\mathrm{ord}_P : k(C)^\times \longrightarrow \mathbb{Z}$ discrete val.

& $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$

& $\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$.

Say $t \in k(C)^\times$ uniformiser at $P \Leftrightarrow \mathrm{ord}_P(t) = 1$.

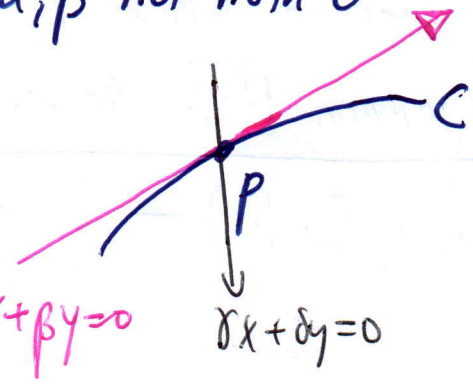
Example 2.5 $C = \{g = 0\} \subseteq \mathbb{A}^2$, $g \in k[x,y]$.

$\Rightarrow k(C) = \mathrm{FF}(k[x,y]/(g))$. Write: $g = g_0 + g_1 + g_2 + \cdots$ (g_i degree i homog.)

Then: if $P = (0,0)$ smooth pt:

$\Rightarrow g_0 = 0$ and $g_1(x,y) = \alpha x + \beta y$, α, β not both 0

For $\gamma, \delta \in k$: Fact: $\gamma x + \delta y \in k(C)$ is a unif. at $P \Leftrightarrow \alpha\delta - \beta\gamma \neq 0$.



Example 2.6 $\{y^2 = x(x-1)(x-\lambda)\} \subseteq \mathbb{A}^2$. ($\lambda \neq 0, 1$)

$\Rightarrow$ Projective Closure: $\{y^2 z = x(x-z)(x-\lambda z)\} \subseteq \mathbb{P}^2$

$\Rightarrow$ Only pt at ∞ is $(0:1:0)$.

Aim: compute $\mathrm{ord}_P(x)$, $\mathrm{ord}_P(y)$ at $P = (0:1:0)$.

If put $t = \frac{x}{y}$ & $\omega = \frac{z}{y}$ then $\omega = t(t-\omega)(t-\lambda\omega)$, $P = (0,0)$.

Is: smooth pt, & each factor on RHS are uniformizers, so have order 3. So, $\mathrm{ord}_P(\omega) = 3 \Rightarrow \mathrm{ord}_P(x) = -2$, $\mathrm{ord}_P(y) = -3$.

Riemann-Roch Spaces.

Let C smooth proj curve.

DEF Divisor $\equiv$ Formal sum of pts of C. $D = \sum_{P \in C} n_P \cdot P$ ($n_P \in \mathbb{Z}$)

(& finitely many n_P are nonzero)

D effective $\Leftrightarrow D \geq 0 \Leftrightarrow n_P \geq 0 \ \forall P \in C$.

& $\forall f \in k(C)^\times$ then $\mathrm{div}(f) = \sum_{P \in C} \mathrm{div}_P(f) \cdot P$. (finite sum)

The Riemann Roch space of divisor $D \in Div(C)$ is:

$$\mathcal{L}(D) = \{ f \in k(C)^{\times} : div(f) + D \geq 0 \} \cup \{0\}.$$

Is: a k-Vector Space of rational functions in C.

"functions whose poles are no worse than in D".

Riemann Roch theorem, $g=1$

$$\dim_{\mathbb{C}}(\mathcal{L}(D)) = \begin{cases} \deg(D), & \text{if } \deg(D) > 0 \\ 0 \text{ or } 1 & \text{if } \deg(D) = 0 \\ 0 & \text{if } \deg(D) < 0. \end{cases}$$

Example 2.6 (Revisited) $\mathcal{L}(2P) = \langle 1, x \rangle$. $\mathcal{L}(3P) = \langle 1, x, y \rangle$.

Elliptic Curves: lecture 3.

Prop 2.7 $C \subseteq \mathbb{P}^2$ smooth plane cubic & $P \in C$ point of inflection.
Then, can change coords s.t. $C: Y^2Z = X(X-Z)(X-\lambda Z)$,
for some $\lambda \neq 0, 1$.

Proof Change coords, s.t. $P = (0:1:0)$ & $T_P C = \{Z=0\}$.
$\Rightarrow C = \{F(X,Y,Z)=0\} \subset \mathbb{P}^2$.
Since P inflection: $F(t,1,0) = c \cdot t^3$. $\Rightarrow$ F has terms:
X^2Y, XY^2 or Y^3. being 0.
$\Rightarrow F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$.
(Y^2Z: coeff $\neq 0$; X^3: coeff $\neq 0$, else $Z \mid F$.)
Rescale X, Y, Z s.t. $C: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$.
Sub $Y \leftarrow Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$. $\Rightarrow$ WLOG: $a_1 = a_3 = 0$.
$\Rightarrow C: Y^2Z = Z^3 f(\frac{X}{Z})$, f some cubic.
Since f smooth: has distinct roots. WLOG $0, 1, \lambda$.
$\Rightarrow Y^2Z = X(X-Z)(X-\lambda Z)$ ✓

Remark May be shown: points of inflection of a plane curve $C: \{F(X_1, X_2, X_3)=0\} \subseteq \mathbb{P}^2$ are given by:
$F=0$ & $\det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right) = 0$. (Hessian)

Degree of morphism. Let $\Phi: C_1 \to C_2$ map of smooth proj curves.

Then: $\phi^*: K(C_2) \longrightarrow K(C_1)$.

DEF i) $\deg(\phi) = [K(C_1) : \phi^* K(C_2)]$.

ii) ϕ separable if $K(C_1)/\phi^* K(C_2)$ separable ext.

iii) Suppose $P \in C_1$, $Q \in C_2$ & $\phi(P) = Q$. & $t \in K(C_2)$ unif at Q.

DEF $e_\phi(P) = Ord_P(\phi^* t)$. (Always ≥ 1, indep of t).

Theorem 2.8 $\phi: C_1 \to C_2$ nonconst morphism of smooth proj curves. Then, $\sum_{\phi(P)=Q} e_\phi(P) = \deg(\phi)$ $\forall Q \in C_2$.

Moreover: If ϕ separable then $e_\phi(P) = 1$ for all but fin many P.

In particular: i) ϕ surjective (on $\bar{K}$-points)

ii) $\# \phi^{-1}(Q) \leq \deg(\phi)$

iii) If ϕ Separable then equality holds for ii) for all but finitely many $Q \in C_2$.

Remark 2.9 If C algebraic curve: rational map is given by

$\phi: C \dashrightarrow \mathbb{P}^n$, $P \mapsto (f_0 : \cdots : f_n)$. $f_i \in K(C)$ not all 0.

Fact: If C smooth then ϕ morphism (Part II AG).

§3: Weierstrass Equations. (In §3: k perfect field, not necessarily alg closed)

DEF An elliptic curve E/K is: smooth + proj curve, genus 1, defined over K & with specified K-rational pt O_E.

Example $\{\{X^3 + pY^3 + p^2Z^3 = 0\} \subseteq \mathbb{P}^2$ NOT elliptic curve over $\mathbb{Q}$, since it has no $\mathbb{Q}$-rational point.

Theorem 3.1 Every elliptic curve E is isomorphic to a curve in Weierstrass form via some isomorphism taking $O_E \to (0:1:0)$.

Remark Prop 2.7 = special case where E smooth plane cubic & O_E = pt of inflection.

Fact If $D \in \mathrm{div}(E)$ defined over k ($\Leftrightarrow$ fixed by $\mathrm{Gal}(\bar{k}/k)$), then: $\mathcal{L}(D)$ has basis in $k(E)$. (not just $\bar{k}(E)$)

Proof (of Theorem 3.1). Have: $\mathcal{L}(2O_E) \subseteq \mathcal{L}(3O_E)$.

Basis: $\{1, x\} \subseteq \{1, x, y\}$.

$\Rightarrow \mathrm{ord}_{O_E}(x) = -2$, $\mathrm{ord}_{O_E}(y) = -3$.

$\Rightarrow$ The 7 elements $1, x, y, x^2, xy, x^3, y^2$ are in $\mathcal{L}(6O_E)$ of dimension 6, so $\exists$ linear dependence.

& If leave out x^3 or y^2, all 6 remaining terms different order of vanishing at O_E.

$\Rightarrow$ Coeff of x^3, y^2 nonzero. ($a_i \in k \ \forall i$).

& Rescale x, y to get: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Let: E' the curve defined by this equation. (or its proj closure)

Need to show: E, E' isomorphic.

There is morphism $E \longrightarrow E' \subset \mathbb{P}^2$

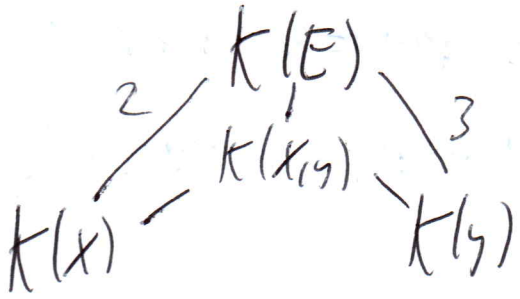
$$P \longmapsto (x(P) : y(P) : 1) = \left(\frac{x}{y} : 1 : \frac{1}{y}\right).$$

$$O_E \longmapsto (0:1:0).$$

$$[k(E) : k(x)] = \deg\left(E \xrightarrow{x} \mathbb{P}^1\right) = \mathrm{ord}_{O_E}\left(\frac{1}{x}\right) = 2$$

$\Rightarrow [k(E) : k(y)] = \deg(E \xrightarrow{y} \mathbb{P}^1) = \operatorname{ord}_{O_E}(\frac{1}{y}) = 3.$

$\Rightarrow$



$[k(E) : k(x,y)] = 1$ (by tower law)

$\Rightarrow k(E) = k(x,y) = \phi^* k(E')$, so $\deg(\phi) = 1$.

$\Rightarrow$ Isomorphism (next time).

Elliptic Curves: Lecture 4 — 26/01/2024.

Theorem 3.1 Every elliptic E/K is isomorphic to an elliptic curve in Weierstrass form (over K), sending $O_E \to (0:1:0)$.

Proof Proved: can pick $x, y \in K(E)$ s.t. have elliptic curve E': $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

& have: morphism $\phi: E \to E'$, $\phi(O_E) = (0:1:0)$, and $\deg(\phi) = 1$ ($\Rightarrow \phi$ birational).

If ~~E singular~~ E' singular, then ~~E, E'~~ are rational #:

$\Rightarrow E'$ smooth. So, by Prop 2.9, ϕ^{-1} morphism $\Rightarrow \phi$ iso. ✓

Prop 3.2 E, E' elliptic curves over K in Weierstrass form. Then: $E \cong E'$ over K $\Leftrightarrow$ equations for E, E' are related by change of vars: $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$ where: $r, s, t, u \in K$ & $u \neq 0$.

Proof $\langle 1, x \rangle = L(2 \cdot O_E) = \langle 1, x' \rangle \Rightarrow x = \lambda x' + r$. ($\lambda \neq 0$)

& $\langle 1, x, y \rangle = L(3O_E) = \langle 1, x', y' \rangle$.

$\Rightarrow y = \mu \cdot y' + \sigma x' + t$. for $\lambda, \mu, \sigma, t \in K$, ($\mu \neq 0$)

By coefficients of x^3 & y^2, get: $\lambda^3 = \mu^2$, so $\exists u \in K^*$, with $\lambda = u^2$ & $\mu = u^3$.

Put $s = \frac{\sigma}{u^2}$, to get result ✓

A Weierstrass equation defines: elliptic curve, iff: defines smooth curve. □

$\Leftrightarrow \Delta(a_1, \ldots, a_6) \neq 0$. ($\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$ polynomial).

If $\mathrm{Char}(K) \neq 2,3$: may reduce to case $y^2 = x^3 + ax + b$.

$\Rightarrow \Delta = -16(4a^3 + 27b^2)$.

Corollary 3.3 Assume $\mathrm{Char}(K) \neq 2,3$. Then the elliptic curves

$E: y^2 = x^3 + ax + b$

$E': y^2 = x^3 + a'x + b'$

] isomorphic $\Leftrightarrow$ $a' = u^4 a$, $b' = u^6 b$, $(u \in K^\times)$.

Proof Prop 3.2 with $r = s = t = 0$.

DEF j-invariant $j(E) = \dfrac{1728(4a^3)}{4a^3 + 27b^2}$.

Corollary 3.4 $E \cong E' \Leftrightarrow j(E) = j(E')$. Converse holds if $K = \bar{K}$.

Proof Have $a' = u^4 a$ & $b' = u^6 b$, $u \in K^\times$.

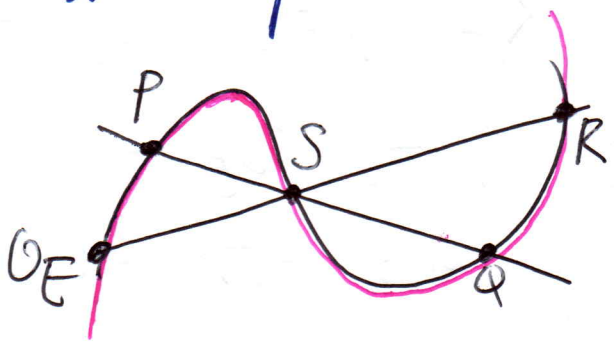
$\Leftrightarrow (a^3 : b^2) = ((a')^3 : (b')^2) \Leftrightarrow j(E) = j(E')$.

& Converse holds if $K = \bar{K}$ since reverse arrows.

§4: Group Law.

Let: $E \subseteq \mathbb{P}^2$ smooth plane curve.

& $O_E \in E(K)$.



For $P, Q \in E$: let S = 3rd pt, on E & line $\overline{PQ}$.

& R = 3rd pt, on $E \cap \overline{O_E S}$.

$\Rightarrow$ Define: $P \oplus Q = R$.

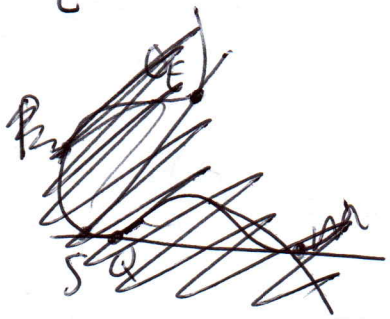
[If $P = Q$, then use Tangent $T_P E$ instead of $\overline{PQ}$, etc.]

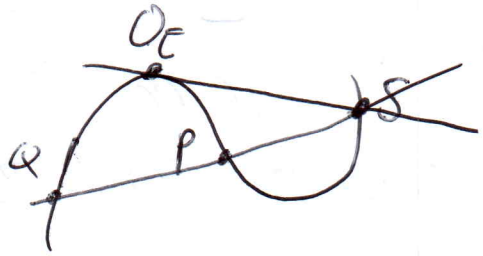
Called: Chord + Tangent process.

Theorem 4.1 $(E, \oplus)$ is an abelian group.

Proof Abelian: obvious. (Order of P, Q didn't matter for S)

Identity: O_E is the identity. 

Inverse: 



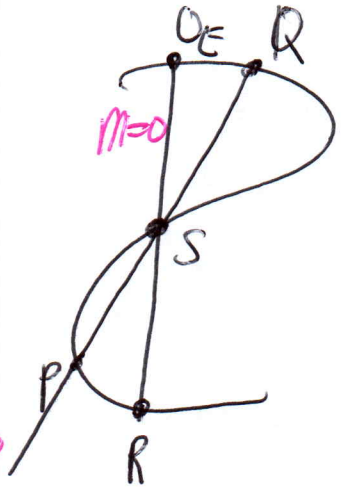
Denote: S = 3rd pt of $E \cap T_{O_E}E$
& Q = 3rd pt of $E \cap \overline{PS}$. $\Rightarrow P \oplus Q = O_E$.

Assoc: much harder! Need more theory.

DEF $D_1, D_2 \in \mathrm{Div}(E)$ linearly equiv $\Leftrightarrow \exists f \in \bar{K}(E)^*$, with: $\mathrm{div}(f) = D_1 - D_2$. (Write: $D_1 \sim D_2$).
& $[D] = \{D' \in \mathrm{Div}(E) : D \sim D'\}$.

Define: $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$ & $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$
(where: $\mathrm{Div}^0(E)$ = degree 0 divisors of E).

Define: $\Psi : E \longrightarrow \mathrm{Pic}^0(E)$
$P \longmapsto [(P) - (O_E)]$.



Prop 4.2 i) $\Psi(P \oplus Q) = \Psi(P) + \Psi(Q)$
ii) Ψ is bijection.

Proof Define lines ℓ, m as on diag.
$\Rightarrow$ i) $\mathrm{div}(\ell/m) = (P) + (S) + (Q) - [(O_E) + (S) + R]$
$\Rightarrow \mathrm{div}(\ell/m) = (P) + (Q) - (O_E) - (P \oplus Q)$.

So, $(P)+(Q) \sim (P \oplus Q) + (O_E)$. $\Rightarrow \psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) If $\psi(P) = \psi(Q)$ & $P, \neq Q$ on E. $\Rightarrow (P)-(O_E)$, $(Q)-(O_E)$ are linearly equiv, so: $\exists f \in \bar{K}(E)^*$: $div(f) = (P)-(Q)$.

$\Rightarrow E \xrightarrow{f} \mathbb{P}^1$ is a morphism.

& $deg(f) = 1$ (since has simple zero at P)

$\Rightarrow E \cong \mathbb{P}^1$ # (since genus $1 \neq 0$). Hence ψ injective.

ψ surj: $\forall D \in Pic^\circ(E)$. Look at: $D + (O_E)$. Degree 1 divisor.

$\Rightarrow$ By RR, $\dim_{\bar{K}} \mathcal{L}(D+(O_E)) = 1$, so find $f \in \mathcal{L}(D+O_E)$, $f \neq 0$, with $div(f) + D + (O_E)$ effective (≥ 0)

But: LHS has degree 1. So, $\exists P \in E$, $div(f) + D + (O_E) = (P)$.

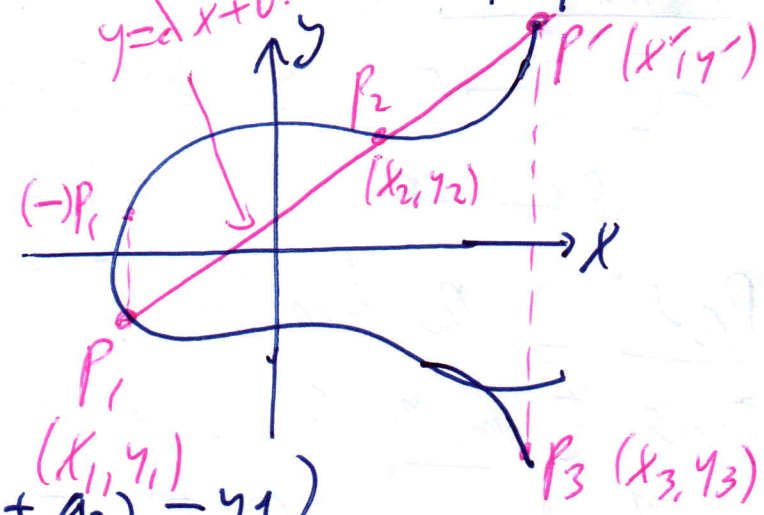
$\Rightarrow (P)-(O_E) \sim D$, so $\psi(P) = [D]$ ✓

Conclusion: ψ identifies $(E, \oplus)$ with $(Pic^\circ(E), +)$, which is assoc. Hence, $(E, \oplus)$ assoc ✓

Elliptic Curve: lecture 5.

29/01/2024.

Formulas on Elliptic Curve.



let: $E: y^2+a_1xy+a_3y$
$= x^3+a_2x^2+a_4x+a_6$.

Compute: $(-)P_1 = (x_1, -(a_1x_1+a_3)-y_1)$.

Substitute $y=\lambda x+v$ in E gives: $\lambda^2+a_1\lambda - a_2 = x_1+x_2+x'$

$\Rightarrow x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2$.

& $y_3 = -(a_1x'+a_3)-y'$

$= -(a_1x_3+a_3)-(\lambda x_3+v)$

$= -(\lambda+a_1)x_3 - a_3 - v$. $\Rightarrow$ Remains to find λ, v.

Case 1: $x_1 = x_2$ & $P_1 \neq P_2$. $\Rightarrow P_1 \oplus P_2 = O_E$.

Case 2: $x_1 \neq x_2$. $\Rightarrow \lambda = \dfrac{y_2-y_1}{x_2-x_1}$.

& $v = y_1 - \lambda x_1 = \dfrac{x_2y_1 - x_1y_2}{x_2-x_1}$.

Case 3: $P_1 = P_2$ $\Rightarrow$ Compute equation for tangent.

Corollary 4.3 $E(K)$ is Abelian group.

Proof Clearly, it is subgroup of $(E, \oplus)$.

- Identity: $O_E \in E(K)$ (by def)
- Closure/inversion: By formulas above
- Assoc/Commutative: Inherited ✓

Theorem 4.4 Elliptic curves are Group Varieties i.e.

$[-1]: E \to E$ & $\oplus : E \times E \to E$ are morphisms of

$P \mapsto -P$ $\quad (P,Q) \mapsto P \oplus Q$ algebraic varieties.

Proof i) By formulas, $[-1]: E \to E$ is birational. So, since E smooth, is a morphism (Remark 2.9)

ii) By formulas, $\oplus : E^2 \to E$ is a rational, regular map on $U = \{(P,Q) \in E^2 : P, Q, P \oplus Q, P \ominus Q \neq 0\}$.

For $P \in E$, let $\tau_P : E \to E$, $X \mapsto P \oplus X$. Is a rational map of smooth projective curves $\Rightarrow$ Morphism.

For $A, B \in E$: factor $\oplus$ as:

$$E \times E \xrightarrow{\tau_A \times \tau_B} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A \oplus B}} E.$$

$\Rightarrow \oplus$ Regular on $(\tau_A \times \tau_B) U$ $\forall A, B$. So, regular on E^2. ✓

Statement of Results.

i) If $K = \mathbb{C}$ & $\Lambda \subset \mathbb{C}$ lattice $\Rightarrow E(\mathbb{C}) = \mathbb{C}/\Lambda \cong (\mathbb{R}/\mathbb{Z})^2$

ii) $K = \mathbb{R}$: $E(\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \text{if } \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \text{if } \Delta < 0 \end{cases}$

iii) $K = \mathbb{F}_q \Rightarrow \left| \#E(\mathbb{F}_q) - (q+1) \right| \leq 2\sqrt{q}$

iv) $K =$ Finite ext of $\mathbb{Q}_p$. $\Rightarrow E(K)$ has a subgroup, finite idx, isomorphic to $(\mathcal{O}_K, +)$.

v) $K = \mathbb{Q}$ (or finite ext of $\mathbb{Q}$). $\Rightarrow E(K)$ f.g. Abelian group. (Mordell – Weil)

Basic Group Theory. If A f.g. Abelian group, then:
$A \cong (\text{finite group}) \times \mathbb{Z}^r$, $r \geq 0$. (Structure Theorem)
The proof of Mordell-Weil gives an upper bound for rank of $E(K)$. But: $\nexists$ any general algorithm to compute rank exactly.

Brief remarks ($K=\mathbb{C}$). Have: $\Lambda = \{a\omega_1 + b\omega_2 : a,b \in \mathbb{Z}\}$
where $\{\omega_1, \omega_2\}$ is $\mathbb{C}$-basis as $\mathbb{R}$-VS.

$$\Rightarrow \left\{\begin{matrix}\text{Meromorphic fns} \\ \text{on RS } \mathbb{C}/\Lambda\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\Lambda\text{-invariant mero} \\ \text{funcs on } \mathbb{C}\end{matrix}\right\}$$

The Function field of $\mathbb{C}/\Lambda$ is: generated by $p(z)$ & $p'(z)$,

where $p(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda^*} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$.

$$p'(z) = -2\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

$$(p'(z))^2 = 4p(z)^3 - g_2 p(z) - g_3.$$

One can show: $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, $E = \{y^2 = 4x^3 - g_2 x - g_3\}$.
(Isomorphism of RS ↑ & as groups)

Uniformisation Theorem Any elliptic E over $\mathbb{C}$ arises in this way.

DEF $\forall n \in \mathbb{Z}$: $[n] : E \to E$, $P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n}$.
& $[-n] = [-1] \circ [n]$.

DEF n-torsion subgroup of E: $E[n] = \ker(E \xrightarrow{[n]} E)$.
If $K = \mathbb{C}$, then: $E(\mathbb{C}) = \mathbb{C}/\Lambda$.

$\Rightarrow$ $\begin{cases} E[n] = (\mathbb{Z}/n\mathbb{Z})^2 & (1) \\ \deg[n] = n^2 & (2) \end{cases}$

Will show: (2) holds for any field k

& (1) holds if $\mathrm{char}(k) \nmid n$.

Elliptic curves: lecture 6 31/01/2023.

Lemma 4.5 $\mathrm{Char}(K) \neq 2$. Then: if $E: y^2 = (x-e_1)(x-e_2)(x-e_3)$ for $e_i \in \bar{K}$, then $E[2] = \{O, (e_i, 0) \mid 1 \leq i \leq 3\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof For $P = (x,y) \in E$, $[2]P = 0 \iff P = -P \iff (x,y) = (x,-y)$. So, must have $y = 0$ ✓ Note all nonzero elements have order 2, so group $\cong (\mathbb{Z}/2\mathbb{Z})^2$. ✓

§5: Isogenies.

Let: E_1, E_2 elliptic curves.

DEF i) Isogeny $\phi: E_1 \to E_2$ is: nonconst morphism with $\phi(O_{E_1}) = O_{E_2}$. (Nonzero $\iff$ Surjective on $\bar{K}$-points, thm 2.8)

ii) Say ~~isogenies~~ E_1, E_2 isogenous.

DEF $\mathrm{Hom}(E_1, E_2) = \{\text{Isogenies } \phi: E_1 \to E_2\} \cup \{0\}$.

This is: Abelian group under: $(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$.

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ isogenies: $\Rightarrow \psi \circ \phi$ is isogeny.

$\Rightarrow$ By Tower Law: $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$.

Prop 5.1 If $n \in \mathbb{Z}_{\neq 0}$ then $[n]: E \to E$ isogeny.

Proof By Theorem 4.4: (n) is morphism, and clearly $(n)O_E = O_E$. So, need to show: $[n] \neq [0]$. Assume: Char $K \neq 2$.

Case $n=2$: $E[2] \neq E \Rightarrow [2] \neq (0)$

Case n odd $\exists\, T \in E[2],\ T \neq 0 \Rightarrow nT = T \neq 0 \Rightarrow [n] \neq [0]$

Now, use $[mn] = [m] \circ [n] \Rightarrow [n] \neq 0\ \forall n \neq 0$ ✓

If $\mathrm{Char}(K) = 2$, then: Can replace Lemma 4.5 with an explicit lemma about 3-torsion points.

Corollary 5.2 $\mathrm{Hom}(E_1, E_2)$ is: Torsion-free $\mathbb{Z}$-module.

Theorem 5.3 Let $\phi: E_1 \to E_2$ isogeny. Then,

$\phi(P+Q) = \phi(P) + \phi(Q)\ \ (\forall P, Q \in E_1)$

Sketch Proof ϕ induces: $\phi_*: \mathrm{Div}^0(E_1) \longrightarrow \mathrm{Div}^0(E_2)$

$P \longmapsto \phi(P)$

& $\phi^*: K(E_2) \hookrightarrow K(E_1)$.

$\Rightarrow \exists$ Norm map $N_{K(E_1)/K(E_2)}$ (since $K(E_2) \subseteq K(E_1)$ Field exts)

Fact: $\forall f \in K(E_1)$, $\mathrm{div}(N_{K(E_1)/K(E_2)}(f)) = \phi_*(\mathrm{div}\, f)$.

$\Rightarrow$ ϕ_* Sends: Principal divisors $\longrightarrow$ Principal divisors.

Since $\phi(O_{E_1}) = O_{E_2}$: diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \wr\downarrow & & \wr\downarrow \\ \mathrm{Pic}^0(E_1) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E_2) \end{array}$$

(sending: $P \longmapsto [(P) - (O_{E_1})]$ etc)

& ϕ_* is group hom.

$\Rightarrow \phi$ group hom ✓

Lemma 5.4 $\phi: E_1 \to E_2$ isogeny. Then: $\exists$ morphism $\overline{\xi}$ with:

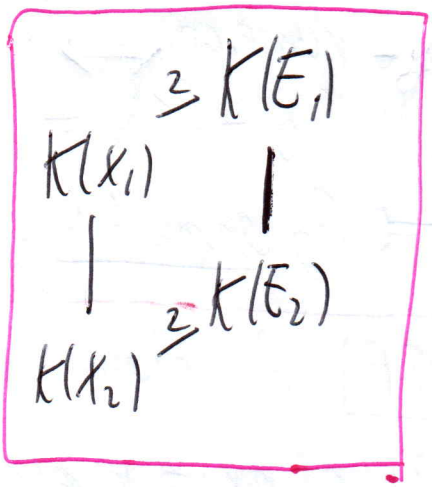
$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ {\scriptstyle x_1}\downarrow & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xrightarrow{\overline{\xi}} & \mathbb{P}^1 \end{array}$$

commuting. (x_i = x-coordinate on a Weierstrass eqn for E_i.) $\square$

Moreover: if $\xi(t) = \frac{r(t)}{s(t)}$ for $r(t), s(t)$ coprime, then:

$\deg(\phi) = \deg(\xi) = \max(\deg(r), \deg(s))$.

Proof] For $i=1,2$: $K(E_i)/K(X_i)$ is degree 2 ext. & is Galois, with Galois group $\langle [-1]^* \rangle$



By Theorem 6.3: $\phi \circ [-1] = [-1] \circ \phi$.

$\Rightarrow$ If ~~$f \in K(X_2)$~~ $f \in K(X_2)$, then: ~~$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$~~

$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$

$\Rightarrow \phi^* f \in K(X_1)$.

In particular: $\exists\, \xi \in K(t)$, with: $\phi^* X_2 = \xi(X_1)$.

$\Rightarrow$ By Tower Law: $\deg \phi = \deg \xi$.

For degree: $K(X_2) \hookrightarrow K(X_1)$.

$X_2 \longmapsto \xi(X_2) = \frac{r}{s}(X_2)$ $\quad r, s \in k[t]$ coprime.

$\Rightarrow$ Min poly of X_1 over $K(X_2)$ is: $F(t) = r(t) - s(t) X_2$.

[$F(X_1) = 0$: ✓ & F irred in $K[X_2, t]$ since F linear in X_2, so by Gauss: F irred in $K(X_2)[t]$.

$\Rightarrow F$ min poly of X_1 over $K(X_2)$]

$\Rightarrow \deg \phi = \deg(\xi) = [K(X_2) : K(X_1)] = \deg F = \max(\deg r, \deg s)$. ∎

Lemma 5.5 Deg $[2] = 4$.

Proof] Assume: $\mathrm{Char}(K) \neq 2, 3$.

$\Rightarrow E \stackrel{\text{a}}{=} y^2 = x^3 + ax + b = f(x)$, say.

For $P=(x,y)$: $x(2P) = \left(\frac{3x^2+a}{2y}\right)^2 - 2x$.

$= \frac{(3x^2+a)^2 - 8xf(x)}{4f(x)^2} = \frac{x^4+\dots}{4f(x)^2}$.

The numerator & denominator are coprime since if $\exists \theta \in \bar{K}$ with $f(\theta)=f'(\theta)=0$ then f has multiple root ↯

$\Rightarrow$ By lemma 9.4: $\deg[2] = 4$ ✓

DEF A abelian group. Then $q: A \to \mathbb{Z}$ is Quadratic Form if:

(i) $q(nx) = n^2 q(x)$ $\forall x \in A$, $n \in \mathbb{Z}$

(ii) $(x,y) \mapsto q(x+y) - q(x) - q(y)$ is $\mathbb{Z}$-Bilinear.

Lemma 5.6 $q: A \to \mathbb{Z}$ QF $\Leftrightarrow$ Parallelogram Law

(i.e. $q(x+y) + q(x-y) = 2(q(x)+q(y))$).

Proof $\Rightarrow$: If $\langle \cdot, \cdot \rangle = q(x+y) - q(x) - q(y)$, then:

$\langle x, x \rangle = q(2x) - 2q(x) = 2q(x)$.

& By (ii), $\langle x+y, x+y \rangle + \langle x-y, x-y \rangle = 2(\langle x, x \rangle + \langle y, y \rangle)$.

$\Leftarrow$: Example sheet 2

Elliptic Curve: lecture 7. 02/02/2024.

Theorem 5.7 $\deg: \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ quadratic form.

Proof Assume $\mathrm{Char}(K) \neq 2, 3$ (Theorem is true in general, tho)

$\Rightarrow$ WLOG: $E_2: \{y^2 = x^3 + ax + b\}$

& $P, Q \in E_2, [P, Q, P+Q, P-Q \neq 0.]$ & $x_1, \dots x_4$ x-coords of these.

Lemma 5.8 $\exists\, W_0, W_1, W_2 \in \mathbb{Z}[a,b][x_1, x_2]$

with: degree ≤ 2 in x_1, ≤ 2 in x_2 & have:

$(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2)$.

Proof Direct Calculation / Formula Sheet.

OR: write $y = \lambda x + v$ be line through P, Q.

$\Rightarrow x^3 + ax + b - (\lambda x + v)^2 = (x - x_1)(x - x_2)(x - x_3)$.

$= x^3 - S_1 x^2 + S_2 x - S_3$.

Compare coeffs $\Rightarrow \lambda^2 = S_1$, $-2\lambda v = S_2$, $v^2 = S_3 + b$.

Eliminate λ, v $\Rightarrow \underbrace{(S_2 - a)^2 - 4S_1(S_3 + b)}_{= F(x_1, x_2, x_3)} = 0$

Notice: F has degree ≤ 2 in each x_i, and x_3 root of $F(x_1, x_2, t)$.

Repeat for line through $P, -Q$. $= W(t)$

$\Rightarrow$ Let x_4 as the other root.

$\Rightarrow W_0(t - x_3)(t - x_4) = W(t) = W_0 t^2 - W_1 t + W_2$

$\Rightarrow (1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2)$ ✓

Back to Proof of Theorem 5.7

Will show: if $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ then:

$$\deg(\phi+\psi) + \deg(\phi-\psi) \leq 2[\deg\phi + \deg\psi]$$

May assume $\phi, \psi, \phi+\psi, \phi-\psi \neq 0$ (else trivial)
($\deg(-1)=1$, $\deg[2]=4$)

Say: $\phi : (x,y) \longmapsto (g_1(x), \dots)$

$\psi : (x,y) \longmapsto (g_2(x), \dots)$

$\phi+\psi : (x,y) \longmapsto (g_3(x), \dots)$

$\phi-\psi : (x,y) \longmapsto (g_4(x), \dots)$

By Lemma 5.8: $(1 : g_3+g_4 : g_3 g_4) = ((g_1-g_2)^2 : \dots)$

$\Rightarrow$ If $g_i = r_i/s_i$ for $r_i, s_i \in K(t)$ coprime, then:

$$(s_3 s_4 : s_3 r_4 + s_4 r_3 : r_3 r_4) = ((r_1 s_2 - r_2 s_1)^2 : \dots)$$

($s_3 s_4$, $r_3 r_4$: coprime)

$\Rightarrow \deg(\phi+\psi) + \deg(\phi-\psi)$

$= \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4))$

$= \max(\deg(r_3 r_4), \deg(r_3 s_4 + r_4 s_3), \deg(s_3 s_4))$

$\leq 2\max(\deg(r_1), \deg(s_1)) + 2\max(\deg(r_2), \deg(s_2))$

$= 2\deg\phi + 2\deg\psi.$

But: making $(\phi, \psi) \longmapsto (\phi+\psi, \phi-\psi)$ gives reverse ineq. (using $\deg[2]=4$) $\square$

$\Rightarrow$ deg satisfies Parallelogram law, hence QF ✓

Corollary 5.9 $\deg(n\phi) = n^2 \deg(\phi)$ $\forall n$ & $\phi \in \mathrm{Hom}(E_1, E_2)$.

In particular, $\deg[n] = n^2$.

Example 5.10 Let: E/K elliptic curve. ($\mathrm{Char}(K) \neq 2$)

& $0 \neq T \in E(K)[2]$. ($\Rightarrow$ WLOG: $E = \{y^2 = x(x^2 + ax + b)\}$)

have: $b \neq 0$ & $a^2 - 4b \neq 0$ (Smoothness), $T = (0,0)$.

$\Rightarrow$ For $P = (x,y)$ & $P' = P + T = (x', y')$:

$x' = \left(\frac{y}{x}\right)^2 - a - x = b/x$

& $y' = -\left(\frac{y}{x}\right) x' = -by/x^2$.

Denote: $\xi = x + x' + a = \left(\frac{y}{x}\right)^2$ & $\eta = y + y' = \frac{y}{x}\left(x - \frac{b}{x}\right)$

$\Rightarrow \eta^2 = \left(\frac{y}{x}\right)^2 \left(\left(x + \frac{b}{x}\right)^2 - 4b\right) = \xi\left((\xi - a)^2 - 4b\right)$

$= \xi\left(\xi^2 - 2a\xi + (a^2 - 4b)\right)$.

Denote: $E' = \{y^2 = x(x^2 + a'x + b')\}$, $a' = -2a$, $b' = a^2 - 4b$.

$\Rightarrow \exists$ isogeny $\phi : E \to E'$

$(x,y) \longmapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1\right)$

$O_E \longmapsto (0:1:0)$ (compare ord_∞)

& To compute $\deg(\phi)$: note $\left(\frac{y}{x}\right)^2 = \frac{x^2 + ax + b}{x}$

$\Rightarrow$ By Lemma 5.4, get $\deg(\phi) = 2$. Say: ϕ 2-isogeny. $\square$

§6 : Invariant Differentials

Let C curve over $k = \bar{k}$.

DEF Space of differentials Ω_C is: k-VS generated by df, $f \in k(C)$, subject to conditions:

1) $d(f+g) = df + dg$
2) $d(fg) = f \cdot dg + g \cdot df$
3) $da = 0 \quad \forall a \in k$.

Fact: Ω_C is a 1-dim $k(C)$-VS. (AG)

Elliptic Curves: Lecture 8 | 05/02/2024

Let: $0 \neq \omega \in \Omega_C$, $P \in C$ smooth pt, $t \in K(C)$ unif. Then, $\omega = f\,dt$ for some $f \in K(C)^*$. Define: $ord_P(\omega) \equiv ord_P(f)$.

Turns out: this is indep. of choice of t (well-defined).

Fact: If $f \in K(C)^*$ & $Ord_P(f) = n > 0$ and $Char(K) \nmid n$, then: $ord_P(df) = n-1$.

Assume: C is smooth projective curve.

DEF] $div(\omega) = \sum_{P \in C} ord_P(\omega) P \in Div(C)$.

[Using fact: $ord_P(\omega) = 0$ for all but finitely many P.]

DEF] $g(C) = \dim_K \{\omega \in \Omega_C : div(\omega) \geq 0\}$ = Regular diffs.

As consequence of RR: if $0 \neq \omega \in \Omega_C$, then: $deg(div\,\omega) = 2g(C) - 2$.

Lemma 6.1] Assume $Char(K) \neq 2$.

$E: \{y^2 = (x-e_1)(x-e_2)(x-e_3)\}$ for e_i distinct.

Then: $\omega = \frac{dx}{y}$ is a differential on E, and no zeros/poles.

(Hence: $g(C) = 1$.) In particular, the 1-dim VS of regular diffs on E is spanned by ω.

Proof] Denote: $T_i = (e_i, 0) \Rightarrow E[2] = \{0, T_1, T_2, T_3\}$.

For $0 \neq P \in E$: $div(X - X_P) = (P) + (-P) - 2(0)$.

If $P \in E \setminus E[2]$, then: $ord_P(x - x_P) = 1$ ~~$\Rightarrow div(dx) = 0$~~ [1]

If $P \in E \setminus E[2] \Rightarrow \operatorname{ord}_P(x - x_P) = 1 \Rightarrow \operatorname{ord}_P(dx) = \neq 0$

If $P \in \{T_i\} \Rightarrow \operatorname{ord}_P(x - x_P) = 2 \Rightarrow \operatorname{ord}_P(dx) = 1$

If $P = 0 \Rightarrow \operatorname{ord}_P(x - x_P) = -2 \Rightarrow \operatorname{ord}_P(dx) = -3$.

$\Rightarrow \operatorname{div}(dx) = (T_1) + (T_2) + (T_3) - 3(0)$.

$\Rightarrow \operatorname{div}(\omega) = \operatorname{div}\left(\frac{dx}{y}\right) = 0$ ✓

DEF For $\phi : C_1 \to C_2$ nonconst morphism, define:

$\phi^* : \mathcal{L}_{C_2} \to \mathcal{L}_{C_1}$ by

$f\,dg \longmapsto \phi^* f\, d(\phi^* g)$.

Lemma 6.2 For $P \in E$, define $\tau_P : E \to E$, $X \mapsto X + P$.

& $\omega = \frac{dx}{y}$. Then, $\tau_P^* \omega = \omega \ \forall P$. [$\omega$ = invariant diff.]

Proof Know: $\tau_P^* \omega$ is a Regular differential on E.

$\Rightarrow \exists \lambda_P \in K^*$ with $\tau_P^* \omega = \lambda_P \omega$.

Then: the map $E \to \mathbb{P}^1$, $P \mapsto \lambda_P$ is a morphism of smooth projective curves, not Surjective (misses $0, \infty$).

$\Rightarrow$ Map is constant (Theorem 2.8).

$\exists \lambda \in K^*$, $\tau_P^* \omega = \lambda \omega \ \forall P \in E$. Choose $P = 0 \Rightarrow \lambda = 1$ ✓

Remark If $K = \mathbb{C}$, then since $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, $z \mapsto (\wp(z), \wp'(z))$

the differential $\frac{dx}{y} = \frac{\wp'(z)\,dz}{\wp'(z)} = dz$.

⇒ Matches with obvious choice of differential.

Lemma 6.3 Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ and: ω the invariant differential on E_2. Then: $(\phi+\psi)^*\omega = \phi^*\omega + \psi^*\omega$.

Proof Denote $E = E_2$, and write: $E \times E \longrightarrow E$

$\mu: (P,Q) \longmapsto P+Q$

$pr_1: (P,Q) \longmapsto P$

$pr_2: (P,Q) \longmapsto Q$.

Fact: $\Omega_{E\times E}$ is 2D $K(E\times E)$-vector space, with the basis: $\{pr_1^*\omega, pr_2^*\omega\}$.

$\Rightarrow \exists f,g \in K(E\times E)$ with $\mu^*\omega = f\, pr_1^*\omega + g\, pr_2^*\omega$ (1)

Now, define $i_Q : E \longrightarrow E\times E$, $P \longmapsto (P,Q)$ for fixed $Q \in E$.

Apply i_Q to (1), gives: $(\mu i_Q)^*\omega = (i_Q^* f)(pr_1 i_Q)^*\omega + (i_Q^* g)(pr_2 i_Q)^*\omega$

($\mu i_Q = \tau_Q$; $i_Q^* f$: identity; $pr_2 i_Q$: constant.)

$\Rightarrow \tau_Q^*\omega = (i_Q^* f)\omega$, so: $i_Q^* f = 1 \ \forall Q \in E$

$\Rightarrow f(P,Q) = 1 \ \forall P,Q \in E$, so $f = 1$.

Similarly, $g = 1$, so indeed $\mu^*\omega = pr_1^*\omega + pr_2^*\omega$ ✓

& Pull back via $E \longrightarrow E\times E$, $P \longmapsto (\phi(P), \psi(P))$ to get result ✓

Lemma 6.4 $\phi: C_1 \longrightarrow C_2$ nonconst morphism. Then:

ϕ separable $\Longleftrightarrow$ $\phi^*: \Omega_{C_2} \longrightarrow \Omega_{C_1}$ nonzero.

Example $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ (multiplicative group)

$n \geq 2$ & $\phi : \mathbb{G}_m \longrightarrow \mathbb{G}_m, \; x \longmapsto x^n$.

$\Rightarrow \phi^*(dx) = d(\phi(x)) = d(x^n) = n x^{n-1} dx$.

$\Rightarrow$ If $\mathrm{Char}(k) \nmid n$, then: ϕ separable, so: $\# \phi^{-1}(\rho) = \deg(\phi)$ for all but finitely many $Q \in \mathbb{G}_m$.

But, ϕ group hom $\Rightarrow \# \phi^{-1}(\rho) = |\ker(\phi)| \; \forall Q \in \mathbb{G}_m$.

$\Rightarrow \deg(\phi) = \# \ker(\phi) = n$.

$\Rightarrow k \; (= \bar{k})$ contains n distinct roots of unity.

Elliptic Curves: lecture 9 | 07/02/2024

Theorem 6.5 If $\mathrm{char}(K) \nmid n$, then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Proof By lemma 6.3 & Induction: $[n]^*\omega = n\omega \neq 0$.

$\Rightarrow [n]$ separable, so $\#[n]^{-1}(Q) = \deg[n]$ for all but finitely many $Q \in E$.

But: $[n]$ Group hom, so $\#[n]^{-1}(Q) = \deg[n]$ $\forall Q \in E$.

$\Rightarrow \#E[n] = \deg[n] = n^2$ (by Corollary 5.9)

By structure theorem: $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$, $(d_1 | \cdots | d_t)$

Killed by $n \Rightarrow d_1 | \cdots | d_t | n$.

If p prime, $p | d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$ has size p^2, so $t = 2$

Now, $d_1 | d_2 | n$ & $d_1 d_2 = n^2 \Rightarrow d_1 = d_2 = n$ ✓ $E(n) \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Remark If $\mathrm{Char}(K) = p$, then $[p]$ inseparable. ($[p]^*\omega = 0$)

Can show: either $E[p^r] \cong (\mathbb{Z}/p^r\mathbb{Z})$ $\forall r \geq 1$ [Ordinary]

or $E[p^r] = 0$. [Supersingular]

Note: Trivialises a Q on example sheet 2.

---

§7: Elliptic curves over Finite Fields.

Lemma 7.1 A Abelian ($\mathbb{Z}$-module). & $q : A \to \mathbb{Z}$ positive-def. QF. Then: $|q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}$

Proof May assume $x \neq 0$. $\langle x, y \rangle$

$\Rightarrow q(x) \neq 0$.

Take: $m, n \in \mathbb{Z}$ & know that $q(mx + ny) \geq 0$.

$$0 \leq q(mx+ny) = \tfrac{1}{2}\langle mx+ny,\ mx+ny\rangle$$

$$= m^2 q(x) + mn\langle x,y\rangle + n^2 q(y).$$

$$= q(x)\left(m + \frac{\langle x,y\rangle}{2q(x)}n\right)^2 + \left(q(y) - \frac{\langle x,y\rangle^2}{4q(x)}\right)n^2.$$

Take: $m = -\langle x,y\rangle$ & $n = 2q(x)$ (Both integers)

$\Rightarrow$ Get $\langle x,y\rangle^2 \leq 4q(x)q(y)$ ✓

Theorem 9.2 (Hasse). Let E elliptic $/\mathbb{F}_q$. Then:

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Proof: Recall: $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ Cyclic, order r & generated by $\mathbb{F}_r$ $x \mapsto x^q$.

Let: E Weierstrass eqn for E, coeffs $a_1, \dots, a_6 \in \mathbb{F}_q$

$\Rightarrow a_i^q = a_i$ $\forall i$. So, $\phi : E \longrightarrow E$ ("Frobenius endo")

$$(x,y) \longmapsto (x^q, y^q)$$

is isogeny, degree q.

Know: $E[\mathbb{F}_q] = \{P \in E : \phi(P) = P\} = \ker(1-\phi)$

Claim: $1-\phi$ separable.

Why: $\phi^*\omega = \phi^*\left(\frac{dx}{y}\right) = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}}{y^q} = 0$. $(p|q)$

By Lemma 6.3 $\Rightarrow (1-\phi)^*\omega = \omega - \underbrace{\phi^*\omega}_{=0} = \omega \neq 0$.

$\Rightarrow 1-\phi$ separable.

By Theorem 2.8 & fact that $1-\phi$ group hom:

$\square$

Argue as before, that $\#\ker(1-\phi) = \deg(1-\phi)$

By Theorem 5.7: $\deg : \mathrm{Hom}(E,E) \longrightarrow \mathbb{Z}$ pos def QF

By Lemma 7.1: $|\deg(1-\phi) - 1 - \deg(\phi)| \leq 2\sqrt{\deg \phi}$

$\Rightarrow |\#E[\mathbb{F}_q] - (q+1)| \leq 2\sqrt{q}$. ✓

DEF For $\phi, \psi \in \mathrm{End}(E)$: $(= \mathrm{Hom}(E,E))$

put: $\langle \phi, \psi \rangle = \deg(\phi+\psi) - \deg(\phi) - \deg(\psi)$.

& $\mathrm{Tr}(\phi) = \langle \phi, 1 \rangle$.

Corollary 7.3 $E/\mathbb{F}_q$ Elliptic curve, & ϕ Frobenius Ends.

Then, $\#E(\mathbb{F}_q) = q+1-\mathrm{tr}(\phi)$. & $|\mathrm{tr}(\phi)| \leq 2\sqrt{q}$.

ZETA FUNCTIONS.

For K NF: $\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} (N(I))^{-s} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime}}} (1 - N(\mathfrak{p})^{-s})^{-1}$.

For K Function field: (i.e. $K = \mathbb{F}_q(C)$) where $C/\mathbb{F}_q$ is a smooth projective curve: $\zeta_K(s) = \prod_{x \in |C|} (1 - N(x)^{-s})^{-1}$

where $|C|$ = Closed points of C

= Orbit of Absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on $E(\overline{\mathbb{F}}_q)$.

& $N_x = q^{\deg(x)}$ where $\deg(x)$ = Size of this orbit.

$\Rightarrow \zeta_K(s) = F(q^{-s})$ for some $F \in \mathbb{Q}[\![T]\!]$.

$F(T) = \prod_{x \in |C|} (1 - T^{\deg(x)})^{-1}$

$$\log F(T) = \sum_{x \in |C|} \sum_{m \geq 1} \frac{1}{m} T^{m \deg(x)}$$

$$\Rightarrow T \cdot \frac{d}{dT} \log F(T) = \sum_{x \in |C|} \sum_{m \geq 1} \deg(x) \cdot T^{m \deg(x)}$$

$$= \sum_{n \geq 1} \left(\sum_{\substack{x \in |C| \\ \deg(x) \mid n}} \deg(x) \right) T^n$$

$$= \sum_{n \geq 1} \# C(\mathbb{F}_{q^n})\, T^n.$$

$$\Rightarrow F(T) = \exp\left(\sum_{n \geq 1} \frac{\# C(\mathbb{F}_{q^n})}{n} T^n \right).$$

DEF The Zeta function on smooth proj curve $C/\mathbb{F}_q$:

$$Z_C(T) = \exp\left(\sum_{n \geq 1} \frac{\# C(\mathbb{F}_{q^n})}{n} T^n \right)$$

Next lecture: compute for C = elliptic curve!

Elliptic Curves: lecture 10 | 09/02/2024

DEF Zeta Func of $C/\mathbb{F}_q$ smooth proj curve is:

$$Z_C(T) = \exp\left(\sum_{n\geq 1} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n\right).$$

Theorem 7.4 $E/\mathbb{F}_q$ elliptic & $\#E(\mathbb{F}_q) = q+1-a$. Then:

$$Z_E(T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

Proof Let $\phi: E \longrightarrow E$ q-power Frobenius map.

By Corollary 7.3: $\#E(\mathbb{F}_q) = q+1-tr(\phi) \Rightarrow a = tr(\phi)$

By: Example sheet 2, Q6: $\phi^2 - a\phi + q = 0$.

$\Rightarrow \phi^{n+2} - a\phi^{n+1} + q\cdot\phi^n = 0$, so: apply Trace to this.

$Tr(\phi^{n+2}) - a\,Tr(\phi^{n+1}) + q\cdot Tr(\phi^n) = 0$.

This 2nd order Difference equation has: $tr(1) = 2$, ~~$tr(a) = q$~~. $tr(\phi) = a$.

$\Rightarrow$ Has solution $tr(\phi^n) = \alpha^n + \beta^n$: $\alpha, \beta \in \mathbb{C}$

where α, β are roots of $X^2 - aX + q = 0$.

By Corollary 7.3: $\#E(\mathbb{F}_{q^n}) = q^n + 1 - tr(\phi^n) = 1 + q^n - \alpha^n - \beta^n$

$$\Rightarrow Z_E(T) = \exp\left(\sum_{n\geq 1}\left(\frac{T^n}{n!} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n}\right)\right)$$

$$= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \checkmark = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

Remark Hasse's Theorem $\Rightarrow |a| \leq 2\sqrt{q}$, so $\alpha = \bar{\beta}$.

Let: $K = \mathbb{F}_q(E)$. $\Rightarrow |\alpha| = |\beta| = \sqrt{q}$.

Then, $\zeta_K(s) = 0 \Rightarrow Z_E(q^{-s}) = 0$, so $q^s = \alpha$ or β.

$\Rightarrow q^{\mathrm{Re}(s)} = |\alpha|$ or $|\beta| = \sqrt{q}$. Hence, $\underline{\mathrm{Re}(s) = \frac{1}{2}}$.

---

§8: Formal Groups.

DEF R ring, $I \subseteq R$ ideal. I-adic topology on R:
has basis $\{r + I^n : r \in R, n \geq 1\}$.

DEF (x_n) in R Cauchy $\Leftrightarrow \forall k, \exists N, x_m - x_n \in I_k \ \forall m, n \geq N$.

& R complete $\Leftrightarrow$ i) $\bigcap_{n \geq 0} I^n = \{0\}$; ii) All Cauchy seqs converge.

Remark $x \in I \Rightarrow \frac{1}{1-x} = 1 + x + x^2 + \cdots$. $\Rightarrow \underline{1 - x \in R^\times}$.

Examples $R = \mathbb{Z}_p$, $I = p\mathbb{Z}_p$

or $R = \mathbb{Z}[[t]]$, $I = (t)$.

Lemma 8.1 (Hensel's Lemma)

R I-adically complete & $F \in R[X]$, & $s \geq 1$.

Suppose: $\exists a \in R$, $F(a) \equiv 0 \bmod I^s$ & $F'(a) \in R^\times$.

Then: $\exists!\ b \in R$, with $F(b) = 0$ & $b \equiv a \pmod{I^s}$.

Proof Let $u \in R^\times$ & $F'(a) \equiv u \bmod I$. (e.g. $u = F'(a)$).

Replace: $F(X)$ with $\frac{F(X+a)}{u} - a$ $\Rightarrow$ Assume: $a=0$, $F'(0) \equiv 1 \pmod{I}$.

Put $X_0 = 0$ & $X_{n+1} = X_n - F(X_n)$. (1)

By induction: $X_n \equiv 0 \pmod{I^s}$ $\forall n$. (2)

& $F(X) - F(Y) = (X-Y)(F'(0) + XG(X,Y) + YH(X,Y))$ (3)

for some $G, H \in R[X,Y]$.

Claim] $X_{n+1} \equiv X_n \bmod I^{n+s}$ $\forall n \geq 0$.

Proof] Induction on n. For $n=0$, ✓

& If true for $n-1$: $X_n \equiv X_{n-1} \bmod I^{n+s-1}$

By (3): $F(X_n) - F(X_{n-1}) = (X_n - X_{n-1})(1+c)$, $c \in I$.

$\equiv X_n - X_{n-1} \bmod I^{n+s}$ ✓

$\Rightarrow F(X_n) - X_n \equiv F(X_{n-1}) - X_{n-1} \bmod I^{n+s}$

$\Rightarrow X_{n+1} \equiv X_n \bmod I^{n+s}$.

Hence, indeed, (X_n) Cauchy, and since R complete, get:

$\exists b \in R$, $X_n \longrightarrow b$.

Taking $n \to \infty$ in (1) gives: $b = b - F(b)$, so $F(b) = 0$

Taking $n \to \infty$ in (2) gives: $b \equiv 0 \bmod I^s$

$\equiv a \bmod I^s$ ✓

Uniqueness] Use (3) + Remark ✓

Let: $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$

the equation for E.

Take: Affine piece $Y \neq 0$, & let $t = -X/Y$, $w = -Z/Y$.

$\Rightarrow w = t^3 + a_1 tw + a_2 t^2 w + a_3 w^2 + a_4 tw^2 + a_6 w^3 \equiv f(t,w)$.

Apply Lemma 8.1 with: $R = \mathbb{Z}[a_1, \dots, a_6][\![t]\!]$, $I = (t)$,

$F(X) = X - f(t,X) \in R[X]$, $s = 3$, $a = 0$:

Check: $F(0) = -f(t,0) \equiv -t^3 \equiv 0 \pmod{I^3}$

$F'(0) = 1 - a_1 t - a_2 t^2 \in R^\times$.

$\Rightarrow \exists!\ w(t) \in R$, with: $w(t) = f(t, w(t))$ & $w(t) \equiv 0 \pmod{t^3}$.

Remarks 1) Taking $a = 1$ in Proof of Lemma 8.1:

$w(t) = \lim_{n \to \infty} w_n(t)$ where: $w_0(t) = 0$ & $w_{n+1}(t) \equiv f(t, w_n(t))$

2) In fact: $w(t) = t^3(1 + A_1 t + A_2 t^2 + \dots)$ where:

$A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1 a_2 + 2a_3$, etc.

Elliptic Curves: lecture 11 | 12/02/2024

From last time: E: $w = t^3 + a_1 tw + \cdots + a_6 w^3 \equiv f(t,w)$.

By Hensel: $\exists! w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$, $w(t) = f(t, w(t))$, & $w(t) \equiv 0 \bmod t^3$.

Lemma 8.2 R integral dom, I-complete. & $a_1, \ldots, a_6 \in R$ and $K = \mathrm{Frac}(R)$. Then: $\hat{E}(I) = \{(t,w) \in E(K) : t, w \in I\}$ is a subgroup of $E(K)$.

Note By uniqueness in Hensel, $\hat{E}(I) = \{(t, w(t)) \in E(K) : t \in I\}$.

Proof of Lemma For $(t,w) \neq (0,0)$, get $O_E \in \hat{E}(I)$

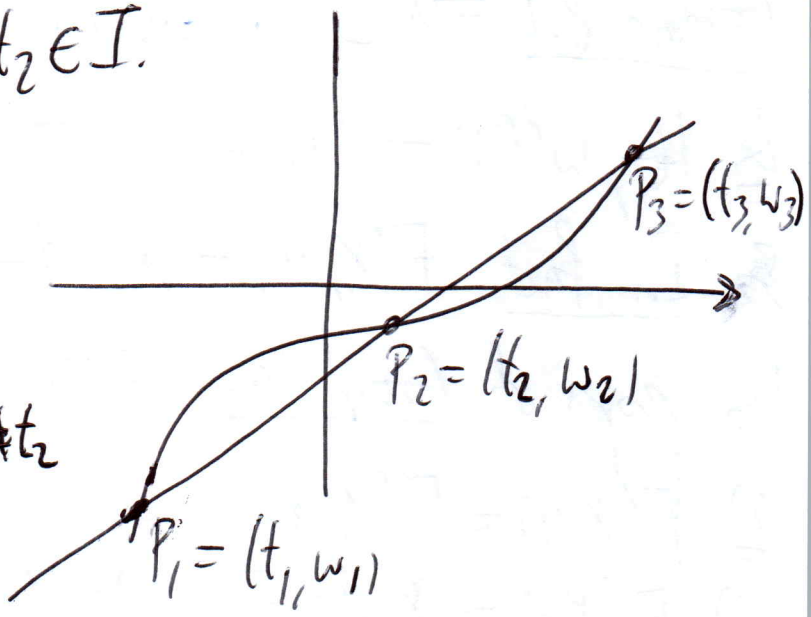
$\Rightarrow$ Suffices to show if $P_1, P_2 \in \hat{E}(I)$ then $-P_1 - P_2 \in \hat{E}(I)$.

Have: $P_1, P_2 \in \hat{E}(I) \Rightarrow t_1, t_2 \in I$.

& $w_1 = w(t_1)$ & $w_2 = w(t_2)$.

$w(t) = \sum_{n \geq 2} A_{n-2} t^{n+1}$, $A_0 = 1$.

$\Rightarrow \lambda = \begin{cases} \dfrac{w(t_2) - w(t_1)}{t_2 - t_1} & \text{if } t_1 \neq t_2 \\ w'(t_1) & \text{else.} \end{cases}$



$= \sum_{n \geq 2} A_{n-2} (t_1^n + t_1^{n-1} t_2 + \cdots + t_2^n)$ | $w = \lambda t + v$. $\in I$.

$\Rightarrow v = w_1 - \lambda t_1 \in I$ too.

So, substituting $w = \lambda t + v$ into $w = f(t,w)$ gives:

$$\lambda t+v = t^3 + a_1 t(\lambda t+v) + a_2 t^2(\lambda t+v) + a_3 (\lambda t+v)^2$$
$$+ a_4 t(\lambda t+v)^2 + a_6(\lambda t+v)^3.$$

Let: $A = (\text{Coeff of } t^3) = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$

$B = (\text{Coeff of } t^2) = a_1\lambda + a_2 v + a_3\lambda^2 + 2a_4\lambda v + 3a_6\lambda^2 v.$

$\Rightarrow A \in R^\times$, $B \in I$, so $t_3 = -B/A - t_1 - t_2 \in I$

& $w_3 = \lambda t_3 + v \in I$: ✓

Taking: $R = \mathbb{Z}[a_1, \dots, a_6][\![t]\!]$, $I = (t)$:

By Lemma 8.2: $\exists\, i \in R$, with $i(t) = 0$. & $[-1](t, w(t)) = (i(t), w(i(t)))$.

Taking: $R = \mathbb{Z}[a_1, \dots, a_6][\![t_1, t_2]\!]$: $I = (t_1, t_2)$:

Lemma 8.2 $\Rightarrow \exists\, F \in \mathbb{Z}[a_1, \dots, a_6][\![t_1, t_2]\!]$, with: $F(0,0) = 0$

& $(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1,t_2) + w(F(t_1,t_2)))$.

In fact: $F(X,Y) = X + Y - a_1 XY - a_2(X^2Y + XY^2) + \cdots$

By props of Group law: deduce:

i) $F(X,Y) = F(Y,X)$

ii) $F(X,0) = X$ & $F(0,Y) = Y$

iii) $F(X, F(Y,Z)) = F(F(X,Y), Z)$

iv) $F(X, i(X)) = 0$.

Group!

DEF] R ring, A formal Group Law over R is $F \in R[\![X,Y]\!]$ satisfying i), ii) & iii).

Exercise $\forall F$ group law $\exists!\ i(X) = -X + \cdots \in R[\![X]\!]$, with: $F(X, i(X)) = 0$.

Examples i) $F(X,Y) = X+Y \Rightarrow \hat{G}_a$

ii) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1 \Rightarrow \hat{G}_m$

iii) F as in elliptic func : $\Rightarrow \hat{E}$.

DEF $\mathcal{F}, \mathcal{G}$ formal group laws over R., given by the power series F, G resp.

i) Morphism $\mathcal{F} \to \mathcal{G}$ is: $f \in R[\![T]\!]$, with $f(0) = 0$ & $f(F(X,Y)) = G(f(X), f(Y))$.

ii) $\mathcal{F} \cong \mathcal{G} \iff \exists\ \mathcal{F} \xrightarrow{f} \mathcal{G},\ \mathcal{G} \xrightarrow{g} \mathcal{F}$ morphisms with $f \circ g\,(X) = g \circ f\,(X) = X$.

Theorem 8.3 If $\mathrm{Char}(R) = 0$ then Any formal group law $\mathcal{F}$ over R is isomorphic to $\hat{G}_a$ over $R \otimes \mathbb{Q}$.

More precisely: i) $\exists!$ Power series $\mathrm{Log}(X) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots$ $(a_i \in R)$, with:

$$\log(F(X,Y)) = \log(X) + \log(Y) \quad (*)$$

ii) $\exists!$ Power series $\mathrm{Exp}(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$ $(b_i \in R)$

with: $\mathrm{Exp}(\mathrm{Log}(T)) = \mathrm{Log}(\mathrm{Exp}(T)) = T$.

Proof Denote $F_1(X,Y) \equiv \frac{\partial}{\partial X} F(X,Y)$.

Uniqueness: Denote $p(T) = \frac{\partial}{\partial T} \log(T) = 1 + a_2 T + a_3 T^2 + \dots$

Differentiate (*) WRT X gives: $p(F(X,Y))\, F_1(X,Y) = p(X)$.

Put $X=0 \Rightarrow p(Y) F_1(0,Y) = 1$, so $p(Y) = F_1(0,Y)^{-1}$. ✓

~~$\Rightarrow E(J) \overset{def}{=} \{(t,w) \in E(K): t,w \in J\} \subseteq E(K)$ is a subgroup.~~

~~[Note: By Hensel, $\hat{E}(J) = \{(t, w(t)) \in E(K): t \in J\}$]~~

Existence: Denote $p(T) = F_1(0,T)^{-1} = 1 + a_2 T + a_3 T^2 + \dots$ (for some $a_i \in R$), and: $\operatorname{Log}(T) \equiv T + \frac{a_2}{2} T^2 + \frac{a_3}{3} T^3 + \dots$

Then: $F(F(X,Y),Z) = F(X, F(Y,Z))$.

$\frac{\partial}{\partial X}$: $\Rightarrow F_1(F(X,Y),Z)\, F_1(X,Y) = F_1(X, F(Y,Z))$

$X=0$ $\Rightarrow F_1(Y,Z) F_1(0,Y) = F_1(0, F(Y,Z))$.

$\Rightarrow F_1(Y,Z)\, p(Y)^{-1} = p(F(Y,Z))^{-1}$.

$\Rightarrow F_1(Y,Z)\, p(F(Y,Z)) = p(Y)$.

Integrate WRT Y, $\Rightarrow \log(F(Y,Z)) = \log(Y) + h(Z)$.

(for some power series h)

By symmetry of Y, Z: get $h(Z) = \operatorname{Log}(Z)$ ✓

Elliptic Curves: Lecture 12 — 14/02/2024.

Lemma 8.4 Let $f(T) = aT + \dots \in R[\![T]\!]$, $a \in R^\times$.

Then: $\exists!\ g = a^{-1}T + \dots \in R[\![T]\!]$ s.t. $fg(T) = gf(T) = T$.

Proof Construct polys $g_n(T) \in R[T]$, with: $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ & $g_{n+1} \equiv g_n \pmod{T^{n+1}}$.

Then, $g = \lim_{n\to\infty} g_n$ satisfies $f(g(T)) = T$.

Base case: $g_1(T) = a^{-1}T$.

Inductive Step Suppose $n \geq 2$ & $g_{n-1}(T)$ exists. Then, have:

$f(g_{n+1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$. (Some $b \in R$.)

Put: $g_n(T) = g_{n-1}(T) + \lambda \cdot T^n$ for $\lambda \in R$ (to be chosen later)

$\Rightarrow f(g_n(T)) = f(g_{n-1}(T) + b\cdot T^n) \equiv f(g_{n-1}(T)) + a\lambda T^n \pmod{T^{n+1}}$

$\equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}$

So, take $\lambda = -b/a$, which exists since $a \in R^\times$. ✓

To get $g(f(T)) = T$: well, $g = a^{-1}T + \dots \in R[\![T]\!]$.

$\Rightarrow$ Apply the construction to g, to get $h(T) = aT + \dots \in R[\![T]\!]$ with $g(h(T)) = T$.

$\Rightarrow f(g(h(T))) = h(T) = f(T)$ ✓ So indeed.

Theorem 8.3 (ii) now follows by Lemma 8.4 ✓

[& Denominator part is Example Sheet 2, Q12.]

Notation] $\mathcal{F}$ formal group (e.g. $\mathbb{G}_a$, $\mathbb{G}_m$, $\hat{E}$) given by a Power Series $F \in R[[X,Y]]$.

& Suppose: R I-adically complete. ($I \subseteq R$)

Then: $\forall x,y \in I$, put $x \oplus_{\mathcal{F}} y = F(x,y)$.

& $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an Abelian group.

Examples] For $\mathcal{F} = \mathbb{G}_a$: $\mathbb{G}_a(I) = (I, +)$

& $\mathbb{G}_m(I) = (1+I, \times)$

& $\hat{E}(I)$ = Subgroup of $E(K)$ (from Lemma 8.2)

Corollary 8.5] $\mathcal{F}$ formal group over R & $n \in \mathbb{Z}$, $n \in R^*$.

1) $[n]: \mathcal{F} \to \mathcal{F}$ Isomorphism of formal groups

2) If $\mathcal{F}$ complete WRT I, then $\mathcal{F}(I) \xrightarrow{x^n} \mathcal{F}(I)$ is an isomorphism of groups. (In particular, no n-torsion.)

Proof] Know $[1]T = T$ & $[n]T = F([n-1]T, T)$ $\forall n \geq 2$

& $\forall n < 0$, have $[-1]T = i(T)$.

Know: $F(X,Y) = X+Y+XY(\cdots)$: $[2]T = 2T + \cdots$

and by induction, $[n]T = nT + \cdots \in R[[T]]$.

$\Rightarrow$ i) follows from Lemma 8.4, since $[n]$ ≠ Isomorphism if $n \in R^*$. Also, ii) follows ✓

---

§9: Elliptic Curves & Local Fields.

Let: K field, complete WRT discrete valuation $v: K^* \to \mathbb{Z}$.

& Valuation Ring $\mathcal{O}_K = \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$.

& Unit Group $\mathcal{O}_K^\times = \{x \in K^\times : v(x) = 0\}$.

& Maximal Ideal $\pi\mathcal{O}_K$. ($\pi \in K$ Uniformiser)

& Residue Field $k = \mathcal{O}_K / \pi\mathcal{O}_K$.

Assume: $\mathrm{Char}(K) = 0$ & $\mathrm{Char}(k) = p \neq 0$ (Mixed Char).

(E.g. $K = \mathbb{Q}_p$ & $\mathcal{O}_K = \mathbb{Z}_p$ & $k = \mathbb{F}_p$).

Let: E/K elliptic curve.

DEF] Weierstrass eqn for E is one with coeffs $a_1, \ldots, a_6$.

Integral $\Leftrightarrow$ $a_1, \ldots, a_6 \in \mathcal{O}_K$

minimal $\Leftrightarrow$ $v(\Delta)$ minimal, among all Integral Weierstrass eqns for E.

Remark] 1) Let $x \mapsto u^2 x$, $y \mapsto u^3 y$. $\Rightarrow a_i \mapsto u^i a_i$.

So, integral Weierstrass eqns exist (Clear denoms)

2) $a_i \in \mathcal{O}_K \Rightarrow \Delta \in \mathcal{O}_K \Rightarrow$ minimal Weierstrass eqns exist
($v(\Delta) \geq 0$)

3) If $\mathrm{Char}(k) \neq 2, 3$ then can find minimal Weierstrass eqns of form $y^2 = x^3 + ax + b$.

Lemma 9.1] E/K integral W-eqn:

$$y^2 + a_1 yx + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let: $P = (x, y) \in E(K)$ nonzero. Then: either $x, y \in \mathcal{O}_K$ or:

$\exists s \geq 1$, $v(x) = -2s$ & $v(y) = -3s$.

Proof] Case $v(x) \geq 0$: If $v(y) < 0$ then $v(\text{LHS}) < 0$ and $v(\text{RHS}) \geq 0$ ⚡. So, $v(y) \geq 0$ too.

Case $v(x) < 0$: $v(\text{LHS}) \geq \min(2v(y), v(x)+v(y), v(y))$

$v(\text{RHS}) = 3v(x)$

$\Rightarrow v(y) < v(x)$. (Do cases)

So, $v(\text{LHS}) = 2v(y)$ & $v(\text{RHS}) = 3v(x)$, so good ✓

Let: K complete. $\Rightarrow \mathcal{O}_K$ complete WRT $\pi^r \mathcal{O}_K$ $\forall r \geq 1$.

Fix: minimal W-eqn for E/K. $\Rightarrow$ Gives Formal group $\hat{E}$ over $\mathcal{O}_K$.

Taking $R = \mathcal{O}_K$ & $I = \pi^r \mathcal{O}_K$ $(r \geq 1)$ in Lemma 8.2: gives

$$\hat{E}(\pi^r \mathcal{O}_K) = \left\{(x,y) \in E(K) : -\frac{x}{y}, -\frac{1}{y} \in \pi^r \mathcal{O}_K\right\}.$$

Elliptic Curves: lecture 13 — 16/02/2024

For $r \geq 1$ define the following:

$$\hat{E}(\pi^r \mathcal{O}_K) = \left\{(x,y) \in E(K) : -\frac{x}{y}, -\frac{1}{y} \in \pi^r \mathcal{O}_K\right\} \cup \{0\}$$

$$= \left\{(x,y) \in E(K) : v\left(\frac{x}{y}\right), v\left(\frac{1}{y}\right) \geq r\right\} \cup \{0\}$$

$$= \left\{(x,y) \in E(K) : \exists s \geq r,\ v(x) = -2s,\ v(y) = -3s\right\}$$

$$= \left\{(x,y) \in E(K) : v(x) \leq -2r,\ v(y) \leq -3r\right\} \cup \{0\}$$

By lemma 8.2: $E_r(K) \equiv \hat{E}(\pi^r \mathcal{O}_K) \subseteq E(K)$.

$\Rightarrow \cdots \subseteq E_3(K) \subseteq E_2(K) \subseteq E_1(K) \subseteq E(K)$.

More generally: if $\mathcal{F}$ formal group law, then (over $\mathcal{O}_K$)

$\cdots \subseteq \mathcal{F}(\pi^3 \mathcal{O}_K) \subseteq \mathcal{F}(\pi^2 \mathcal{O}_K) \subseteq \mathcal{F}(\pi \mathcal{O}_K)$.

[Claim] $\exists R \geq 1$, $\forall r \geq R$, $\mathcal{F}(\pi^r \mathcal{O}_K) \cong (\mathcal{O}_K, +)$

& $\dfrac{\mathcal{F}(\pi^r \mathcal{O}_K)}{\mathcal{F}(\pi^{r+1} \mathcal{O}_K)} \cong (k, +)$ $\forall r \geq 1$.

[Reminder: k has char $p > 0$ & $\mathrm{Char}(K) = 0$.]

Theorem 9.2] $\mathcal{F}$ formal group law / $\mathcal{O}_K$ & $e = v(p)$.

If $r > \dfrac{e}{p-1}$, then: $\log : \mathcal{F}(\pi^r \mathcal{O}_K) \xrightarrow{\cong} \hat{G}_a(\pi^r \mathcal{O}_K)$

is isomorphism of groups & Inverse $\exp$.

Remark $\hat{G}_a(\pi^r \mathcal{O}_K) = (\pi^r \mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$ so first part of claim follows.

Proof Recall: $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$, $b_i \in \mathcal{O}_K$.

& Know: $v_p(n!) = \frac{n - s_p(n)}{p-1} \leq \frac{n-1}{p-1}$.

$$\Rightarrow v\left(\frac{b_n x^n}{n!}\right) \geq nr - \left(\frac{n-1}{p-1}\right)e = (n-1)\left(r - \frac{e}{p-1}\right) + r.$$

This is: always $\geq r$, and $\longrightarrow \infty$, since $r > \frac{e}{p-1}$.

$\Rightarrow \exp(x)$ converges in $\pi^r \mathcal{O}_K$.

[Same argument applies to $\log(1+x)$ ✓]

Lemma 9.3 $\dfrac{\mathcal{G}(\pi^r \mathcal{O}_K)}{\mathcal{G}(\pi^{r+1}\mathcal{O}_K)} \cong (k, +)$ $\forall r \geq 1$.

Proof By def. of Formal group: $F(X,Y) = X + Y + XY(\cdots)$

$\Rightarrow F(\pi^r x, \pi^r y) \equiv \pi^r (x+y) \bmod \pi^{r+1}$

$\Rightarrow \mathcal{G}(\pi^r \mathcal{O}_K) \longrightarrow (k, +)$ is Surjective group hom.

$\pi^r x \longmapsto (x \bmod \pi)$

Kernel is: $\mathcal{G}(\pi^{r+1}\mathcal{O}_K)$. So ✓

Corollary If $|k| < \infty$, then $\mathcal{G}(\pi \mathcal{O}_K)$ has: Subgroup of Finite idx, isomorphic to $(\mathcal{O}_K, +)$.

Notation Reduction mod π, $\mathcal{O}_K \longrightarrow \dfrac{\mathcal{O}_K}{\pi \mathcal{O}_K} = k$

$$x \longmapsto \tilde{x} := x + \pi\mathcal{O}_K.$$

Prop 9.4 Let: E/K elliptic curve. The Reduction mod π of any 2 minimal W-eqns for E/K define Isomorphic

curves over k.

Proof] W-eqns related by: $[u,r,s,t]$: $u,r,s,t \in K$, $u \neq 0$.

& $\Delta_1 = u^{12}\Delta_2$ So, by minimality, $u \in \mathcal{O}_K^\times$

By transformation formulae for a_i & b_i: & fact that $\mathcal{O}_K$ integrally closed: get $r,s,t \in \mathcal{O}_K$.

$\Rightarrow$ W-eqns for reductions mod π are related by: $[\tilde{u},\tilde{r},\tilde{s},\tilde{t}]$, hence, since $\tilde{u} \in k^*$, they isomorphic ✓

DEF] Reduction $\tilde{E}/k$ of E/K is: defined by the reduction mod π of minimal W-eqn for E.

Say: E good reduction if $\tilde{E}$ nonsingular ($\Rightarrow$ Elliptic)

& E Bad reduction otherwise.

For integral W-eqn:

- $v(\Delta) = 0 \Rightarrow$ Good reduction
- $0 < v(\Delta) < 12 \Rightarrow$ Bad reduction
- $v(\Delta) \geq 12 \Rightarrow$ Can be either. (Beware!) (might not be minimal)

There is: well-def'ed map $\mathbb{P}^2(K) \longrightarrow \mathbb{P}^2(k)$

$(X:Y:Z) \longmapsto (\tilde{X}:\tilde{Y}:\tilde{Z})$

[Where: choose representative $(X:Y:Z)$ s.t. $\min(v(X), v(Y), v(Z)) = 0$.]

Restrict to give: $E(K) \longrightarrow \tilde{E}(k)$

$P \longmapsto \tilde{P}$

If $P=(x,y) \in E(K)$, then by Lemma 9.1:

(*) $x, y \in \mathcal{O}_K \Rightarrow \tilde{P} = (\tilde{x}, \tilde{y}) \in \tilde{E}(k)$ ($v=0$)

(*) $\left.\begin{matrix} v(x) = -2s \\ v(y) = -3s \end{matrix}\right] \Rightarrow P = (x:y:1) = (\pi^{3s}x : \pi^{3s}y : \pi^{3s}z)$

$\Rightarrow \tilde{P} = (0:1:0)$.

$\Rightarrow E_1(K) \equiv \hat{E}(\pi\mathcal{O}_K) = \{P \in E(K) : \tilde{P} = O\}$

"Kernel of Reduction".

Let: $\tilde{E}_{ns} = \begin{cases} \tilde{E} & \text{if } E \text{ good reduction} \\ \tilde{E} - \{\text{singular pt}\} & \text{if Bad reduction.} \end{cases}$

$\Rightarrow$ The Chord + Tangent process still defines group law on $\tilde{E}_{ns}$.

In Bad Reduction: $\tilde{E}_{ns} \cong \tilde{G}_a$, or $\tilde{G}_m$.

$\tilde{G}_a$: Additive Reduction

$\tilde{G}_m$: Mult reduction.

Elliptic Curves: Lecture 14) 19/02/2024

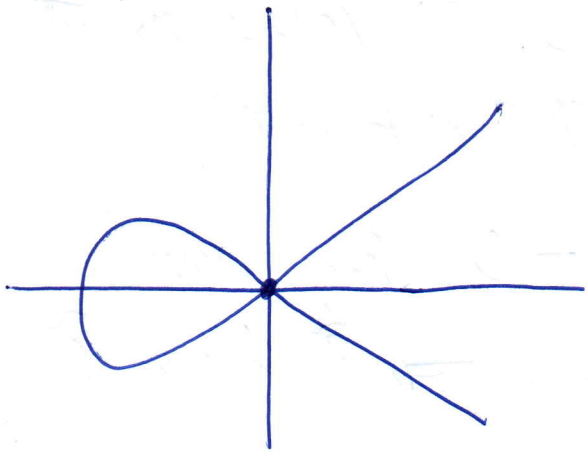
From last time Defined: $\widetilde{E}_{ns} = \begin{cases} \widetilde{E}, & \text{good reduction} \\ \widetilde{E} - \{\text{sing pt}\}, & E \text{ bad reduction.} \end{cases}$

The Chord & Tangent process still defines: group law, on $\widetilde{E}_{ns}$.

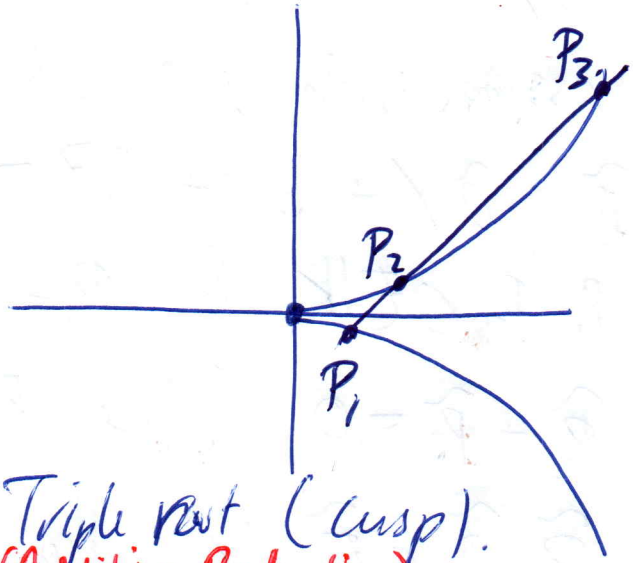
In case of Bad reduction: $\widetilde{E}_{ns} \cong \mathbb{G}_m$ (over k, or over quadratic ext of k)

or $\widetilde{E}_{ns} \cong \mathbb{G}_a$ (over k).

For simplicity: assume $\mathrm{char}(k) \neq 2$. $\Rightarrow \widetilde{E} = \{y^2 = f(x)\}$.



Double root (Node)
(Multiplicative Reduction)



Triple root (cusp).
(Additive Reduction)

Double root $\Rightarrow$ Example sheet 3.

Triple root: have: $\widetilde{E}_{ns} \longrightarrow \mathbb{G}_a$, by: $(x,y) \longmapsto x/y$

$(t^{-2}, t^{-3}) \longmapsto t$

$\infty \longmapsto 0$

Need to check: chord & Tangent process gives the desired group law.

Let: $ax + by = 1$ & P_1, P_2, P_3 on this line.

& $P_i = (x_i, y_i)$, $t_i \equiv x_i/y_i$. Then: $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$

$\Rightarrow t_i^3 - at_i - b = 0$.

$\Rightarrow t_1, t_2, t_3$ are roots of $X^3 - aX - b = 0$.
& Looking at coeffs of $X^2 \Rightarrow t_1 + t_2 + t_3 = 0$ ✓

DEF $\boxed{E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}}$.

Prop 9.5 $E_0(K) \subseteq E(K)$ Subgroup.
& Reduction mod π is surj group hom $E_0(K) \twoheadrightarrow \tilde{E}_{ns}(k)$.

Proof Group hom: Know, a line $\ell \subset \mathbb{P}^2$ is defined by: $aX + bY + cZ = 0$. $(a, b, c \in K)$
May assume: $\min(v(a), v(b), v(c)) = 0$. So, reduce mod π:
$\Rightarrow \tilde{\ell}$: $\tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$ $(\tilde{a}, \tilde{b}, \tilde{c} \in \tilde{K} = k)$
If $P_1, P_2, P_3 \in E(K)$ & $P_1 + P_2 + P_3 = O$, then have:
$\tilde{P_1} + \tilde{P_2} + \tilde{P_3} = O$ (since P_i lie on $\ell \Rightarrow \tilde{P_i}$ lie on $\tilde{\ell}$)
& If $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{ns}(k)$, then $\tilde{P}_3 \in \tilde{E}_{ns}(k)$ since $\tilde{E}_{ns}$ gives a group (checked before).
$\Rightarrow$ If $P_1, P_2 \in E_0(K)$ then $P_3 \in E_0(K)$ & $\tilde{P_1} + \tilde{P_2} + \tilde{P_3} = O$ ✓
[Exercise: Check this if 2 of P_i are the same.]

Surjectivity Let: $f(x, y) = y^2 + a_1 xy + a_3 y - (x^3 + \cdots)$
Let: $\tilde{P} \in \tilde{E}_{ns}(k) - O$, say $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$. $\tilde{x}_0, \tilde{y}_0 \in \mathcal{O}_K$.
Then, $\tilde{P}$ non-singular $\Rightarrow$ Either $\frac{\partial f}{\partial X}(x_0, y_0) \not\equiv 0$ or $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0$

If i): then let $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$.

$\Rightarrow \left\{ \begin{array}{l} g(x_0) \equiv 0 \bmod \pi \\ g'(x_0) \in \mathcal{O}_K^\times \end{array} \right]$ $\Rightarrow$ By Hensel 7b, $\left\{ \begin{array}{l} g(b) = 0 \\ b \equiv x_0 \bmod \pi \end{array} \right.$

$\Rightarrow (b, y_0) \in E(K)$ has reduction $\widehat{P} = (x_0, y_0)$ ✓

& Case ii) is exactly the same ✓

Recall: $\forall r \geq 1$, had $E_r(K) = \{(x,y) \in \mathcal{O}_K : \begin{array}{l} v(x) \leq -2r \\ v(y) \leq -3r \end{array} \} \cup \{0\}$.

$E_1(K) = E(\pi^r \mathcal{O}_K)$.

$\Rightarrow E_r(K) \subseteq \cdots \subseteq E_2(K) \subseteq E_1(K) \subseteq E_0(K) \overset{?}{\subseteq} E(K)$

$\| \wr$

$(\mathcal{O}_K, +)$

Quotients $\cong (k, +)$ $\qquad \cong \widetilde{E}_{ns}(k)$.

Lemma 9.6 If k finite then $E_0(K) \subseteq E(K)$ finite idx.

Proof Since $|k| < \infty$, know: $|\mathcal{O}_K / \pi^r \mathcal{O}_K| < \infty \ \forall r \geq 1$.

$\Rightarrow \mathcal{O}_K = \varprojlim (\mathcal{O}_K / \pi^r \mathcal{O}_K)$ Profinite group, so Compact.

& $\mathbb{P}^n(K)$ is Union of sets: $\{(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) : a_j \in \mathcal{O}_K\}$

hence compact as well.

& $E(K) \subseteq \mathbb{P}^n(K)$ closed $\Rightarrow$ Compact.

Hence: $E(K)$ is Compact topological group.

If $\widehat{E}$ has a singular point $(\widehat{x_0}, \widehat{y_0})$, then: $E(K) \setminus E_0(K)$

$= \{(x,y) \in E(K) : v(x - x_0) \geq 1, \ v(y - y_0) \geq 1\}$

is: closed subset of $E(K)$.

$\Rightarrow E_0(K)$ is Open subgroup of $E(K)$.

Notice that cosets of $E_0(K)$ in $E(K)$ is an open cover for $E(K)$, hence by compactness, gives: $[E(K):E_0(K)] < \infty$.

Remark 1) Results true when k infinite, too!

DEF $c_K(E) \equiv [E(K):E_0(K)]$ Tamagawa number.

Remarks 1) Good reduction $\Rightarrow c_K(E) = 1$

But, converse is false.

2) Can be shown: Either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$.

[Essential that we work over minimal W-eqn.]

Theorem 9.7 $K/\mathbb{Q}_p$ finite. Then, $E(K)$ contains subgroup of finite index $\cong (\mathcal{O}_K, +)$.

Let: $L/K/\mathbb{Q}_p$ finite exts. $\Rightarrow f = [k':k]$.

& e defined by

$$\begin{array}{ccc} K^\times & \xrightarrow{v_K} & \mathbb{Z} \\ \cap & & \downarrow \times e. \\ L^\times & \xrightarrow{v_L} & \mathbb{Z} \end{array}$$

Facts: 1) $[L:K] = ef$

2) If L/K Galois then $\exists$ natural map $Gal(L/K) \to Gal(k'/k)$ which is Surjective kernel size e.

Elliptic Curve: lecture 15 | 21/02/2024

In this section: $[K:\mathbb{Q}_p] < \infty$ & L/K finite with $[L:K] = e$. f.

Say, L/K unram $\Leftrightarrow e = 1$.

Facts] for each $m \geq 1$:

a) K has unique ext. degree m, k_m

b) K has unique unram ext. degree m, k_m]

& Galois groups, with cyclic galois group.

DEF] $K^{nr} \equiv \bigcup_{n \geq 1} k_n \quad (\subseteq \bar{K})$ maximal unram ext.

Theorem 9.8] $[K:\mathbb{Q}_p] < \infty$. & E/K elliptic, good reduction, and ptn. If $P \in E(K)$, then: $K([n]^{-1}P)/K$ unram.

[$[n]^{-1}P = \{Q \in E(\bar{K}) : nQ = \mathcal{O}P\}$

& $K(\{Q_1, \dots, Q_n\}) = K(x_1, \dots, x_n, y_1, \dots, y_n)$, $Q_i = (x_i, y_i)$]

Proof] $\forall m \geq 1$, $\exists$ SES $0 \to E_1(K_m) \to E(K_m) \to \tilde{E}(k_m) \to 0$.

Take $\bigcup_{m \geq 1}$ gives: $0 \to E_1(K^{ur}) \to E(K^{ur}) \to \tilde{E}(\bar{k}) \to 0$.

$$\begin{array}{ccccccc} 0 & \to & E_1(K^{ur}) & \to & E(K^{ur}) & \to & \tilde{E}(\bar{k}) \to 0 \\ & & \textcircled{1}\downarrow \times n & & \textcircled{2}\downarrow \times n & & \textcircled{3}\downarrow \times n \\ 0 & \to & E_1(K^{ur}) & \to & E(K^{nr}) & \to & \tilde{E}(\bar{k}) \to 0 \end{array}$$

①: Isomorphism (by Cor 8.5, applied to each K_m) ~~(ptn)~~

③: Surjective by Theorem 2.8 & kernel $\cong (\mathbb{Z}/n\mathbb{Z})^2$ by 6.5 (again using ptn).

$\Rightarrow$ By Snake lemma:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker^0 & \longrightarrow & \ker & \longrightarrow & \ker & \cong (\mathbb{Z}/n\mathbb{Z})^2 & \\
0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \tilde{E}(k) & \longrightarrow & 0 \\
 & & \downarrow \times n & & \downarrow \times n & & \downarrow \times n & & \\
0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \tilde{E}(k) & \longrightarrow & 0 \\
 & & \longrightarrow \operatorname{coker}^0 & \longrightarrow & \operatorname{coker} & \longrightarrow & \operatorname{coker} & \longrightarrow & 0
\end{array}$$

$\Rightarrow \ker(E(K^{nr}) = E(K^{nr})[n] = (\mathbb{Z}/n\mathbb{Z})^2$

& $\operatorname{coker}(E(K^{nr}) = E(K^{nr})/nE(K^{nr}) = 0.$

$\Rightarrow \forall P \in E(K)$: $\exists Q \in E(K^{nr})$, $nQ = P$.

$\Rightarrow K([n]^{-1}P) \subseteq K^{nr}$ (since: $[n]^{-1}P = \{Q+T : T \in E[n]\} \subseteq E(K^{nr})$)

$\Rightarrow K([n]^{-1}P)/K$ Unramified ✓

---

§10: Elliptic Curves over NF's.

1]: Torsion Subgroup. Let: $[K:\mathbb{Q}] < \infty$ & E/K elliptic.

Say $\mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal. $K_{\mathfrak{p}}$ = $\mathfrak{p}$-adic completion of K

$k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$.

DEF] $\mathfrak{p}$ prime of K: **good reduction** if $E/K_{\mathfrak{p}}$ good reduction.

Lemma 10.1] E/K has finitely many primes $\mathfrak{p}$ of Bad reduction.

Proof] Take W-eqn for E, coeffs $a_1, \dots, a_6 \in \mathcal{O}_K$.

Then: E non-singular $\Rightarrow 0 \neq \Delta \in \mathcal{O}_K$, so $(\Delta) = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$.

Denote: $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ Claim: S contains all bad reductions.

If $\mathfrak{p} \notin S$ then $v_{\mathfrak{p}}(\Delta) = 0 \Rightarrow E/K_{\mathfrak{p}}$ good reduction ✓
So, indeed, finitely many Bad reduction primes.

Remark If K has class number 1: (e.g. $K = \mathbb{Q}$) then can always find W-eqn E, s.t. $a_i \in \mathcal{O}_K$, which is minimal at ALL primes $\mathfrak{p}$. [Fails if class number > 1].

Basic Group Theory.

A_{tors}

⊛ If A f.g. Abelian group $\Rightarrow A \cong (\text{finite}) \times \mathbb{Z}^r$. ($r$ = rank)

Lemma 10.2 $E(K)_{tors}$ is finite.

Proof Take **ANY** prime $\mathfrak{p}$. Saw: $E(K_{\mathfrak{p}})$ has a subgroup A of finite index, with $A \cong (\mathcal{O}_{\mathfrak{p}}, +)$.
In particular: A is torsion-free, & $E(K)_{tors} \subseteq E(K_{\mathfrak{p}})_{tors} \hookrightarrow \frac{E(K_{\mathfrak{p}})}{A}$
$\Rightarrow E(K)_{tors}$ is finite ✓

Lemma 10.3 $\mathfrak{p}$ prime of Good reduction. $\mathfrak{p} \nmid n$. Then: reduction mod $\mathfrak{p}$ gives: injective group hom $E(K)[n] \hookrightarrow \tilde{E}(k_{\mathfrak{p}})$.

Proof By Prop 9.5: $E(K_{\mathfrak{p}}) \to \tilde{E}(K_{\mathfrak{p}})$ group hom, with kernel $E_1(K_{\mathfrak{p}})$. So, by Corollary 8.5 ($\mathfrak{p} \nmid n$), gives: $E_1(K_{\mathfrak{p}})$ has no n-torsion ✓

Example 1 $E/\mathbb{Q}$ elliptic, $y^2 + y = x^3 - x^2$. $\Rightarrow \Delta = -11$.
$\Rightarrow E$ has Good ~~torsion~~ reduction $\forall p \neq 11$.

p	2	3	5	7	11	13
$\#\tilde{E}(\mathbb{F}_p)$	5	5	5	10	–	10

By Lemma 10.3: $\#E(\mathbb{Q})_{tors} \mid 5 \cdot 2^a$, some $a \geq 0$.

$\#E(\mathbb{Q})_{tors} \mid 5 \cdot 3^b$, some $b \geq 0$.

$\Rightarrow \#E(\mathbb{Q})_{tors} \mid 5$.

& For $T = (0,0) \in E(\mathbb{Q})$, get: $5T = 0$, so indeed $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$.

Example 2) $E/\mathbb{Q}$ & $y^2 + y = x^3 + x^2$. $\Delta = -43$.

p	2	3	5	7	11	13
$\#\tilde{E}(\mathbb{F}_p)$	5	6	10	8	9	19.

By Lemma 10.3: $\#E(\mathbb{Q})_{tors} \mid 2 \cdot 5^a$, $a \geq 0$.
& $\#E(\mathbb{Q})_{tors} \mid 9 \cdot 11^b$, $b \geq 0$. $\Rightarrow = \underline{1}$.

$\Rightarrow P = (0,0)$ is point of Infinite order! $E(\mathbb{Q})$ infinite.

Example 3 | $E_D : y^2 = x^3 - D^2 x$. $D \in \mathbb{Z}$ square-free.

$\Rightarrow \Delta = 2^6 \cdot D^6$.

& $E_D(\mathbb{Q})_{tors} \supseteq \{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Let: $f(x) = x^3 - D^2 x$. If $p \nmid 2D$ then $\#\tilde{E}_D(\mathbb{F}_p)$
$= 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right)$. & If $p \equiv 3 \bmod 4$ then $\#\tilde{E}_D(\mathbb{F}_p)$
$= p+1$. ⊞

Elliptic Curves: Lecture 16 | 23/02/2024

Example 3 (continued): $E_D = \{y^2 = \underbrace{x^3 - D^2 x}_{\equiv f(x)}\}$.

If $p \nmid 2D$ & $p \equiv 3 \bmod 4$, then: $\#\tilde{E}(\mathbb{F}_p) = p+1$.

[Since: $\left(\frac{f(-x)}{p}\right) = \left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right) = -\left(\frac{f(x)}{p}\right)$]

$\Rightarrow$ If $m = \#E_D(\mathbb{Q})_{tors}$, then: $4 \mid m \mid p+1$ for all p large. (i.e. $p \nmid 2Dm$) & $p \equiv 3 \bmod 4$.

If $8 \mid p+1$ or $\ell \mid p+1$ # for some odd prime ℓ, then this contradicts Dirichlet's Theorem on Arithmetic Primes.

$\Rightarrow m = 4$ & $E_D(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

So, $\mathrm{Rank}(E_D(\mathbb{Q})) \geq 1 \iff \exists (x,y) \in \mathbb{Q},\ y \neq 0,\ y^2 = f(x)$.

$\iff D$ Congruent number.

[Lemma 10.4] $E/\mathbb{Q}$ elliptic & W-eqn $\{a_1, \dots, a_6\} \subset \mathbb{Z}$.

Suppose: $0 \neq T \in E(\mathbb{Q})_{tors}$. Then:

1) $4x, 8y \in \mathbb{Z}$; 2) If $2 \mid a_1$ or $2T \neq 0$ then $x, y \in \mathbb{Z}$.

Proof | The W-eqn defines formal group $\hat{E}$ over $\mathbb{Z}$.

For $r \geq 1$, $\hat{E}(p^r\mathbb{Z}_p) = \{(x,y) \in E(\mathbb{Q}) : v_p(x) \leq -2r,\ v_p(y) \leq -3r\} \cup \{0\}$.

By Prop 4.2: $\hat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ $\forall r > \frac{1}{p-1}$.

$\Rightarrow$ ~~$\hat{E}(4\mathbb{Z}_2)$~~ $\hat{E}(4\mathbb{Z}_2)$ and $\hat{E}(p\mathbb{Z}_p)$ Torsion-free.

$\Rightarrow v_2(x) \geq -2$ & $v_p(x) \geq 0$
$v_2(y) \geq -3$ $\quad\quad$ $v_p(y) \geq 0$ $\forall p$ odd. ✓

For iii), say $T \in \hat{E}(2\mathbb{Z}_2) \Rightarrow v_2(x) = -2$ & $v_2(y) = -3$.

Know: $\dfrac{\hat{E}(2\mathbb{Z}_2)}{\hat{E}(4\mathbb{Z}_2)} \cong (\mathbb{F}_2, +)$ & $\hat{E}(4\mathbb{Z}_2)$ Torsion-free.

$\Rightarrow$ Let: $2T = 0$, so $T = -T = (x, y) = (x, -y - a_1 x - a_3)$

$\Rightarrow 2y + a_1 x + a_3 = 0$.

$\Rightarrow \underbrace{8y}_{\text{odd}} + a_1 \underbrace{(4x)}_{\text{odd}} + \underbrace{4a_3}_{\text{even}} = 0 \quad (8y, 4x \in \mathbb{Z})$

$\Rightarrow a_1$ odd ✓

Example $y^2 + xy = x^3 + 4x + 1$: $(-\frac{1}{4}, \frac{1}{8}) \in E(\mathbb{Q})[2]$.

Theorem 10.5 [Lutz – Nagell].

Let: $y^2 = x^3 + ax + b$ & $a, b \in \mathbb{Z}$. Suppose $0 \neq T = (x, y) \in E(\mathbb{Q})_{tors}$.

Then $x, y \in \mathbb{Z}$ (by Lemma 10.4)

& Either $y = 0$, or $y^2 \mid 4a^3 + 27b^2$.

Proof If $2T = 0$ then $y = 0$ ✓

Else, $2T$ is nonzero torsion point $(x_2, y_2) \in E(\mathbb{Q})_{tors}$.

By Lemma 10.4: $x_2, y_2 \in \mathbb{Z}$.

But: $x_2 = \left(\dfrac{f'(x)}{2y}\right)^2 - 2x \Rightarrow y \mid f'(x)$.

E nonsingular $\Rightarrow$ $f(x)$, $f'(x)$ coprime

$\Rightarrow$ $f(x)$, $(f'(x))^2$ coprime.

$\Rightarrow \exists\, g, h \in \mathbb{Q}[x]$, $gf + h(f')^2 = 1$.

& have: $(3x^2+4a)(f'(x))^2 - 27(x^3+ax-b)f(x) = 4a^3+27b^2$.

Since $y \mid f'(x)$ and $y^2 \mid f(x)$, get $y^2 \mid 4a^3+27b^2$ ✓

Remark Mazur showed: If $E/\mathbb{Q}$ elliptic curve, then:

$$E(\mathbb{Q})_{tors} \cong \begin{cases} (\mathbb{Z}/n\mathbb{Z}) & 1 \le n \le 12 \ \& \ n \neq 11 \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z}), & 1 \le n \le 4 \end{cases}$$

& All 15 possibilities occur.

---

§11: Kummer Theory.

Let: K field & $\mathrm{char}(K) \nmid n$. Assume: $\zeta_n \in K$.

Lemma 11.1 Let $\Delta \subseteq K^*/(K^*)^n$. Finite subgroup.

Then, $L = K(\sqrt[n]{\Delta}) \Rightarrow L/K$ Galois & $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$.

Proof Galois, since:

⊛ Normal since $\mu_n \subseteq K$

⊛ Separable since $\mathrm{char}(K) \nmid n$

Define: Kummer Pairing $\mathrm{Gal}(L/K) \times \Delta \longrightarrow \mu_n$

$$\langle \cdot, \cdot \rangle : (\sigma, x) \longmapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$$

Well-defined: If $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$, then:

$\left(\frac{\alpha}{\beta}\right)^n = 1 \Rightarrow \frac{\alpha}{\beta} \in \mu_n \subset K \Rightarrow \sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}$ ✓

$\Rightarrow \frac{\sigma(\alpha)}{\sigma(\beta)} = \frac{\alpha}{\beta}$

Bilinear: $\langle \sigma\tau, x\rangle = \frac{\sigma\tau(x)}{x} = \frac{\sigma\tau(x)}{\tau(x)} \frac{\tau(x)}{x}$

$= \frac{\sigma(x)}{x} \frac{\tau(x)}{x} = \langle \sigma, x\rangle \langle \tau, x\rangle$.

& $\langle \sigma, xy\rangle = \frac{\sigma(\sqrt[n]{xy})}{\sqrt[n]{xy}} = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \frac{\sigma(\sqrt[n]{y})}{\sqrt[n]{y}} = \langle \sigma, x\rangle \langle \sigma, y\rangle$.

Nondegenerate: Let $\sigma \in Gal(L/K)$.

If $\langle \sigma, x\rangle = 1 \ \forall x \in \Delta$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x} \ \forall x \in \Delta$,

so σ fixes L pointwise. $\Rightarrow \sigma = id$.

For $x \in K^*/(K^*)^n$. If $\langle \sigma, x\rangle = 1 \ \forall \sigma \in Gal(L/K)$

then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$, so $\sqrt[n]{x} \in K \Rightarrow x \in (K^*)^n$

$\Rightarrow x = 1$ (since coset)

So: ∃ Injective group homs:

i) $Gal(L/K) \hookrightarrow Hom(\Delta, \mu_n)$.

ii) $\Delta \hookrightarrow Hom(Gal(L/K), \mu_n)$

From (i): $Gal(L/K)$ Abelian. killed by $(\cdot)^n$.

Fact If G Finite Abelian, exponent $| n$, then:

$Hom(G, \mu_n) \cong G$ (non-canonically)

$\Rightarrow |Gal(L/K)| \leq |\Delta| \leq |Gal(L/K)| \Rightarrow$ Equality ✓

Elliptic Curves: Lecture 17 | 26/02/2024

Reminder: $\mathrm{char}(K) \nmid n$ & $\mu_n \subseteq K$.

Theorem 11.2) $\exists$ Bijection: $\{$Finite Subgroups of $K^*/(K^*)^n\} \longleftrightarrow$

and $\{$Finite Abelian exts L/K, exponent dividing $n\}$

where: $\mathrm{Exponent}(A) = \{\mathrm{lcm}\{\mathrm{ord}(a) : a \in A\}\}$.

Proof | i) Let $\Delta \subseteq K^*/(K^*)^n$, $L = K(\sqrt[n]{\Delta})$, $\Delta' = \frac{(L^*)^n \cap K^*}{(K^*)^n}$.

Need to show: $\Delta = \Delta'$. Know: $\Delta \subseteq \Delta'$

$\Rightarrow K(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'})$. But, $L = K(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'}) \subseteq L$.

$\Rightarrow K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$

$\Rightarrow |\Delta| = |\Delta'|$ by Lemma 11.1, hence $\Delta = \Delta'$ ✓

ii) Let L/K Finite Abelian ext, exponent dividing n.

& $\Delta = \frac{(L^*)^n \cap K^*}{(K^*)^n}$. Then: $K(\sqrt[n]{\Delta}) \subseteq L$, and need equality.

Let: $G = \mathrm{Gal}(L/K)$. $\Rightarrow$ By Kummer Pairing, $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$

Claim: This map is Surjective.

Proof of Claim Let $\chi : G \to \mu_n$ Group Hom.

Know, distinct Automorphisms of G are linearly indep.

$\Rightarrow \exists\, a \in L$ s.t. $\left(\sum_{\tau \in G} \chi(\tau)^{-1}\tau\right)(a) \neq 0$.

$\equiv y$.

For $\sigma \in G$, $\sigma(y) = \sum_{\tau \in G} \chi(\tau)^{-1} \sigma\tau(a)$ (since $\mu_n \subseteq K$)

$= \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1} \tau(a) = \chi(\sigma) y$ (*)

$\Rightarrow \sigma(y^n) = y^n \ \forall \sigma \in G$. So, $y^n \in K$. Denote $X = y^n \neq 0$.

Then, $X \in \underline{(L^*)^n \cap K^*} \Rightarrow$ [redacted] $\chi(K^*)^n \subseteq \Delta$

& By (*), $\chi : \sigma \mapsto \frac{\sigma(y)}{y} = \frac{\sigma(\sqrt[n]{X})}{\sqrt[n]{X}}$

$\Rightarrow \Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $X \mapsto \chi$ is Surjective ✓

Hence: $[K(\sqrt[n]{\Delta}) : K] \underset{\text{Lemma 11.1}}{=} |\Delta| = |G| = [L : K] \Rightarrow$ ✓

Prop 11.3 Let: K NF (so, $\mathrm{char}(K) = 0$) & $\mu_n \subset K$.

Let: [redacted] S finite set of primes of K.

Then: there are only finitely many exts L/K, such that:

1) L/K Finite, Abelian, exponent $| n$

2) L/K Unramified outside of S.

Proof By Theorem 11.2: $L = K(\sqrt[n]{\Delta})$, some $\Delta \subseteq \frac{K^*}{(K^*)^n}$.

For $\mathfrak{p}$ prime of K, have: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$, $\mathfrak{P}_i$ distinct.

If $x \in K^*$ represents some element of K^*, then:

$n v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(x) = e_i v_{\mathfrak{p}}(x)$

$\Rightarrow$ If $\mathfrak{p} \notin S$, then: $v_{\mathfrak{p}}(x) \equiv 0 \bmod n$ $(e_i = 1 \ \forall i)$

$\Rightarrow \Delta \subset \boxed{K(S,n) \equiv \left\{ x \in \frac{K^*}{(K^*)^n} : v_{\mathfrak{p}}(x) \equiv 0 \bmod n \ \forall \mathfrak{p} \notin S \right\}}$

Proof is then complete with following lemma.

Lemma 11.4 $K(S,n)$ Finite.

Proof The map $K(S,n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{|S|}$

$$x \longmapsto \left(v_{\mathfrak{p}}(x) \bmod n \right)_{\mathfrak{p} \in S}$$

Is: group hom (clearly)

& Kernel is $K(\phi, n)$.

Since S finite $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^{|S|}$ finite, so Suffices: $K(\phi,n)$ finite.

If $x \in K^*$ representing $K(\phi,n)$:

$\Rightarrow (x) = \mathfrak{a}^n$, some $\mathfrak{a}$ ideal (Fractional)

There is SES: $0 \longrightarrow \frac{O_K^*}{(O_K^*)^n} \longrightarrow K(\phi,n) \longrightarrow Cl_K[n] \longrightarrow 0$

$$x \longmapsto [\mathfrak{a}]$$

Know: $|Cl_K| < \infty$ & O_K^* f.g. Abelian (Dirichlet unit thm)

Hence: $K(\phi,n)$ Finite ✓

---

§12: Elliptic Curves over Number Fields

(II: The Weak Mordell-Weil Theorem)

Lemma 12.1 E/K Elliptic curve & L/K Finite Abelian ext. Then, natural map $\frac{E(K)}{nE(K)} \longrightarrow \frac{E(L)}{nE(L)}$ has Finite Kernel.

Proof For each element in kernel, pick coset rep $P \in E(K)$.

So, find Q_1 s.t. $nQ = P$. ($P \in$ Kernel).

$\Rightarrow \forall \sigma \in Gal(L/K), n(\sigma Q - Q) = \sigma(P) - P = O$.

$\Rightarrow \sigma(Q) - Q \in E[n]$

Since $Gal(L/K)$ & $E[n]$ Finite, only finitely many maps

$Gal(L/K) \longrightarrow E[n]$

$\sigma \longmapsto \sigma(Q) - Q$.

But: if $P_1, P_2 \in E(K)$, $P_i = nQ_i$ for $Q_i \in E[L]$,

and $\sigma(Q_1) - Q_1 = \sigma(Q_2) - Q_2$ $\forall \sigma \in Gal(L/K)$:

$\Rightarrow \sigma(Q_1 - Q_2) = Q_1 - Q_2$ $\forall \sigma \in Gal(L/K)$.

$\Rightarrow Q_1 - Q_2 \in E[K]$, so $P_1 - P_2 \in nE(K)$, so they represent same element of the kernel ✓

$\Rightarrow \ker\left(\frac{E(K)}{nE(K)} \longrightarrow \frac{E(L)}{nE(L)}\right) \hookrightarrow Maps(Gal(L/K), E[n])$ is Finite ✓

Elliptic Curves: Lecture 18 | 28/02/2024

The Weak Mordell-Weil Theorem.

Let: K NF, E/K Elliptic curve. $n \geq 2$ Then: $\frac{E(K)}{nE(K)}$ finite.

Proof Lemma 12.1 $\Rightarrow$ may replace K, with: finite Galois ext. of K. So, WLOG $\mu_n \subset K$ & $E[n] \subset E(K)$.

Let: $S \equiv \{\mathfrak{p} \mid n\} \cup \{\text{Primes of Bad reduction for } E/K\}$.

For each $P \in E(K)$: the ext. $K([n]^{-1}P)/K$ is Unram outside S (by Theorem 9.8)

& Since $\mathrm{Gal}(\bar{K}/K)$ acts on $[n]^{-1}(P)$: Follows that $K([n]^{-1}P)/K$ is Galois ext.

Let: $Q \in [n]^{-1}P$. Since $E[n] \subset E(K)$: $K(Q) = K([n]^{-1}P)$

& $\mathrm{Gal}(K(Q)/K) \hookrightarrow E[n]$

$\sigma \longmapsto \sigma Q - Q$

⊛ Group Hom: $\sigma\tau(Q) - Q = \sigma(\tau(Q) - Q) + \sigma Q - Q$.

⊛ Injective: $\sigma Q = Q \Rightarrow \sigma$ fixes $K(Q) \Rightarrow \sigma = id$.

$\Rightarrow K(Q)/K$ Abelian ext, exponent $\ln$ ($\mathrm{Gal} \leq (\mathbb{Z}/n\mathbb{Z})^2$)

& Unram. outside S.

By Prop 11.3: as $P \in E(K)$ varies, only finitely many possibilities of $K(Q)$.

So, Let L = Composite of all such extensions $K(Q)$.

$\Rightarrow$ L/k Finite, Galois & $\frac{E(k)}{nE(k)} \longrightarrow \frac{E(L)}{nE(L)}$ is 0 map.

By Lemma 12.1 $\Rightarrow$ $\frac{E(k)}{nE(k)}$ finite ✓ (Finite kernel.)

Remark If $k = \mathbb{R}$ or $\mathbb{C}$ or $[k : \mathbb{Q}_p] < \infty$, then:

$\frac{E(k)}{nE(k)}$ Finite, but $E(k)$ Uncountable ($\Rightarrow$ not f.g.)

Fact If k NF, $\exists$ Quadratic form ("Canonical Height") $\hat{h} : E(k) \longrightarrow \mathbb{R}_{\geq 0}$ s.t. $\forall B \geq 0$, $\{P \in E(k) : \hat{h}(P) \leq B\}$ Finite (*)

Mordell-Weil Theorem.

Let: k NF, E/k Elliptic. Then, $E(k)$ is F.g. Abelian.

Proof Fix $n \geq 2$. By weak M-W: $E(k)/nE(k)$ Finite.

Pick: Coset reps $P_1, \dots, P_m$. ✱✱

Let $\sum \equiv \{P \in E(k) : \hat{h}(P) \leq \max_{1 \leq i \leq m} \hat{h}(P_i)\}$.

Claim: $\sum$ Generates $E(k)$.

Indeed: If not, $\exists P \in E(k) \setminus \{\text{Span} \sum\}$, of minimal height. [Exists by (*)].

$\Rightarrow P = P_i + nQ$, some $1 \leq i \leq m$ & $Q \in E(k)$.

$\Rightarrow Q \in E(k) \setminus \{\text{Span} \sum\}$.

By minimality of P_i get: $4\hat{h}(P) \leq 4\hat{h}(Q) \leq n^2 \hat{h}(Q)$

$= \hat{h}(nQ) = \hat{h}(P - P_i) \leq \hat{h}(P - P_i) + \hat{h}(P + P_i)$

$= 2\hat{h}(P) + 2\hat{h}(P_i)$. ✱

So, we proved claim, and by (*), $\sum$ finite, so ✓

---

§13: Heights.

For simplicity: take $K = \mathbb{Q}$.

Write: $\mathbb{P}^n = \mathbb{P}^n(\mathbb{Q})$, $P = (a_0 : a_1 : \dots : a_n)$. $a_i \in \mathbb{Z}$, and $\gcd(a_0, \dots, a_n) = 1$.

DEF $H(P) = \max_{0 \le i \le n} |a_i|$.

Lemma 13.1 Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ coprime & homogeneous polynomials, of degree d. Let: $F : \mathbb{P}^1 \to \mathbb{P}^1$.

$$(X_1 : X_2) \mapsto (f_1(X_1, X_2) : f_2(X_1, X_2))$$

Then: $\exists\, c_1, c_2 > 0$ s.t. $c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d$.

$\forall P \in \mathbb{P}^1(\mathbb{Q})$:

Proof WLOG: $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$.

$$\Rightarrow H(F(P)) \le \max(|f_1(a,b)|, |f_2(a,b)|) \le c_2 \max(|a|^d, |b|^d) \le c_2 H(P)^d.$$

[c_2 = [redacted] sum of $|\text{coeffs}|$ of f_i, $i = 1, 2$, will do].

Lower bound: Claim $\exists\, g_{ij} \in \mathbb{Z}[X_1, X_2]$, homog, deg $d-1$, and: $k \in \mathbb{Z}_{>0}$, s.t. $\sum_{j=1}^{2} g_{ij} f_j = k \cdot X_i^{2d-1}$ $(i = 1, 2)$.

Indeed: running Euclidean Alg on $f_1(X, 1)$ & $f_2(X, 1)$ gives: $r, s \in \mathbb{Q}[X]$, degree $< d$, with:

$$r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1.$$

& Homogenise & Clear denoms, gives Claim $(i = 2)$. Similar, $i = 1$. ☐3

So, write: $P = (a_1; a_2)$ $a_1, a_2 \in \mathbb{Z}$ coprime.

(†) $\Rightarrow \sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = k \cdot a_i^{2d-1}$, $(i = 1, 2)$

$\Rightarrow \gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(k a_1^{2d-1}, k a_2^{2d-1})$

& Also, $|k a_i^{2d-1}|$ $\Rightarrow k$

$$\leq \max_{j=1,2} |f_j(a_1, a_2)| \sum_{i=1}^{2} |g_{ij}(a_1, a_2)|$$

$\leq k \cdot H(F(p))$ $\quad$ $\leq \gamma_i \cdot H(p)^{d-1}$.

$\Rightarrow k \cdot |a_i|^{2d-1} \leq k \cdot H(F(p)) \gamma_i H(p)^{d-1}$.

$\Rightarrow H(p)^{2d-1} \leq \max(\gamma_1, \gamma_2) H(F(p)) H(p)^{d-1}$.

$\Rightarrow \dfrac{1}{\max(\gamma_1, \gamma_2)} H(p)^{d} \leq H(F(p))$. ✓

Elliptic Curves: Lecture 19 | 01/03/2024

Notation For $x \in \mathbb{Q}$, say $x = \frac{r}{s}$ & $\gcd(r,s)=1$, write:
$H(x) = H((x:1)) = \max(|r|, |s|)$.

Let: $E/\mathbb{Q}$ elliptic curve, $y^2 = x^3 + ax + b$.

DEF Height $H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$, $P \mapsto \begin{cases} H(x), & P=(x,y) \\ 1, & P = O_E \end{cases}$

& Log Height $h : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$, $P \mapsto \log(H(P))$.

Lemma 13.2 let E, E' ~~isogeny~~ ~~def~~ elliptic curves over $\mathbb{Q}$ & $\Phi : E \to E'$ isogeny (defined over $\mathbb{Q}$).
Then: $\exists C > 0$, s.t. $|h(\Phi(P)) - (\deg \phi)\, h(P)| < C \quad \forall P \in E(\mathbb{Q})$.

[NOTE C depends on Φ but not on P.]

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E' \\ x \downarrow & & \downarrow x \\ \mathbb{P}^1 & \xrightarrow[\xi]{} & \mathbb{P}^1 \end{array}$$

Proof From Lemma 5.4:
have: $\deg(\Phi) = \deg(\xi) \equiv d$.

Lemma 13.1 $\Rightarrow \exists C_1, C_2 > 0$ with:
$C_1 H(P)^d \leq H(\phi(P)) \leq C_2 H(P)^d$. $[\forall P \in E(\mathbb{Q})]$

$\Rightarrow |h(\phi(P)) - d \cdot h(P)| \leq \max(\log(C_2), -\log(C_1)) \equiv C$ ✓

Example $\phi = [2] : E \to E$. $\Rightarrow \exists C > 0$, $|h(2P) - 4h(P)| \leq C$.

DEF Canonical Height $\boxed{\hat{h}(P) \equiv \lim_{n \to \infty} 4^{-n} h(2^n P).}$

Check convergence: for $m \geq n \geq 1$, have:

$$|4^{-m}h(2^m p) - 4^{-n}h(2^n p)| \le \sum_{n\le r<m} |4^{-(r+1)}h(2^{r+1}p) - 4^{-r}h(2^r p)|$$

$$= \sum_{n\le r<m} \frac{1}{4^r}\,|h(2\cdot 2^r p) - 4h(2^r p)| < c\sum_{r\ge n} 4^{-r} = \frac{c}{3\cdot 4^n} \to 0 \checkmark$$

So. Sequence Cauchy $\Rightarrow \hat{h}(p)$ exists ✓

Lemma 13.3 $|h(p) - \hat{h}(p)|$ Bounded for $p \in E(\mathbb{Q})$.

Proof In proof of convergence, set $n = 0$.

Gets: $|4^{-n}h(2^n p) - h(p)| \le c/3$. $\forall n$.

$\Rightarrow$ Take $n \to \infty$ so $|\hat{h}(p) - h(p)| \le c/3$ ✓

Lemma 13.4 $\forall B > 0$, $\#\{P \in E(\mathbb{Q}) : \hat{h}(p) \le B\} < \infty$.

Proof $\hat{h}(p)$ bounded $\Rightarrow h(p)$ bounded (Lemma 13.3)

$\Rightarrow$ Finitely many possibilities for x, hence, for P ✓

Lemma 13.5 $E \xrightarrow{\phi} E'$ over $\mathbb{Q}$ (ϕ defined over $\mathbb{Q}$).

Then: $\hat{h}(\phi(p)) = (\deg \phi)\hat{h}(p)$ $\forall P \in E(\mathbb{Q})$.

Proof By Lemma 13.2: $\exists C > 0$, $|h(\phi p) - (\deg\phi)h(p)| < C$.

Replace $P \mapsto 2^n P$; divide by 4^n & take $n \to \infty$, so

get $|\hat{h}(\phi p) - (\deg\phi)\hat{h}(p)| \le c \cdot 4^{1-n} \to 0$ ✓

Remarks (i) For $\deg(\phi) = 1$, $\hat{h}$ (unlike h) does not depend on exact choice of W-eqn.

(ii) Taking $\phi = [n] : E \to E \Rightarrow \hat{h}(nP) = n^2\hat{h}(P)$.

Lemma 13.6 $E/\mathbb{Q}$ elliptic. Then, $\exists C>0$, with:
$H(P+Q)H(P-Q) \leq C \cdot H(P)^2 H(Q)^2$ $\forall P,Q \in E(\mathbb{Q})$ with $P, Q, P \pm Q \neq O_E$.

Proof Let: E have W-eqn $y^2 = x^3 + ax + b$. $(a, b \in \mathbb{Z})$.
& Let $P, Q, P+Q, P-Q$ have x-coords x_1, x_2, x_3, x_4.
By lemma 5.8: $\exists W_0, W_1, W_2 \in \mathbb{Z}[X_1, X_2]$, with:
W_i has degree ≤ 2 in X_1, X_2 (separately)
& $(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2)$. $W_0 = (X_1 - X_2)^2$
Write: $x_i = \frac{r_i}{s_i}$ for r_i, s_i coprime integers.
$\Rightarrow (s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = ((r_1 s_2 - r_2 s_1)^2 : - : -)$
& $s_3 s_4,\ r_3 s_4 + r_4 s_3,\ r_3 r_4$ coprime.
$\Rightarrow H(P+Q)H(P-Q) = \max(|r_3|, |s_3|) \max(|r_4|, |s_4|)$
$\leq 2 \max(|r_3 r_4|, |r_3 s_4 + r_4 s_3|, |s_3 s_4|)$
$\leq 2 \max(|(r_1 s_2 - r_2 s_1)^2|, -, -)$
$\leq C \cdot H(P)^2 H(Q)^2$ since W_i degree ≤ 2 in X_i.

Theorem 13.7 $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is Quadratic Form.

Proof Use: lemma 13.6 + fact that $|h(2P) - 4h(P)|$ bdd.
$\Rightarrow h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + C$. $\forall P, Q \in E(\mathbb{Q})$
Replacing $P, Q \mapsto (2^n P, 2^n Q)$, divide by 4^n & take $n \to \infty$
gives $\hat{h}(P+Q) + \hat{h}(P-Q) \leq 2(\hat{h}(P) + \hat{h}(Q))$.

Then, replace $(P,Q) \mapsto \left(\frac{P+Q}{2}, \frac{P-Q}{2}\right)$ gives equality ✓

$\Rightarrow h$ is Quadratic Form ✓

Remark What about more general NF's?

For K Number Field: let $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n(K)$.

Define: $H(P) = \prod_v \max_{1 \le i \le n} |a_i|_v$

[Product over all places v of K, and $|\cdot|_v$ normalised, such that Product formula is true.]

$\Rightarrow$ Results from section then generalise to General NF's.

Elliptic Curves: Lecture 20 | 04/03/2024

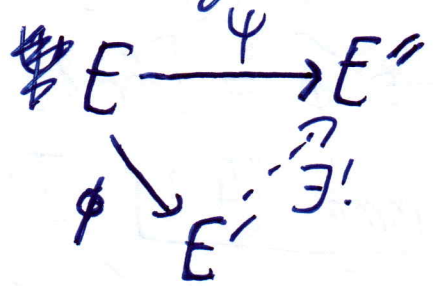
§14: Dual Isogenies & Weil Pairing.

Let: K perfect field & E/K Elliptic.

Prop 14.1 Let $\Phi \subset E(\bar{K})$ be finite $Gal(\bar{K}/K)$-stable subgroup. Then, $\exists E'/K$ elliptic & separable isogeny $\phi: E \to E'$ defined over K, s.t.

$\forall \psi: E \to E''$, $\ker(\psi) \supseteq \Phi$,

$\exists!$ factoring of ψ through ϕ.



Prop 14.2 Let $\phi: E \to E'$ Isogeny degree n. Then, $\exists!$ $\hat{\phi}: E' \to E$, $\hat{\phi}\phi = [n]$. "Dual Isogeny"

Proof If ϕ Separable $\Rightarrow$ $|\ker \phi| = n$.

$\Rightarrow$ By Prop 14.1: with $\psi = [n]$, done ✓

If ϕ inseparable: Omitted !!

Uniqueness: If $\psi_1 \phi = \psi_2 \phi$ then $(\psi_1 - \psi_2)\phi = 0$

$\Rightarrow \deg(\psi_1 - \psi_2)\deg(\phi) = 0$, so $\deg(\psi_1 - \psi_2) = 0$

$\Rightarrow \psi_1 = \psi_2$ ✓

Remarks 1) Write $E_1 \sim E_2 \iff E_1, E_2$ Isogenous.

Then, $\sim$ is Equivalence Relation.

2) $\deg[n] = n^2 \Rightarrow \begin{cases} \deg \hat{\phi} = \deg \phi \\ \widehat{[n]} = [n]. \end{cases}$

iii) $\phi\hat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi \Rightarrow \phi\hat{\phi} = [n]_{E'}$.

In particular, $\hat{\hat{\phi}} = \phi$.

iv) If $E \xrightarrow{\psi} E' \xrightarrow{\psi'} E''$ then $\widehat{\psi'\psi} = \hat{\psi}\hat{\psi'}$.

v) If $\phi \in \mathrm{End}(E)$ then $\phi^2 - [\mathrm{tr}\,\phi]\phi + [\deg\phi] = 0$.

$\Rightarrow \phi([\mathrm{tr}\,\phi] - \phi) = [\deg\phi]$

$\Rightarrow \hat{\phi} = [\mathrm{tr}\,\phi] - \phi$. In particular, $[\mathrm{tr}\,\phi] = \phi + \hat{\phi}$.

Lemma 14.3 If $\phi, \psi \in \mathrm{Hom}(E, E')$ then:

$$\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}.$$

Proof If $E = E'$ then follows from linearity of the trace map (using above formula for $\hat{\phi}$)

In general, let $\alpha: E \to E'$ any isogeny.

Then, $(\alpha\phi): E \to E$ is in $\mathrm{End}(E)$

$$\Rightarrow \widehat{\alpha\phi+\alpha\psi} = \widehat{\alpha\phi} + \widehat{\alpha\psi}.$$

$$\Rightarrow \widehat{\phi+\psi}\hat{\alpha} = (\hat{\phi}+\hat{\psi})\hat{\alpha}.$$ So, cancel $\hat{\alpha}$ ✓

Remark Can prove other way: e.g. show Lemma 14.3 first, and then prove degree map is QF.

DEF $\mathrm{Div}(E) \xrightarrow{\text{sum}} E$

$$\sum n_P \cdot P \mapsto \sum n_P \cdot P.$$

Recall: $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$. (by $P \mapsto [(P) - (O_E)]$)

Deduce:

Lemma 14.4 Let D divisor, in $\mathrm{Div}(E)$. Then,

$D \sim 0 \Leftrightarrow \deg(D) = 0$ & $\mathrm{Sum}(D) = 0_E$

Let $\phi : E \to E'$ Isogeny, of degree n. & $\hat{\phi} : E' \to E$.

Assume: $\mathrm{Char}(K) \nmid n$. $\Rightarrow$ ϕ, $\hat{\phi}$ Separable.

Define: Weyl pairing ~~$e_\phi : E[\phi] \to$~~ $(E[\phi] = \ker \phi)$

$e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n$ by:

$\forall S \in E[\phi]$, $T \in E'[\hat{\phi}]$, then, $nT = 0$, so $\exists f \in \bar{K}(E')^\times$

with $\mathrm{div}(f) = nT - n(0)$.

Pick: $T_0 \in E(\bar{K})$, with $\phi(T_0) = T$.

$$\Rightarrow \phi^*(T) = \phi^*(0) + \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P).$$

This has: $\mathrm{Sum} = nT_0 = \hat{\phi}\phi T_0 = \hat{\phi}(T) = 0$.

$\Rightarrow \exists\, g \in \bar{K}(E)^\times$, $\mathrm{div}(g) = \phi^* T - \phi^* 0$.

So, $\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}\, f) = n(\phi^*(T) - \phi^*(0))$

$= \mathrm{div}(g^n)$.

$\Rightarrow \phi^* f = c \cdot g^n$, for some $c \in \bar{K}^*$.

So, rescale our choice of f $\Rightarrow$ Get $c = 1$, so $\phi^* f = g^n$.

Now, $S \in E[\phi]$. $\Rightarrow \tau_S^*(\mathrm{div}\, g) = \mathrm{div}(g)$.

$\Rightarrow \mathrm{div}(\tau_S^* g) = \mathrm{div}(g)$. So, $\exists\, \xi \in \bar{K}^*$, $\tau_S^* g = \xi g$.

$\Rightarrow \xi = \dfrac{g(X+S)}{g(X)}$. Indep of choice of $X \in E(\bar{K})$

Check: $\xi^n = \dfrac{g(X+S)^n}{g(X)^n} = \dfrac{(f\circ\phi)(X+S)}{(f\circ\phi)(X)} = 1$ (since: $S \in E[\phi]$)

Define: $(S,T) \xmapsto{e_\phi} \xi$ as the Weil Pairing.

Prop 14.5] e_ϕ Bilinear & Non-degenerate.

Proof ⊛ First Argument: $e_\phi(S_1+S_2, T)$

$= \dfrac{g(X+S_1+S_2)}{g(X+S_2)} \dfrac{g(X+S_2)}{g(X)} = e_\phi(S_1,T)\, e_\phi(S_2,T)$.

⊛ ~~First~~ Second Argument: Let $T_1, T_2 \in E'[\hat{\phi}]$.

$\Rightarrow div(f_1) = n(T_1) - n(0)$ & $div(f_2) = n(T_2) - n(0)$.

and: $\phi^* f_1 = g_1^n$, $\phi^* f_2 = g_2^n$.

Know: $\exists\, h \in \bar{K}(E')^*$, with: $div(h) = (T_1) + (T_2) - (T_1+T_2) - (0)$.

So, put $f = \dfrac{h_1 h_2}{h^n}$ and $g = \dfrac{g_1 g_2}{\phi^* h}$.

Check: $div(f) = n(T_1+T_2) - n(0)$

& $\phi^* f = \dfrac{(\phi^* f_1)(\phi^* f_2)}{(\phi^* h)^n} = \left(\dfrac{g_1 g_2}{\phi^* h}\right)^n = g^n$

$\Rightarrow e_\phi(S, T_1+T_2) = \dfrac{g(X+S)}{g(X)} = \dfrac{g_1(X+S)}{g_1(X)} \dfrac{g_2(X+S)}{g_2(X)} \dfrac{h(\phi(X))}{h(\phi(X+S))}$

$= e_\phi(S,T_1)\, e_\phi(S,T_2)$ ✓

Non-degeneracy: If $e_\phi(S,T) = 1$ $(\forall S)$ $(T$ fixed$)$ then $\tau_S^* g = g$ $\forall S \in E[\phi]$. ∎

Elliptic Curves: Lecture 21 | 06/03/2024

Proof of Prop 14.5 [Continued]

Showing: Non-degeneracy of e_ϕ.

Had: If $e_\phi(S,T)=1$ $\forall S$ (T fixed) $\Rightarrow \tau_S^* g = g$ $\forall S$.

$\exists$ Galois ext $\bar{K}(E) \supseteq \phi^* \bar{K}(E')$ of Galois group $E[\phi]$.

$\bar{K}(E)$ | $\phi^*\bar{K}(E')$

So, $\forall S \in E[\phi]$, $\tau_S^* g = g$

$\Rightarrow g = \phi^* h$, some $h \in \bar{K}(E')$ [Galois]

$\Rightarrow \phi^* f = g^n = (\phi^* h)^n = \phi^*(h^n)$, so: $f = h^n$

$\Rightarrow \operatorname{div}(h) = (T) - (0)$, hence $T = 0$ ✓

So, showed: $E'[\hat{\phi}] \hookrightarrow \operatorname{Hom}(E[\phi], \mu_n)$ is Isomorphism because $\#E[\phi] = \#E[\hat{\phi}] = n$ ✓

Remarks 1) If E, E', ϕ defined over K, then e_ϕ is Galois-invariant, i.e. $e_\phi(\sigma(S), \sigma(T)) = \sigma(e_\phi(S,T))$ for any $\sigma \in \operatorname{Gal}(\bar{K}/K)$, $S \in E[\phi]$, $T \in E[\hat{\phi}]$.

2) Take $\phi = [n] : E \to E$ $(\hat{\phi} = \phi = [n])$

$\Rightarrow e_n : E[n] \times E[n] \to \mu_n$. [Better than μ_{n^2}]

Corollary 14.6 If $E[n] \subset E(K)$ then $\mu_n \subset K$.

Proof $T \in E[n]$ has order n.

By non-degeneracy of e_ϕ: $\exists S \in E[n]$ with $e_n(S,T) = \zeta_n$. ∎

$\Rightarrow \sigma(\xi_n) = \sigma(e_n(S,T)) = e_n(\sigma(S),\sigma(T)) = \xi_n$.

$\Rightarrow \xi_n \in k \;\forall \xi_n \in \mu_n$, so $\mu_n \subset k$.

Example $\exists E/\mathbb{Q}$, with $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Remark In fact, e_n *Alternating*: $e_n(T,T)=1 \;\forall T \in E[n]$.

(This implies $e_n(S,T) = e_n(T,S)^{-1}$.)

---

§15: Galois Cohomology

Let: G group, A G-module ($\mathbb{Z}G$-module).

DEF $H^0(G,A) \equiv A^G = \{a \in A : \sigma(a) = a \;\forall \sigma \in G\}$.

& $C^1(G,A) = \{\text{Maps } G \to A\}$

$\cup$

$Z^1(G,A) = \{(a_\sigma)_{\sigma\in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\}$

$\cup$

$B^1(G,A) \equiv \{(\sigma b - b)_{\sigma\in G} : b \in A\}$.

& $H^1(G,A) \equiv \dfrac{Z^1(G,A)}{B^1(G,A)}$ Cohomology group.

Remark If G acts trivially on A, then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Theorem 15.1 SES of G-modules $0 \to A \xrightarrow{\Phi} B \xrightarrow{\Psi} C \to 0$ gives LES

$$0 \to A^G \xrightarrow{\Phi} B^G \xrightarrow{\Psi} C^G \to H^1(G,A) \xrightarrow{\Phi_*} H^1(G,B) \xrightarrow{\Psi_*} H^1(G,C).$$

(no proof)

F2

DEF of δ For $c \in C^G$: $\exists b \in B$, $\psi(b) = c$.

$\Rightarrow \psi(\sigma b - b) = \sigma\psi(b) - \psi(b) = \sigma c - c = 0$

$\Rightarrow \exists a_\sigma \in A$, $\sigma b - b = \phi(a_\sigma)$.

So, define $\delta(c) = [(a_\sigma)_{\sigma \in G}] \in H^1(G, A)$.

Theorem 15.2 A is G-module, $H \trianglelefteq G$ Normal.

Then $\exists$ "Inflation-Restriction" Exact Sequence:

$$0 \longrightarrow H^1\left(\frac{G}{H}, A^H\right) \xrightarrow{\inf} H^1(G, A) \xrightarrow{res} H^1(H, A).$$ [no proof]

Let: K Perfect field. Then, $Gal(\bar{K}/K)$ is Topological group, with Basis of open subgroups $Gal(\bar{K}/L)$, $[L:K] < \infty$.

If $G = Gal(\bar{K}/K)$, modify def. of $H^1(G, A)$ by insisting:

1) $Stab_G(a)$ Open subgroup of G, $\forall a \in A$

2) All cochains $G \to A$ are Continuous (A discrete top.)

Then: $H^1(Gal(\bar{K}/K), A) = \varinjlim_{L/K \text{ Finite Galois}} H^1(Gal(L/K), A^{Gal(\bar{K}/L)})$.

Direct limit (WRT inflation map).

Hilbert Theorem 90 Let: L/K Finite Galois ext.

Then: $H^1(Gal(L/K), L^*) = 0$.

Proof] Denote: $G = Gal(L/K)$ & let $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^*)$.

Know (Part II Galois Theory): Distinct Automorphisms are linearly Independent.

$\Rightarrow \exists y \in L$, s.t. $x \equiv \sum_{\tau \in G} a_\tau^{-1}\, \tau(y) \neq 0$.

$\Rightarrow \sigma(x) = \sum_{\tau \in G} \sigma(a_\tau^{-1})\, \sigma\tau(y) = a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1}\, \sigma\tau(y) = a_\sigma x$.

$\Rightarrow a_\sigma = \frac{\sigma(x)}{x}$, so $(a_\sigma)_{\sigma \in G} \in B^1(G, L^*)$.

Hence, $H^1(G, L^*) = 0$ ✓

Corollary $H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) = 0$.

Application Assume $\mathrm{char}(K) \nmid n$. $\Rightarrow \exists$ SES of $\mathrm{Gal}(\bar{K}/K)$-modules:

$$0 \to \mu_n \to \bar{K}^* \xrightarrow[x \mapsto x^n]{} \bar{K}^* \to 0$$

$\Rightarrow$ LES

$$K^* \xrightarrow[x \mapsto x^n]{} K^* \to H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \to H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^*)$$

$$\Rightarrow H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong \frac{(K^*)}{(K^*)^n}.$$

& If $\mu_n \subset K$ then $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong \frac{K^*}{(K^*)^n}$

where finite subgroups of LHS are of form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ for L/K finite Galois ext, of exponent $|n$.

$\Rightarrow$ Gives: Another proof of Theorem 11.2.

Elliptic Curves: Lecture 22 | 08/03/2024

From last time Galois Cohomology.

Notation: $H^1(K,-) \equiv H^1(Gal(\bar{K}/K),-)$.

Let: $\phi: E \to E'$ Isogeny of Elliptic curves over K.

$\Rightarrow \exists$ SES of $Gal(\bar{K}/K)$-modules:

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0.$$

$\Rightarrow \exists$ LES (not necessarily $Gal(\bar{K}/K)$ modules):

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K,E) \xrightarrow{\phi_*} H^1(K,E')$$

$\Rightarrow \exists$ SES:

$$0 \to \frac{E'(K)}{\phi E^{\#}(K)} \xrightarrow{\delta} H^1(K,E[\phi]) \to H^1(K,E)[\phi_*] \to 0$$

So:

$$0 \to \prod_v \frac{E'(K_v)}{\phi E(K_v)} \xrightarrow{\delta_v} \prod_v H^1(K_v, E[\phi]) \to \prod_v H^1(K_v,E)[\phi_*] \to 0$$

Next: Take K NF. $\Rightarrow \forall v$ place of K, fix an embedding $\bar{K} \subset \bar{K}_v$. $\Rightarrow Gal(\bar{K}_v/\bar{K}_v) \subset Gal(\bar{K}/K)$.

DEF] The ϕ-Selmer group $S^{(\phi)}(E/K) = \ker(f)$

$$= \ker\left(H^1(K,E[\phi]) \xrightarrow{f} \prod_v H^1(K_v,E)\right)$$

$$= \{\alpha \in H^1(K,E[\phi]) : res_v(\alpha) \in Im(\delta_v) \ \forall v\}.$$

The Tate-Shafarevich Group is:

$$Ш(E/K) = \ker\left(H^1(K,E) \longrightarrow \prod_v H^1(K_v, E)\right).$$

Let: SES $0 \to \dfrac{E'(K)}{\phi E(K)} \longrightarrow S^{(\phi)}(E/K) \to Ш(E/K)[\phi_*] \to 0$

For $\phi = [n]$, gives:

$$0 \to \frac{E(K)}{nE(K)} \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Re-arranging proof of Mordell-Weil gives:

Theorem 15.3 $S^{(n)}(E/K)$ Finite.

Proof For L/K Finite Galois ext, $\exists$ Exact sequence:

$$0 \to \underbrace{H^1(\mathrm{Gal}(L/K), E(L)[n])}_{\text{Finite.}} \xrightarrow{\inf} H^1(K, E[n]) \xrightarrow{\text{res}} H^1(L, E[n])$$

$$\text{UI} \qquad\qquad \text{UI}$$

$$S^{(n)}(E/K) \qquad S^{n}(E/L)$$

$\Rightarrow$ By extending field, can Assume $E[n] \subset E(K)$, and so $\mu_n \subset K$.

$\Rightarrow E[n] \cong \mu_n \times \mu_n$ (as $\mathrm{Gal}(\bar{K}/K)$-module)

$\Rightarrow H^1(K, E[n]) \cong H^1(K, \mu_n) \times H^1(K, \mu_n)$

$$\cong K^*/(K^*)^n \times K^*/(K^*)^n$$

Let: $S = \{\text{Primes of Bad reduction of } E\} \cup \{v \mid n\infty\}$.

(Finite Set of places of K)

DEF $H^1(K,A;S) \subset H^1(K,A)$ is a subgroup unramified outside S and is defined by:

$$H^1(K,A;S) = \ker\left[H^1(K,A) \to \prod_{v\notin S} H^1(K_v^{nr}, A)\right]$$

Proof Continued $\exists$ Commutative Diagram:

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\times n} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) \\ \cap| & & \cap| & & \downarrow \text{res} \\ E(K_v^{nr}) & \xrightarrow[\uparrow]{\times n} & E(K_v^{nr}) & \xrightarrow[\uparrow]{} & H^1(K_v^{nr}, E[n]) \\ (\forall v\notin S:)\ \text{Surj (Thm 9.8)} & & & & =0 \end{array}$$

$\Rightarrow S^{(n)}(E/K) \subseteq H^1(K, E[n], S)$

(Because: $\forall v\notin S$, $\text{Res}_v(\alpha) \in \text{Im}(\delta_v)$.)

$\Rightarrow S^n(E/K) \subseteq H^1(K,E[n];S) \cong \left[H^1(K,\mu_n,S)\right]^2$.

$\&\ \cong H^1(K,\mu_n;S) \cong \ker\left(\frac{K^*}{(K^*)^n} \to \prod_{v\notin S} \frac{(K_v^{nr})^*}{(K_v^{nr})^{*n}}\right) \subseteq K(S,n)$

(in fact, last $\subseteq$ is equality!)

and this is finite (since Lemma 11.4). ✓

Remark $S^{(n)}(E/K)$ Finite & Effectively Computable. It is Conjectured, that $|Ш(E/K)| < \infty$. This would imply that Rank(E/K) is Effectively computable.

---

§16: Descent, via Cyclic Isogeny.

Let: $E, E'/K$ elliptic (K NF) & $\phi: E \to E'$ isogeny (defined over K) & Suppose $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ and

is generated by $T \in E'(K)$.

Then: $\mu_n \cong E[\phi]$ as $Gal(\bar{K}/K)$-module.

$\ell_\phi(S,T) \longleftrightarrow S$

$\Rightarrow$ SES of $Gal(\bar{K}/K)$-modules: $0 \to \mu_n \to E \xrightarrow{\phi} E' \to 0$

& LES: $E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \to H^1(K, E) \to \cdots$

α ↘ ↓ IS (Hilbert 90)

$(K^*)/(K^*)^n$

Theorem 16.1 Let $f \in K(E')$ & $g \in K(E)$ s.t. $div(f) = n(T) - n(0)$ & $\phi^* f = g^n$.

Then: ~~$\alpha(P) = f(P)$ mod $(K^*)^n$~~ $\alpha(P) = f(P) \bmod (K^*)^n$ $\forall P \in E'(K)$ except $0, T$ (where f has poles/zeros).

Proof Let $Q \in \phi^{-1}(P)$. $\Rightarrow \delta(P) \in H^1(K, \mu_n)$ is represented by cocycle $\sigma \mapsto \sigma(Q) - Q \in \ker(\phi) \cong \mu_n$. $E[\phi]$

$\Rightarrow \ell_\phi(\sigma Q - Q, T) = \dfrac{g(X + \sigma Q - Q)}{g(X)}$

Pick $X = Q$: $= \dfrac{g(\sigma Q)}{g(Q)} = \dfrac{\sigma(g(Q))}{g(Q)}$.

$= \dfrac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}$, since $\phi^* f = g^n \Rightarrow g(Q)^n = f(\phi(Q)) = f(P)$.

But: $H^1(K, \mu_n) \cong K^*/(K^*)^n$ $\longleftrightarrow x$ $(\sigma \mapsto \dfrac{\sigma\sqrt[n]{x}}{\sqrt[n]{x}})$

$\Rightarrow \alpha(P) = f(P) \bmod (K^*)^n$ (unless taking $X = Q$ illegal $\Leftrightarrow P = 0, T$.)

Elliptic Curves: Lecture 23 | 11/03/2024

Descent by 2-isogeny.

Let: $E: y^2 = x(x^2+ax+b)$

$E': y^2 = x(x^2+a'x+b')$. $[a' = -2a,\ b' = a^2-4b]$

$\phi: E \to E',\ (x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2}\right)$

$\hat{\phi}: E' \to E,\ (x,y) \mapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{y(x^2-b')}{8x^2}\right)$

Then: $E[\phi] = \{0, T\}$, $T = (0,0) \in E(K)$

& $E'[\hat{\phi}] = \{0, T\}$, $T = (0,0) \in E'(K)$.

Prop 16.2] $\exists$ Group hom $\alpha_{E'}: E'(K) \to K^*/(K^*)^2$

sending $(x,y) \mapsto \begin{cases} x \bmod (K^*)^2 & \text{if } x \neq 0 \\ b' \bmod (K^*)^2 & \text{if } x = 0. \end{cases}$

& $\ker(\alpha_E) = \phi E(K)$.

Proof] Either: Apply Theorem 16.1 with $f = x \in K(E')$ & $g = y/x \in K(E)$.

Or: Direct computation [Sheet 4].

Hence: $\alpha_E: \dfrac{E(K)}{\hat{\phi}E'(K)} \hookrightarrow K^*/(K^*)^2$

& $\alpha_{E'}: \dfrac{E'(K)}{\phi E(K)} \hookrightarrow K^*/(K^*)^2$

Lemma 16.3] $2^{\text{Rank}(E/K)} = \dfrac{|\text{Im}(\alpha_E)| \cdot |\text{Im}(\alpha_{E'})|}{4}$

Proof] If $A \xrightarrow{f} B \xrightarrow{g} C$ homs of Abelian groups:

$$0 \to \ker(f) \to \ker(gf) \xrightarrow{f} \ker(g)$$

$$\hookrightarrow \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0$$

So, since $\hat{\phi}\phi = [2]_E$: get exact sequence:

($\hat{\phi}\phi = [2]_E$: $= \mathbb{Z}/2\mathbb{Z}$; $= \mathbb{Z}/2\mathbb{Z}$)

$$0 \to E(K)[\phi] \to E(K)[2] \to E'(K)[\hat{\phi}]$$

$$\hookrightarrow \frac{E'(K)}{\phi E(K)} \to \frac{E(K)}{2E(K)} \to \frac{E(K)}{\hat{\phi}E'(K)} \to 0$$

$\frac{E'(K)}{\phi E(K)} = \operatorname{Im}(\alpha_E)$

$\frac{E(K)}{\hat{\phi}E'(K)} = \operatorname{Im}(\alpha_{E'})$

$$\Rightarrow \frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{Im}(\alpha_E)| \cdot |\operatorname{Im}(\alpha_{E'})|}{4} \quad (\#).$$

By Mordell-Weil: $\exists \Delta$ finite group, $E(K) \cong \Delta \times \mathbb{Z}^r$.

$$\Rightarrow \frac{E(K)}{2E(K)} \cong \frac{\Delta}{2\Delta} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \Rightarrow \frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r$$

& $E(K)[2] \cong \Delta[2]$ — So combine with $(\#)$ ✓

Lemma 16.4] K Number Field. & $a, b \in \mathcal{O}_K$. E elliptic.

Then: $\operatorname{Im}(\alpha_E) \subset S(K,2)$, where $S = \{\text{Primes dividing } b\}$.

Proof] Need: If $x, y \in K$, $y^2 = x^3 + ax + b$ & $v_{\mathfrak{p}}(b) \neq 0$ then $v_{\mathfrak{p}}(x)$ even.

$\square$ 2

Case $v_p(x) < 0 \Rightarrow$ by Lemma 9.1: $\begin{cases} v_p(x) = -2r \\ v_p(y) = -3r. \end{cases}$ ✓

Case $v_p(x) > 0 \Rightarrow v_p(x^2 + ax + b) = 0$.

$\Rightarrow v_p(x) = v_p(y^2) = 2v_p(y)$ ✓

Lemma 16.5 If $b_1 b_2 = b$ then: $b_1 (K^*)^2 \in \mathrm{Im}(\alpha_E)$

$\Leftrightarrow$ $\boxed{w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4}$

is soluble for $u, v, w \in K$ not all 0.

Proof If $b_1 \in (K^*)^2$ or $b_2 \in (K^*)^2$, then both satisfied.

So, assume $b_1, b_2 \notin (K^*)^2$.

$b_1 (K^*)^2 \in \mathrm{Im}(\alpha_E) \Leftrightarrow \exists (x, y) \in E(K)$, $x = b_1 t^2$ some $t \in K^*$.

$\Leftrightarrow y^2 = b_1 t^2 \left((b_1 t^2)^2 + a b_1 t^2 + b \right)$.

$\Leftrightarrow \left(\frac{y}{b_1 t} \right)^2 = b_1 t^4 + a t^2 + \frac{b}{b_1}$.

$\Rightarrow (u, v, w)$ has solution $\left(t, 1, \frac{y}{b_1 t} \right)$.

Conversely: if (u, v, w) solution, then $uv \neq 0$.

& $\left(b_1 \left(\frac{u}{v} \right)^2, b_1 \left(\frac{uw}{v^3} \right) \right) \in E(K)$ satisfy. ✓

Take: $K = \mathbb{Q}$.

Example 1) $E = \{ y^2 = x^3 - x \}$: $a = 0$, $b = -1$.

$\Rightarrow \mathrm{Im}(\alpha_E) = \langle -1 \rangle \subset \mathbb{Q}^* / (\mathbb{Q}^*)^2$.

& $E' : y^2 = x^3 + 4x$. $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^* / (\mathbb{Q}^*)^2$

Since $\mathrm{Im}(\alpha_E) \subset K(S,2)$: get $b \in \{-1, 2, -2\}$.

$b=-1$ $\quad w^2 = -u^4 - 4v^4$ $\quad$ No sols $/\mathbb{R}$

$b=2$ $\quad w^2 = 2u^4 + 2v^4$ $\quad (u,v,w) = (1,1,2)$

$b=-2$ $\quad w^2 = -4u^4 - v^4$. $\quad$ No sols $/\mathbb{R}$

$\Rightarrow$ Only $b=2$ works. So, $\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

$\Rightarrow \frac{2}{2}\mathrm{Rank}\, E(\mathbb{Q}) = \frac{2 \cdot 2}{4} = 1$ hence $\mathrm{Rank}\,(E(\mathbb{Q})) = 0$.

2) $E: y^2 = x^3 + px$, p prime & $p \equiv 5 \bmod 8$.

Then, for $b_1 = -1$: $w^2 = -u^4 - pv^4$ no sols $/\mathbb{R}$.

$\Rightarrow \mathrm{Im}(\alpha_E) = \langle p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

& $E': y^2 = x^3 - 4px$. $\Rightarrow \mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle$.

Also know $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^*)^2 = (-p)(\mathbb{Q}^*)^2$.

& Know $-p$ already in image.

$b_1 = 2$ $\quad w^2 = 2u^4 - 2pv^4$ $\quad (1)$

$b_1 = -2$ $\quad w^2 = -2u^4 + 2pv^4$ $\quad (2)$

$b_1 = p$ $\quad w^2 = pu^4 - 4v^4$. $\quad (3)$

(1): Assume $u, v, w \in \mathbb{Z}$ & $\gcd(u,v) = 1$. Then, easy to see: $p \nmid u$. $\Rightarrow 2$ square mod p $\lightning$. No sols.

(2): Similarly no sols, since -2 not square mod p.

$\Rightarrow \mathrm{Im}(\alpha'_{E'}) \subset \langle -1, p \rangle$, so $\mathrm{Rank}\, E(\mathbb{Q}) = \begin{cases} 1 \text{ if } (3) \text{ solvable} \\ 0 \text{ else.} \end{cases}$

Elliptic Curves: Lecture 24 | 13/03/2024

Let: $E: y^2 = x(x^2+ax+b)$ & $\phi: E \to E'$ isogeny.

Had: $w^2 = b_1 u^4 + au^2v^2 + b_2 v^4$ $(b_2 = b/b_1)$. (†)

& $0 \to \frac{E(\mathbb{Q})}{\hat{\phi}E'(\mathbb{Q})} \to S^{(\hat{\phi})}(E'/\mathbb{Q}) \to Ш(E'/\mathbb{Q})[\hat{\phi}_*] \to 0.$

$\cap|$

$\alpha_E \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$

Had: $\mathrm{im}(\alpha_E) = \{b_1(\mathbb{Q}^*)^2 : (†) \text{ solvable } /\mathbb{Q}\}$.

$\cap|$

$S^{(\hat{\phi})}(E'/\mathbb{Q}) = \{b_1(\mathbb{Q}^*)^2 : (†) \text{ solvable over } \mathbb{R} \text{ & all } \mathbb{Q}_p\}$.

FACT [Sheet 3 Q9 + Hensel]:

If $a, b, b_1 \in \mathbb{Z}$ & $p \nmid 2b(a^2-4b)$ then (†) solvable $/\mathbb{Q}_p$.

Example 2 [Continued]. $y^2 = x^3 + px$, p prime $\equiv 5 \ (8)$.

$\Rightarrow$ (†): $w^2 = pu^4 - 4v^4$. (3)

& $\mathrm{Rank}(E(\mathbb{Q})) = 1$ if (3) no sol $/\mathbb{Q}$, and 0 else.

Know: (3) solvable $/\mathbb{Q}_2$, since $p-4 \equiv 1 \bmod 8 \Rightarrow \in (\mathbb{Z}_2^*)^2$

(3) solvable $/\mathbb{Q}_p$ since: $\left(\frac{-1}{p}\right) = +1 \Rightarrow -1 \in (\mathbb{Z}_2^*)^2$

(3) solvable $/\mathbb{R}$, since $\sqrt{p} \in \mathbb{R}$.

Conjecture: $\mathrm{Rank}\, E(\mathbb{Q}) = 1$ $\forall p \equiv 5 \bmod 8$.

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
37	5	3	151
53	1	1	7

Example 3) [Lind]. $E: y^2 = x^3 + 17x$.

Compute: $\mathrm{Im}(\alpha_E) = \langle 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

& $E': y^2 = x^3 - 68x \Rightarrow \mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

for $b_1 = 2$: $w^2 = 2u^4 - 34v^4$.

Replace $w \mapsto 2w$: $\boxed{2w^2 = u^4 - 17v^4.}$

Notation] $C(K) = \{(u,v,w) \in K^3 - \{0\} \text{ satisfying } \}/\sim$

Where: $(u,v,w) \sim (\lambda u, \lambda v, \lambda^2 w)$. "weighted $\mathbb{P}$".

Notice: $C(\mathbb{Q}_2) \neq \emptyset$ since $17 \in (\mathbb{Q}_2^*)^4$

$C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Z}_{17}^*)^2$

$C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$.

$\Rightarrow C(\mathbb{Q}_v) \neq \emptyset \ \forall v$ place.

However: No solutions over $\mathbb{Q}$!! Not soluble.

Indeed: Suppose $(u,v,w) \in C(\mathbb{Q})$ & assume $u,v,w \in \mathbb{Z}$

by rescaling, with $\gcd(u,v) = 1$. $w > 0$.

If $17 \mid w$ then $17 \mid v \Rightarrow 17 \mid u$ ⚡.

$\Rightarrow \forall p \mid w$: $p \neq 17$ & 17 is a square mod p. $\left(\frac{17}{p}\right) = 1$.

$\Rightarrow \left(\frac{17}{p}\right) = \left(\frac{p}{17}\right)$ $\forall p$ odd. [But: note 2 is QR mod 17]

Hence: $\left(\frac{w}{17}\right) = 1$, i.e. w is square mod 17.

Mod 17: $2w^2 \equiv v^4 \bmod 17$. $\Rightarrow 2$ is 4'th power mod 17 ⚡

$\in \{\pm 1, \pm 4\}$.

We say C is Counterexample to the Hasse Principle.
$\Rightarrow$ Represents Nontrivial element of $Ш(E/\mathbb{Q})$.

Birch & Swinnerton-Dyer Conjecture.

DEF $L(E,s) \equiv \prod_p L_p(E,s)$, where:

* If p good reduction $\Rightarrow L_p(E,s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$
* If p Bad reduction $\Rightarrow$

$$L_p(E,s) = \begin{cases} (1-p^{-s})^{-1} & \text{if split Multiplicative reduction} \\ (1+p^{-s})^{-1} & \text{if non-split Mult reduct} \\ 1 & \text{if Additive Red.} \end{cases}$$

By Hasse's Theorem: $|a_p| \leq 2\sqrt{p}$.
$\Rightarrow L(E,s)$ Converges for $Re(s) > 3/2$.

Theorem [Modularity Theorem: Wiles, ...]
$L(E,s)$ is L-func. of some weight-2 Modular form (of some level).
$\Rightarrow$ Hence, Analytic continuation exists to ALL of $\mathbb{C}$.
There is also a FE, $L(E,s) \longrightarrow L(E, 2-s)$.

Weak BSD: $Ord_{s=1}(L(E,s)) = Rank[E(\mathbb{Q})] \equiv r$.

Strong BSD: $$\lim_{s \to 1} (s-1)^{-r} L(E,s) = \frac{\Omega_E \, Reg\, E(\mathbb{Q}) \, |Ш(E/\mathbb{Q})| \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}$$

Where: $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ Tamagawa number of $E/\mathbb{Q}_p$
$Reg(E/\mathbb{Q}) = \det([P_i, P_j])_{1 \leq i,j \leq r}$ where $\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{tors}} = \langle P_1, \ldots, P_r \rangle$

and where $[P_i, P_j] = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)$.

$\Omega_E = \int_{E(\mathbb{R})} \left| \frac{dx}{2y + a_1 x + a_3} \right|$ For a_i Coeffs of a Globally minimum W-eqn.

Theorem [Kolyvagin]

If $\operatorname{ord}_{s=1} L(E,s) = 0$ or 1, then weak BSD holds & $|Ш(E/\mathbb{Q})|$ is finite.