by the order of poles $\Rightarrow \alpha_6 \neq 0$, $\alpha_7 \neq 0$.

Divide $\alpha_7 \Rightarrow \alpha_7 = 1$.

Multiplying by α_6^2, change $\bar{x} = \alpha_6 x$,
and assume $\alpha_6 = \alpha_7 = 1$.

(functions defined all point except a pole at p).

* we have a map

$$X \setminus \{p\} \longrightarrow \mathbb{A}^2$$

$$Q \longmapsto (x(Q), y(Q))$$

the image of this map lies in the plane curve.

$$\alpha_1 + \alpha_2 x + \alpha_3 y + \alpha_4 x^2 + \alpha_5 xy + x^3 + y^2 = 0.$$

need to prove: The map extends to the whole of X.
($p \longrightarrow (0:1:0) \in \mathbb{P}^2$) and is an isomorphism

E.X. Assume $p \in X$ is such that $\deg(p) = 2$
what kind of equation can you expect?

Rk. In W.E. $a_i x^j y^k$,
set $w(x) = 2$ → order of pole of x
$w(y) = 3$ → order of pole of y
and if $w(x)j + w(y)k = 6$
$a_3 y \sim 3+3 = 6$
$a_2 x^2 \sim 2 + 2\cdot 2 = 6$

Given finitely generated k-algebra $k[a_1, \dots, a_n]$

we have surjective map:

$\varphi : k[x_1, \dots, x_n] \longrightarrow k[a_1, \dots, a_n]$

the kernel of φ is an Ideal I

$k(V(I)) = k[a_1, \dots, a_n]$.

Tue. 11th / Sept / 18

$F(x,y,z) \in R[x,y,z]$ homog of deg d, plane projective curve over R.

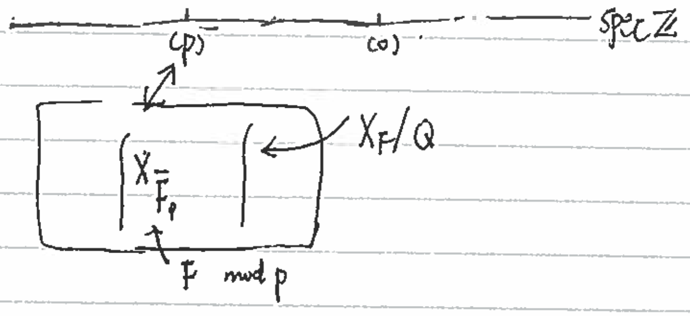
R (Ring / domain, Let K be a field of fractions.)
First approximation, a curve over R can be thought a family of curves over field, parametrized by the prime ideal of R

Let $M \subseteq R$ be a prime ideal $R \to R/M \hookrightarrow ff(R/M) =: k(M)$
$F(x,y,z) \rightsquigarrow \bar{F}_M(x,y,z) =: F \bmod M$.
$F \rightsquigarrow \{ X_{\bar{F}_M}$ plane curve* over $k(M)$ defined by $\bar{F}_M)$

(*) when $\bar{F}_M \neq 0$).

E.g. ① $R = \mathbb{Z}$, (arithmetic case)
② $R = k[t]$ (PID) k field. geometrical case.

* $F \in \mathbb{Z}[x,y,z] \to$ dehom $f(x,y) \in \mathbb{Z}[x,y]$.



* All the "curves" of the family lie in a surface.
$S = \mathrm{Spec}(\mathbb{Z}[x,y]/(f(x,y)))$

To the ② (E.g.) Take $k = \bar{k}$, prime ideal in $\bar{k}[t]$: $(t-a)$ $a \in k$ and 0 (generic p)
Let $M = (t-a)$ Consider $f(x,y) \bmod M$; $f(x,y) \in k[t][x,y]$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| $
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad f(t,x,y) \in k[t,x,y]$

$f(x,y) \bmod M$ in $k[t][x,y]/M$.
can be identified with $f(a,x,y) \in k[x,y]$ ("$t=a$").
$f(t,x,y)=0$ is a surface in $\mathbb{A}^3$, we project it to the t-lines and the fiber over $a \in k$ is the curve $f(a,x,y)=0$ $\longrightarrow$ defined by $f(t,x,y) \in k[t][x,y]$

If $M=(t-a) \Rightarrow R/M$ is evaluate at $t=a$.

* Given E/k of genus 1 "nice curve", for a chosen point $P\in E(k)$, we sketch why it can be given by W.E. and the given point $p=(0:1:0)$.

* We defined $b_2, b_4, b_6 \in \mathbb{Z}[a_1,\dots,a_6]$, $C_4, C_6 \in \mathbb{Z}[a_1,\dots,a_6]$, $\Delta \in \mathbb{Z}[a_1,\dots,a_6]$.

* The W.E. define non-singular curve $\Leftrightarrow \Delta\neq 0$.

* Given $a_1,\dots,a_6 \in R$, we say that W.E./R $y^2+a_1xy+a_3y=a_0x^3+a_2x^2+a_4x+a_6$ define an elliptic curve in R if all the curves in the associated family are elliptic curve.

* Recall: $\forall M\in \mathrm{Spec}R$: The W.E./R defines module M an W.E. over f.f.(R/M) $\Rightarrow$ (fraction field)

This W.E./ff(R/M) define an Elliptic curve $\Leftrightarrow$

$\Delta(W.E./R)$ mod M $=\Delta$ (reduced equation) is not 0 in R/M.

*[For $\forall M$, if $a\notin M \Rightarrow a$ unit]

* Δ mod $M\neq 0$ in $R/M \Leftrightarrow \Delta\notin M$, since this hold for all $M\in \mathrm{Spec}R$,

WE/R defines an elliptic curve over $R \Leftrightarrow \Delta\in R^* \longrightarrow$ (unit in R).

(Surprised) • There are no W.E. over $\mathbb{Z}$ with $\Delta=\pm 1$

• If char(k)=0, there are not W.E./k[t] with $\Delta\in k^*$ "except for trivial case".

(trivial, take coeffs in k).

* Given a W.E/R with $\Delta\in R$, we obtain an elliptic curve over $R[\frac{1}{\Delta}]$ (in the ring, Δ is a unit)

On $\mathbb{A}^1$, $k[t]$ are everywhere defined fcns. $\subseteq k(t)$.

on $\mathbb{A}^1\setminus\{a\}$. $k[t][\frac{1}{t-a}]$, defined ($\frac{1}{t-a}$ is defined everywhere on $\mathbb{A}^1\setminus\{a\}$)

Ex*: W.E./$\mathbb{Z}$, test that $\Delta\neq\pm1$. (prime number can divide Δ)*.

* Suppose $(E/k, p)$ gives us a Weistrass equation.

$(E/k,\ p) \xrightarrow{\ \sim\ } (WE,\ \infty)$

$\downarrow \qquad\qquad y^2+\dots=x^3+\dots$

$(WE',\ \infty)$

$y'^2+0\dots=x'^3+0$

* We find x, y as follows, $H^0(E, 2p)=\langle 1, x\rangle$

* $H^0(E,3p)=\langle 1, x, y\rangle$

adjust x and y, to get $y^2+0=x^3+0'$

We have x', y' the same way, $H^0(E,2p)=\langle 1, x'\rangle$

$H^0(E,3p)=\langle 1, x', y'\rangle$ with $y'^2+0=x'^3+0'$

We must have $x'=\alpha x+r$, $\alpha\neq 0$, $\alpha, \gamma\in k$. $y'=\mu y+sx+t$ $\mu, s, t\in k$. $\mu\neq$

$x' = \lambda^2 x + r$, $y' = \lambda^3 y + sx + t$ $\quad \lambda \in k^*$, $r, s, t \in k$.

$\uparrow (\frac{s}{\lambda^2})\lambda^2$.

R.k. Changing $x' = \lambda^2 x$, $y' = \lambda^3 y$, gives $a_i' = \lambda^i a_i$ $\quad b_i' = \lambda^i b_i$, $c_i' = \lambda^i c_i$

$\Delta' = \lambda^{12}\Delta$ $\quad$ y $\quad \lambda^6 [y^2 + a_1 xy + a_3 x] = [x^3 + a_2 x^2 + a_4 x + a_6]\lambda^6$

$\Rightarrow (\lambda^3 y)^2 + (\lambda a_1)(\lambda^2 x)(\lambda^3 y) + (\lambda^3 a_3) = \cdots \Rightarrow y'^2 + a_1' x' y' + a_3' y' = \ldots$

$b_2 = a_1^2 + 4a_2$ $\quad b_2' = a_1'^2 + 4a_2' = (\lambda a_1)^2 + 4(\lambda^2 a_2) = \lambda^2 b_2$.

(check) $*$ Even with the full chang of coordinate $x' = \lambda^2 x + r$, $y' = \lambda^3 y + sx + t$.

we still have $c_i' = \lambda^i c_i$, i.e. $c_4' = \lambda^4 c_4$, $c_6' = \lambda^6 c_6$. $\Delta' = \lambda^{12}\Delta$

Key: $\frac{c_4^3}{\Delta}$, or $\frac{c_6^2}{\Delta}$ does not change. (!)

Rk. When $(E/K, p)$ is written using a W.E/K, we see an addition property.

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

has an involution: $\quad x \overset{\sigma}{\longmapsto} x \qquad y \overset{\sigma}{\longmapsto} -y - (a_1 x + a_3)$.

$y(y + (a_1 x + a_3)) \rightsquigarrow (-y - (a_1 x + a_3))[-y - (a_1 x + a_3) + (a_1 x + a_3)]$

$\qquad\qquad \sigma(y) \qquad\qquad \sigma(y)$

$= -(y + a_1 x + a_3)(-y) = y(y + a_1 x + a_3)$.

(involution: automorphism of order 2)

E.g. $\begin{cases} x^2 + m = y^2 \\ x^2 + n = z^2 \end{cases}$ has 7 obvious involution! (identity) (3 has 4 fixed pt, 4 has no fixed pt).

(In general 4 fixed pt, (automorphism of

Thr 13th Sept/18

Recall: An elliptic curve given by W.E. exhibit a natural involution.

① A curve X/k of genus $g>1$ has only finite auto

* Any action $\sigma: X \longrightarrow X$ induce a k-automor

$$k(X) \xrightarrow{\sigma^*} k(X)$$
$$\nwarrow k \nearrow$$

* Involution has at most 4 fixed pts including $\infty = (0:1:0)$.

② For an E.C. E/k with $p \in E(k)$, we sketch how to *

* ③ Any non-trivial automorphism of a curve X/k has only finitely many fixed pts

(Dedek-D has finite prime ramification).

③ Consider $X \subseteq \mathbb{P}^3$, given by $\begin{cases} x^2+mu^2 = y^2 \\ x^2+nu^2 = z^2 \end{cases}$ $\quad m,n \neq 0 \quad m \neq n. \quad m,n \in k \quad \text{char}(k) \neq 2.$

This curve exist 7 non-trivial involutions. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Dehom: $x^2+m = y^2$, $x^2+n = z^2$. $\quad \sigma_x: x \to -x \quad \sigma_y: y \to -y, \quad \sigma_z: z \to -z.$ Id

$\sigma_{xy}, \quad \sigma_{xz}, \quad \sigma_{yz}, \quad \sigma_{xyz}$

* X/k has 4 k-rational pts at "∞" $(x:y:z:u) : (1:\pm1:\pm1:0)$

* Fixed pts over k. σ_{xyz}: fixe the 4 pts at ∞.

$\sigma_x, \sigma_y, \sigma_z$ also has 4 fixed pts.

But $\sigma_{xy}, \sigma_{yz}, \sigma_{xz}$ has no fixed pts.

* Given any auto (of finite order) of a curve X/k, we can consider 2 related idea:

$\sigma: X \longrightarrow X$, and $\qquad \sigma^*: k(X) \longrightarrow k(X)$.

consider: $X \longrightarrow X/\langle\sigma\rangle$ (set of orbit), the quotient of X of the action $\langle\sigma\rangle$

consider the invariant subfield. $k(X)^{\langle\sigma^*\rangle} = \{ f \in k(X) \mid \sigma^*(f) = f \}$ $\quad \sigma^* \in \text{Aut}_k(k(X))$.

* Calculate $X/\langle\sigma\rangle$ is hard, if we want structure on it (other than topo).

Easy $G = \langle \sigma \rangle$ finite. σ auto of X.

$X = \operatorname{Spec} A$, get $\sigma^*: A \longrightarrow A$

(A integral domain; $A \subseteq k(X)$, $A \subseteq k(X)$)

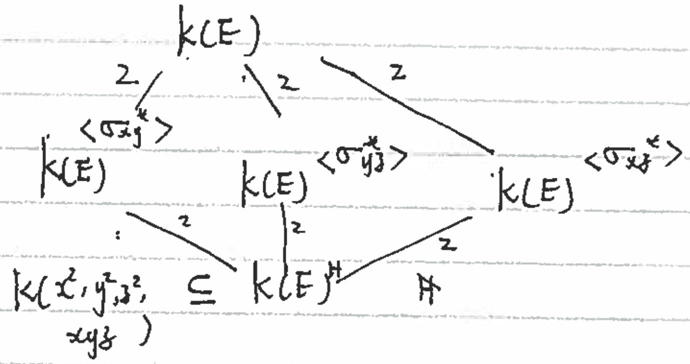
Define the quotient. $X/\langle\sigma\rangle$.

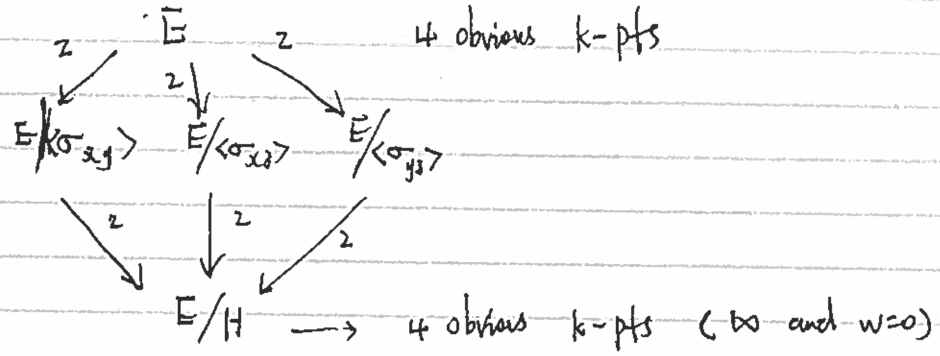
$$X = \operatorname{spec}(A) \longrightarrow X/\langle\sigma\rangle := \operatorname{spec}(A^{\langle \sigma^* \rangle})$$

$$A^{\langle\sigma^*\rangle} := \{ f \in A \mid \sigma^*(f) = f \}$$

Note: $\{\sigma_x, \sigma_y, \sigma_z\}$ generate a subgroup of $\operatorname{Aut}(E/k)$ iso to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

$H := \{\sigma_{xy}, \sigma_{xz}, \sigma_{yz}, id\}$ is a subgroup of order 4.





$k(E)^H$ x^2, y^2, z^2, xyz, Question: $E \overset{?}{\cong} E^H$

$k(E)$: generated by x, y, z.

$$k[x,y,z] \Big/ \begin{pmatrix} x^2+m-y^2 \\ x^2+n-z^2 \end{pmatrix}.$$

Relation: $(xyz)^2 = x^2y^2z^2 = x^2(x^2+m)(x^2+n)$

$*$ Consider $\operatorname{ff}(k[v,w]/w^2 - v(v+m)(v+n))$ v w

Updat: The map exist and is is a k-isomorph.

Ex. All the maps in the above diagram are "unramified" the preimage have the "right number of elements counted correctedly

Over $\bar{k}$, the map have degree 2, and thus should have preimage containing exactly 2 pts.

* Back to W.E. $/k$ → (affine coordinate).

Involution: $x \longrightarrow x$

$y \longrightarrow -y-(a_1x+a_3)$ → involution $E \longrightarrow E$

We can extend to a map $\mathbb{P}^2 \longrightarrow \mathbb{P}^2$, by send $z \to z$

$(0:1:0)$ is a fixed pt.

$y = -y-(a_1x+a_3) \Rightarrow 2y = -a_1x+a_3$

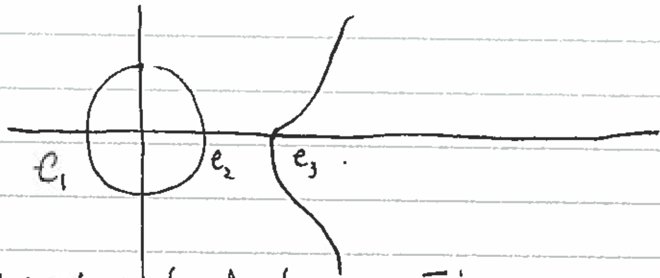
(char $\neq 2$)

* Classic case: $a_1 = a_3 = 0$. we get $2y=0$ ↳ not elliptic curve)

$y=0$ pts $(e_1,0)$ $(e_2,0)$ $(e_3,0)$, e_i solution to $x^3+a_2x^2+a_4x+a_6=0$

(most degenerate)

E/k is supersingular



Total of 4 fixed pts over $\bar{k}$

* Assume (char $k=2$) $\mathbb{D}\, k[x]$

In this case. $a_1x+a_3 \neq 0$ (otherwise $y^2 = x^2+\dots$ not nonsingular).

If (x_0,y_0) a fixed pt: $2y_0 = -(a_1x_0+a_3) \iff a_1x_0+a_3=0$ in char 2.

* (Case $a_1=0$), then $a_3 \neq 0$, then no fixed pts, except ∞.

(Case $a_1 \neq 0$), $\exists!\ x_0 = -\frac{a_3}{a_1}$

* $y_0(y_0+a_1x_0+a_3) = x_0^3+\dots$

E/k is ordinary $\Rightarrow y_0^2 = x_0^3+\dots$

In char $=0$, $y^2=a$, has $\exists!$ solution) → (not perfect,

$\exists$! fixed pt ($x_0 = \frac{a_1}{a_3}$, $y_0 = \sqrt{x_0^3+\dots}$)

In this case $\exists$ 2 fixed pt ...

Tue 18th Sept / 18

Rk: $PGL_{n+1}(k) \subseteq Aut(\mathbb{P}^n(k))$
$A \in M_{n+1}(k)$ $\quad (x_0 : \cdots : x_n) \in \mathbb{P}^n(k)$
$A \cdot (x_0 : \cdots x_n) = (\sum a_{0i} x_i, \ldots,)$

$PGL_{n+1}(k) = GL_{n+1}(k) / k^*$

$k^* \longrightarrow GL_{n+1}(k)$
$\lambda \longmapsto diag(\lambda, \ldots, \lambda)$

Recall: $E/k \quad y^2 + y(a_1 x + a_3) = x^3 \ldots$
involution: $x \longrightarrow x$
$y \longrightarrow -y - (a_1 x + a_3)$.
This involution is induced by an of $\mathbb{R}^2(k)$
$x \rightarrow x \quad y \longrightarrow -y - (a_1 x + a_3 z) \quad z \rightarrow z$.

$$\begin{pmatrix} 1 & -a_1 & 0 \\ 0 & -1 & 0 \\ 0 & -a_3 & 1 \end{pmatrix} \in GL_3(k)$$

Rk: We have inv $E \dashrightarrow E$
Consider $E \longrightarrow \mathbb{P}^1$: projection to the x-
corresponding to the map of fun fields.
$k(E) = ff(k[x,y]/W.E.)$.
$\uparrow \longleftarrow \deg 2.$
$k(x)$ extension is separable even in char $k = 2$.

We have:
$$\begin{array}{ccc} E & \xrightarrow{inv} & E \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array}$$

In fact $E/\langle inv \rangle \cong \mathbb{P}^1$ i.e. $k(E)^{\langle inv \rangle} = k(x)$.

* ~~Fixed~~ The set of fixed pts of inv is related to the ramification subset of the morphism $E \longrightarrow \mathbb{P}^1$

Formula: (Riemann-Hurwitz formula)
Let $\varphi: X \longrightarrow Y$ be a k-morphisms of smooth projective geom.irred connected curve over k.
(a) Then either φ is constant or it is surjective and ...

We say that φ is a separable morphism if the extension is a separable extension.

⑥ If φ is surjective and separable, then for any $p \in Y(\bar{k})$ $\varphi^{-1}(p)$ is a finite set. For all but finite many $p \in Y(\bar{k})$,

$\subseteq X(\bar{k})$

$|\varphi^{-1}(p)| = \deg(\varphi) := [k(X) : k(Y)]$ ⟶ (use separability).

* Riemann-Hurwitz formula (separable morphism)

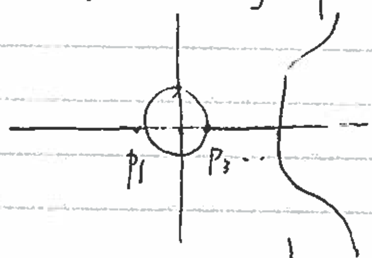
$$2g(X) - 2 = \deg(\varphi)(2g(Y) - 2) + \text{correcting term}.$$

and the correcting term depends only on the ramification of the morphism $\varphi : X \to Y$. It is 0 if the morphism is unramified.

Ex. $\mathrm{Inv} : E \to E$. $\deg(\mathrm{Inv}) = 2$ It is always separable. ☐

$\mathrm{char}(k) \neq 2$, over $\bar{k}$

4 fixed pts p_1, p_2, p_3, ∞



genus($\mathbb{P}^1$) = 0

↑

$$2g(E) - 2 = \deg(\mathrm{Inv})(2g(\mathbb{P}^1) - 2) + \text{correcting}$$

(when project to X-axis (ramified at p_1, p_2, p_3, ∞)

$\therefore$ $0 = 2(-2) + \text{correction}$.

each p_i contributes to a correction ~~faction~~ factor of 1

In the end, $4 = 1 + 1 + 1 + 1$ ⟶ the $\deg(\mathrm{Inv}) - 1$.

(Correction for each point).

* In general, we say $\varphi : X \to Y$ is tame, if $\mathrm{char} k \nmid$ any of the ramification index, then the correcting factor is simply the (ramification index $- 1$)

* $\mathrm{char} k = 2$, Here $\varphi : E \to \mathbb{P}^1$ has degree 2, and the ramification indices are equal to 2

→ char(k) = 2.

$2g(E) - 2 = 2(g(\mathbb{P}^1) - 2) + \text{correction}$. → Contribution.

Rieman Hurwitz:
{ ordinary case: $4 = \delta_{P_1} + \delta_\infty = 2+2$. (wide case)
{ super singular case: $4 = \delta_\infty$ (wide case)

In the wild case, the contribution of each point is at least char(k)

App: R-H can compute genus of curve.

"group scheme"

Thm. Let E/K be a (nice) curve of genus 1, with a point $\infty \in E(k)$. Then the set $E(\bar{k})$ can be endowed with a group structure, s.t. $\forall L$ with $k \subseteq L \subseteq \bar{k}$, $E(k) \subseteq E(L) \subseteq E(\bar{k})$. and $E(k)$ and $E(L)$ are subgroup of $E(\bar{k})$. More precisely,

(a) identity: $\infty \in E(k) \subset E(L) \subseteq E(\bar{k})$

(b) Inverse: in $E(\bar{k})$, when E/K is given by W.E. it is ~~it is~~ the involution.

$\text{Inv}(x:y:1) \longrightarrow (x: -y-(a_1x+a_3):1)$
(coefficients in k)

(c) Addition: $E(\bar{k}) \times E(\bar{k}) \longrightarrow E(\bar{k})$
$(P, Q) \longmapsto P \oplus Q$.

Assume E is given by W.E. P, Q two pts, L is the line $\overline{P-Q}$

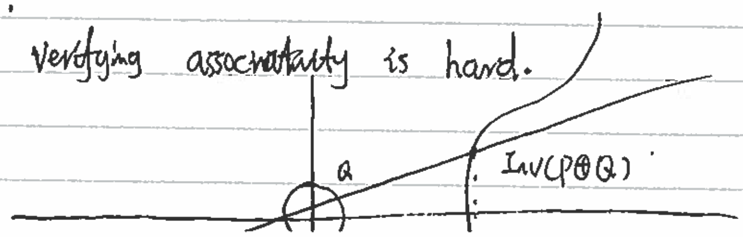
If $P \neq Q$, then $L \cap E(\bar{k}) = \{P, Q, \text{Inv}(P \oplus Q)\}$

If $P = Q$, let L be T_P, $\Rightarrow L \cap E(\bar{k}) = \{P, \text{Inv}(P \oplus P)\}$.

Key facts: ① The coordinate of $\text{Inv}(P \oplus Q)$ is given by rational fcn in the coordinate of P & Q. This show that E/k is an "alg gp".

② Any rational fcn that is used has coefficients in k, and not only in $\bar{k}$. For example, $P, Q \in E(k)$, the line L can be written with coefficients in k.

Warning: verifying associativity is hard.



G a group, $m \in$ ~~$\mathbb{Z}$~~ $\mathbb{N}$,

$G[m] = \{g \in G \mid g^m = e_G\}$

When G is commutative, $G[m]$ is a subgroup.

E.g. In D_8, 6 elements in $D_8[2]$

E.x. In $SL_2(\mathbb{Z})$ can be generated by 2 elemts of finite order.

*

(Torsion Subgp). Let $m \in \mathbb{N}$, we can define a morphism of curves over k.

$[m]: E \longrightarrow E$

$P \longmapsto \underbrace{P \oplus \cdots \oplus P}_{m \text{ times}}$ (need associativity).

↳ multiplication by m.

Thm: ~~I~~ $[m]$ is a surjective morphism of algebraic curve over k.

It show that: $[m]: E(\bar{k}) \longrightarrow E(\bar{k})$ is surjective.

not mean: $[m]: E(k) \longrightarrow E(k)$ is surjective.

* The degree of field extension $[m]^*: k(E) \longrightarrow k(E)$ is m^2.

the preimage of ∞ in $E(\bar{k})$, $[m]$ is a group homomorphism, So the preimage. $\ker[m](\bar{k}) \subseteq E(\bar{k})$ is a subgroup.

① If $\mathrm{char}(k) \nmid m$: $\ker[m](\bar{k}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

② If $\mathrm{char}(k) = p > 0$ $\ker[p^r](\bar{k}) \cong \begin{cases} (0) & \text{supersingular} \\ \mathbb{Z}/p\mathbb{Z} & \text{ordinary} \end{cases}$

20th/Sept/18 Thr.

Recall: We have a group structure on Elliptic curve.

- An E/k with $P_0 \in E(k)$ is endowed with the structure of group scheme.
- We have defined

$$E(\bar{k}) \times E(\bar{k}) \longrightarrow E(\bar{k})$$
$$(P, Q) \longmapsto P \oplus Q \leftarrow$$ coordinate of $P \oplus Q$ given by rational functions of coordinate of P & Q.

- is the motivation $y \longrightarrow -y-(a_1x+a_3)$ where E/k is given by W.E.

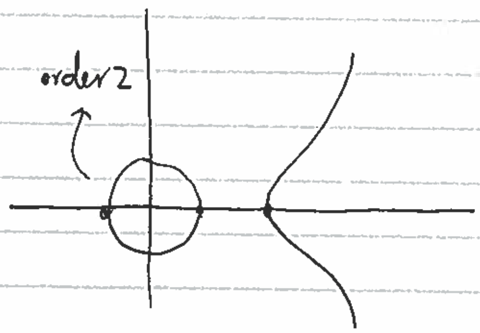
$E(n)$ = kernel of multiplication by n $[n]: E \longrightarrow E$.
defined by algebraic equ., $E(n)(k) \subseteq E(n)(L) \subseteq E(n)(\bar{k})$ $k \subseteq L \subseteq \bar{k}$.

Eg.

Ex. ||When $n=2$||

The x-coordi of the pts of order 2 on E/k given by a W.E.
$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$
are the root of $4x^3+b_2x^2+2b_4x+b_6 \in k[X]$

- To be of order 2: $P \neq \infty$, require $\mathrm{inv}(P) = P$



In $\mathrm{char}(k) \neq 2$, InV has 4 fixed pt over $\bar{k}$
$\mathrm{char}(k) = 2$, InV has $\begin{cases} 2 \text{ fixed pts} \\ 1 \text{ fixed pts} \end{cases}$

* In particular, $E(2)(\bar{k}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } \mathrm{char}(k) \neq 2 \\ \mathbb{Z}/2\mathbb{Z} \text{ or } \{0\} & \text{if } \mathrm{char}(k) = 2 \end{cases}$

Rk: very few curves have group structure.

E.g. $\mathbb{G}_a/k$: additive group

with the property that $\forall L \supseteq k$, $k \subseteq L \subseteq \bar{k}$

$\mathbb{G}_a(L) = (L, +)$

$\mathbb{G}_a = \mathrm{Spec}(k[x]) \longrightarrow$ affine line.

E.g. $\mathbb{G}_m/k$ multiplicative group.

$\forall k \subseteq L \subseteq \bar{k}$, $\quad \mathbb{G}_m(L) = (L^*, \cdot)$

$\mathbb{G}_m = \mathrm{Spec}\, k[x, \frac{1}{x}] = \mathrm{Spec}\,(k[x,y]/xy-1)$.

Multiplication map:

$$k(x,y)/(xy-1) \longrightarrow k(x,y]/(xy-1) \otimes k[x,y]/(xy-1)$$

Come from the multipl. $\mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{G}_m$.

$x \longmapsto x \otimes x$

$y \longmapsto y \otimes y$

* (Torsion pts) For $\mathbb{G}_a$.

$$\mathbb{G}_a[n](\bar{k}) = \{ r \in \bar{k} \mid nr = 0 \} \quad (\ast)$$

$$= \begin{cases} \{0\} & \text{if } p = \mathrm{char}(k) \nmid n. \\ \bar{k} & \text{if } p \mid n. \end{cases}$$

For $\mathbb{G}_m$

$$\mathbb{G}_m[n](\bar{k}) = \{ r \in \bar{k}^* \mid r^n = 1 \}$$

$$= \begin{cases} \cong \mathbb{Z}/n\mathbb{Z} & \text{if } p \nmid n. \\ = \{1\} & \text{if } p = n. \end{cases}$$

Thm: Let X/k be a smooth geom conn curve over k, and assume ~~it~~ is a group scheme.

it is a twist of $\mathbb{G}_m/k$ or $\mathbb{G}_a/k$, i.e. there exist a finite extension L/k s.t. over L, $X \times_{\mathrm{Spec}\,k} \mathrm{Spec}(L)$ is isom to either $\mathbb{G}_m/L$, or $\mathbb{G}_a/L$

E.g. (Twist) (Quadratic twist)

Curve X/k is defined by $y^2 = g(x)$, where $g(x) \in k[x]$.
Let $d \in k$, d not a square, so, $k \subsetneq k(\sqrt{d})$

Let Y/k be curve given by $dy^2 = g(x)$.

* In general, X/k and Y/k are not isomorphic. But over $L = k(\sqrt{d})$ we can change variable

$$\begin{cases} x \to x \\ y \to Y = \frac{1}{\sqrt{d}} y \end{cases}$$

and get an isomorphism:

$$X/L \longrightarrow Y/L$$
$$(x, y) \longmapsto (x, \tfrac{y}{\sqrt{d}})$$

Twist of $\mathbb{G}_m/k$

$\mathbb{G}_m/k : xy - 1 = 0 \rightsquigarrow X^2 - Y^2 = 1$

$x \sim X - Y$

$y \sim X + Y$.

This is an isomor of $\mathrm{char}(k) \neq 2$.

Twist. Let $d \in k$, d not a square $(\mathrm{Char}(k) \neq 2)$
group structure on: ~~y $Y^2 = X^2 + $~~ $x^2 - dy^2 = 1$.

$$(x_1, y_1)(x_2, y_2) \longrightarrow (x_1x_2 + dy_1y_2,\ x_1y_2 + x_2y_1).$$

* formal name of group scheme structure on $x^2 - dy^2 = 1$.

$$\#\ (x_1 + \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) = x_1x_2 + dy_1y_2 + \sqrt{d}(x_1y_2 + x_2y_1)\ \#$$

$R'_{L/k}\mathbb{G}_{m_L}$ where $L = k(\sqrt{d})$

$= \{ (x,y) \in k^2 \mid x^2 - dy^2 = 1 \}$

$\downarrow$

$\{ x + \sqrt{d}y \in L,$ with $Norm(x+\sqrt{d}\,y) = 1 \}$

* Inverse map.

$R^1_{L/K} \mathbb{G}_{m,L} \longrightarrow R^1_{L/K} \mathbb{G}_{m,L}$

$(x, y) \longmapsto (x, -y)$

since $(x+\sqrt{d}y)(x-\sqrt{d}y) = 1$, since the pt is on the curve.

* (Group scheme)
* Ellip curve produce interesting number fields.
* (Motivation) / Consider $[n] : \mathbb{G}_m \longrightarrow \mathbb{G}_m$ over any field k.

$\mathbb{G}_m(\bar{k}) \supset \mathbb{G}_m[n](\bar{k}) = \{$set of n^{th} root of unity in $\bar{k}\}$

* Cyclotomic field: $k(\zeta_n) = k$ (coordinate of the n-torsion pts in $\mathbb{G}_m$)

$k(\zeta_n)$ | k

properties: ① Galois $/k$ (and even abelian)

L | $\mathbb{Q}$ $\rightsquigarrow$ number $\in \mathbb{Q}$, L | K $\rightsquigarrow$ ideal in $\mathcal{O}_K$.

$=$ disc ideal.

L | disc. | $\mathbb{Q}$

L | $k(t)$, $X \downarrow \mathbb{P}^1$ $\leftarrow$ ramification.

* Key properties $\mathbb{Q}(\zeta_\ell)$ | $\mathbb{Q}$ ℓ prime.

disc $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ $=$ a power of ℓ (up to a sign).

* Consider E/k elliptic curve.
$[n]: E \longrightarrow E$, we get an subgroup $E(n)(\bar{k}) =$ n-torsion subgroup of E.

* If E/k is given by W.E, we could discuss the coord.

Def: $K(E[n]) := k$ (all pts of the pts in $E(n)(\bar{k})$).

Note: If $E(n)(k) = E(n)(\bar{k})$, then $k = k(E(n))$.

project: ① Show that the x-coordinate of order 3 are the roots of
$3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 \in k[x]$.

② Make enough computation to come up with a conjecture about information on the ramification of $\mathbb{Q}(E[3]) / \mathbb{Q}$

③ prove that $K(E(n))/k$ is Galois

Thm (Model-Weil Thm)
Let k be a number field, Then.
$E(k) \cong \mathbb{Z}^r \oplus$ finite abelian group.
(or $E(k)$ is a finitely generated abelian group)
r is called the rank of E/k over (k) (depends on k).

$[-1]p =$

$[-2]p = [b, 0]$, $p = [0, 0]$

$[-2]p = p \Rightarrow b = 0$

25th/sept/18 Tue.

E/k

$\forall n \in \mathbb{N}$, $[n] : E \longrightarrow E$. defined over k.

$[n] : E(\bar{k}) \longrightarrow E(\bar{k})$ (surjective)

$\ker([n])(\bar{k}) \rightsquigarrow k$(all coordinate of pts in $E[n](\bar{k})$.

|

k.

Thm (Mordell over $\mathbb{Q}$)

(Weil over any number field

Let k be a number field, Then $E(k)$ is a f.g. abelian group.

i.e. $E(k) \cong \mathbb{Z}^r \oplus E(k)_{tor}$ $r = \text{rank}(E/k)$ (depends on k).

Rk. G a group. [with $|E(k)_{tors}| < \infty$] ($\mathbb{Q}/\mathbb{Z}$).

$G_{tors} = \{ g \in G$ of finite order$\}$ not subgroup in general.

G_{tors} is a subgroup when G is abelian.

Rk. Let $n = |E(k)_{tors}|$. Then $E(k)_{tors} \subseteq E[n](\bar{k}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

* The pf of Mordell-Weil thm is in 2-steps,

(a) $E(k)/[n]E(k)$ is finite.

(b) $E(k)$ is finitely generated.

Note: Let $G = (\mathbb{R}, +)$, $[n] : G \to G$ is surjective.

$G/nG = (0)$, but G is not f.g.

open problem: Have (a) true, find algorithm ~~to~~ for the generator of $E(k)/[n]E(k)$.

Major prob: Behavior of $r(E/k)$ over all E/k.

1938: $\exists$ $E/\mathbb{Q}$ with $r(E/\mathbb{Q}) \geq 3$. (Billing)

(1974, 1975): $rk\, E(\mathbb{Q}) \geq 4$, $rk(E/\mathbb{Q}) \geq 7$

(Penney-Pomerance UGA)

(Elkies) 2006: $rk(E(\mathbb{Q})) \geq 28$

largest know 2009 (Elkies) $\exists$ $E/\mathbb{Q}$ with $rk\, E(\mathbb{Q}) = 19$

Conjecture: " $1/2$ of Elliptic curve has rank 0, the other half has rank 1.

2018 (Preprint Park-Poonen-): * produce heuristic that $rk(E(\mathbb{Q})) \leq 21$ except for finitely many $E/\mathbb{Q}$.

In particular $rk(E/\mathbb{Q})$ ~~over~~ $< \infty$ are the set of all $E/\mathbb{Q}$.

(Elkies) 2009 There are ∞ many $E/\mathbb{Q}$ with rank 19.

(function fields / number fields)

Thm (Mazur 197*)
Let $E/\mathbb{Q}$ be an Elliptic Curve
$E(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & N=1,\dots,10 \text{ or } 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & N=1,2,3,4 \end{cases}$ so $|E(\mathbb{Q})_{tors}| \le 16$.

Thm. (Merel, 199*)
Let k be any ~~field~~ number field, Then $\exists\, C = C(k)$, s.t.
$|E(k)_{tors}| \le C$. $\forall E/k$ elliptic curve.
In fact, than can be improved
$\exists\, C' = C'(d)$ s.t. $\forall$ number field $k/\mathbb{Q}$ with $[k:\mathbb{Q}]=d$
$|E(k)_{tor}| \le C'$, $\forall E/k$

App. Let $p \in E(\mathbb{Q})$ If $ord(p) > 16$, then p has infinite order.

* (Main idea in Mazur's Thm) (Harvard)
Given E/k, and a point $p \in E(k)$ order $N \ge 4$; there exist an algebraic curve $Y_1(N)/k$.
s.t. the pair $(E/k, p)$ defines a k-rational points on $Y_1(N)/k$.
Mazur showed that $N \ne 1 \dots 10$ or 12.
then $Y_1(N)(\mathbb{Q}) = \phi$

* Description of the first few $Y_1(N)$
Let E/k given by a Weierstrass. Eq, $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x +$
Let $p \in E(k)$.
Translate to have $P = (0,0)$, get a new W.E.
$y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ (new a_i's).
If $p = (0,0)$ has order 2. then $[2]p = 0$.
$[-1] = p$, $-p = (x, -y - a_1x - a_3)$
$= (0, -a_3)$
Assume $ord(p) > 2$, then $a_3 \ne 0$.

* Change variable $y \to y + \frac{a_4}{a_3}x$, to elimi. the x term.
$y^2 + a_1xy + a_3y = x^3 + a_2x^2$ (new a_i's).

* Chang variables: $y = \lambda^3 y'$, $x = \lambda^2 x'$

to get $\cdots + a_3\lambda^3 y' = \cdots + a_2\lambda^4 (x')^2$ divide by λ^6.

$\tilde{a}_3 := \frac{a_3}{\lambda^3}$ $\tilde{a}_2 = \frac{a_2}{\lambda}$. want $\tilde{a}_3 = \tilde{a}_2$

$\Rightarrow \frac{a_3}{\lambda^3} = \frac{a_2}{\lambda^2} \longrightarrow \lambda = \frac{a_3}{a_2}$ well defined and $\neq 0$.

$\Rightarrow$ new W.E. $y^2 + a_1 xy + a_3 y = x^3 + a_3 x^2$, $a_3 \neq 0$.

* By convention, $a_1 := 1 - c$, $a_3 = -b$

The W.E. is then:

$\boxed{y^2 + (1-c)xy - by = x^3 - bx^2}$ Tate's normal form.

with rational pt $(0,0) = P$

$[-1]P = (x, -y - a_1 x - a_3) = (0, b)$

* By construction, we have in addition: pts

$[2]P$

$\boxed{[-2]P}$

$[3]P$

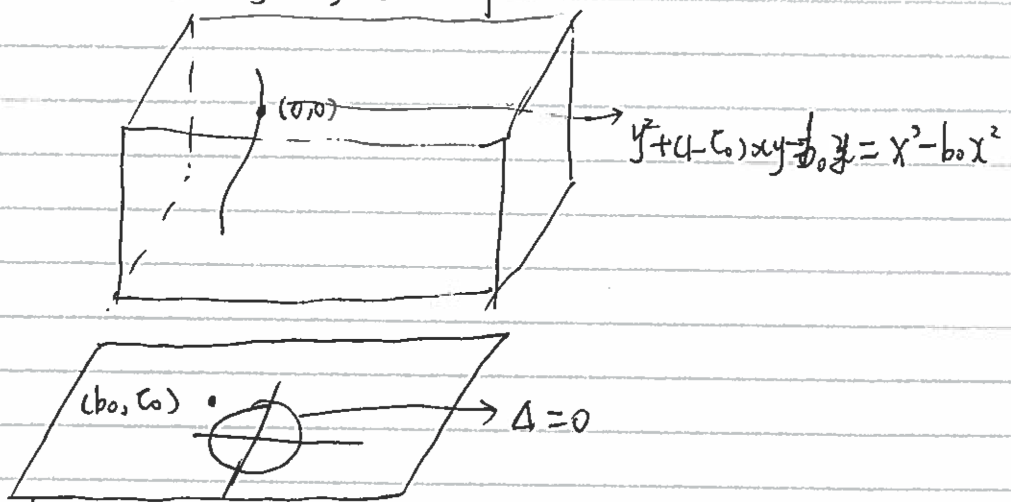
$\boxed{[-3]P}$

Ex. Make them explicit, as well as $[-2]P$ and $[-3]P$.

Ex. $\Delta = \Delta(b,c)$

$= b^3(16b^2 - b(8^2c + 20c - 1) - c(1-c)^3)$

* We have a 2-dim family of Elliptic curve.



* Moreover, given any E/k with $P \in E(k)$, ord(P) > 3 there exist $(b,c) \in k^2$, s.t.

$E/k \Longleftrightarrow$ the in this family over (b_0, c_0)

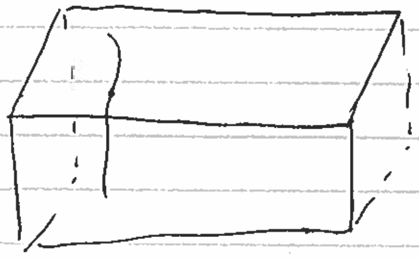
$P \longleftrightarrow (0,0)$ ↳ ord(P) > 3

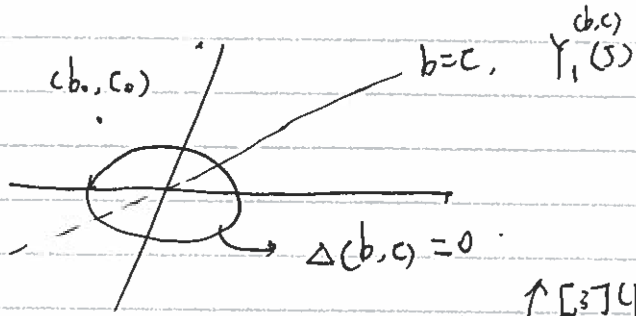
27th/Sept/18

* Torsion. pts on EC.

Proving that no pts of order N on $E(k)$ on E/k ($\forall k$), is equivalent to a certain other curve $Y_1(N)/k$ has no k-rational pts.

* Given E/k and $P \in E(k)$, we have a process to get $(b_0, c_0) \in k^2$. and an isom over k from a W.E. for E/k to the W.E. $y^2 + (1-c_0)xy - b_0 y = x^3 - b_0 x^2$; sending P to $(0,0)$.





Say $P=(0,0)$ $\quad [-1]P = (0,b)$ $\quad$ ↑ $[3](P)$ $(x, y - a_1 x - a_3)$

Other pts $(b,0)$ ..., (b, bc), ... $(c, -b-c)$, (c, c^2) → $[-3](P)$.

* Computation: tangent line at $(0,0)$, $by=0$.

other intersection pt: $x^3 - bx^2 = 0$, $\Rightarrow x=0$, or $x=b$.

New pt: $(b,0)$ $\quad [-2]P = 0$

$2[P] = \mathrm{Inv}([-2](P)) = (b, 0 - [(1-c)b - b]) = (b, bc)$

Def: $Y_1^{(b,c)}(4)$.

We want all (b,c) s.t. $P=(0,0)$ has exact order 4.

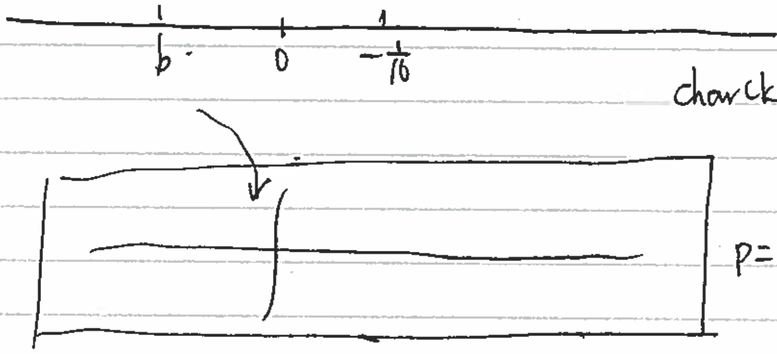
Thus $[2]P \neq \infty$, we want $[2]P = [-2]P$

So $(b,0) = (b, bc)$

Since $b \neq 0 \Rightarrow c=0$, ($b \neq 0$, since $b \mid \Delta(b,c)$).

* We have obtained a family of E.C. over the curve $c=0$, over the (b,c)-plane. $\quad Y_1^{(b,c)}(4) :=$ plane curve $c=0$.

~ the value of b s.t. $\Delta(b,0)=0$.



$Y_1^{(b,c)}(4)$.

char$(k) \neq 2$

$P = (0,0)$.

$y^2 + xy - by = x^3 - bx^2$.

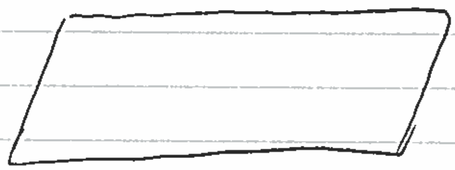
Def: of $Y_1^{(b,c)}(5)$ .. we want $[-2]P = [3]P$

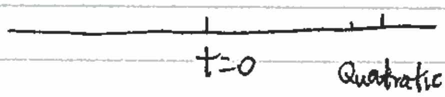
$\Leftrightarrow$ $(b, 0) = (c, -b-c)$

* Family over $Y_1^{(b,c)}(5)$

$y^2 + (1-b)xy - by = x^3 - by^2$ $\quad$ $b = c = t$

$y^2 + (1-t)xy - ty = x^3 - ty^2$.





$Y_1^{(b,c)}(5)$.

$\Delta(t) = t^5(t^2 - 11t - 1)$.

$\Delta = 11^2 + 4 = 125$, $\sqrt{125} = 5\sqrt{5}$.

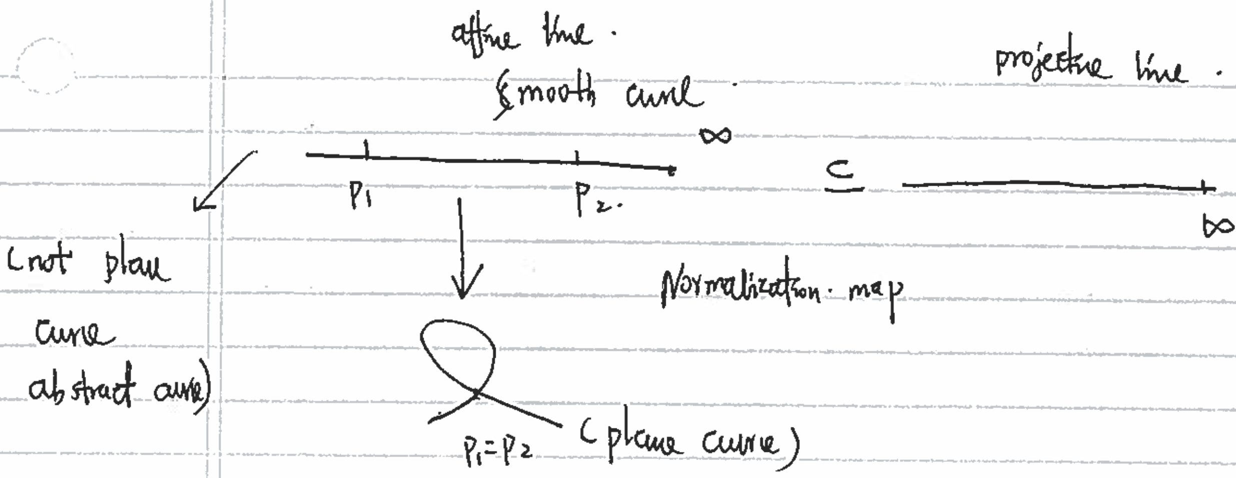
* (Ex*) Do the case $Y_1^{(b,c)}(6)$, $Y_1^{(b,c)}(7)$ ....

Thm: $Y_1^{(b,c)}(N)$ (has genus 0) $\Rightarrow$ is parametrizable, for $N = 1, \ldots, 10$ and 12.

* In our example, $Y_1^{(b,c)}/K$ is always open ~~set~~ subset of the plane curve. Nevertheless, we have a function field associated to $Y_1^{(b,c)}/\mathbb{Q}$. So there is a smooth projective curve with that function field.

(open subset) $\leftarrow$ $\tilde{Y}_1^{(b,c)}(N)$ $\subset$ $\tilde{X}_1^{(b,c)}(N)$ (smooth)

$\downarrow$



$\mathbb{Z}[\alpha]$, α root of $f(x)$. $K=$

(Favorite ring DEDek-D)

(D-D)
"$\mathcal{O}_K$ → Integral closure of $\mathbb{Z}[\alpha]$ in K

$\bigcup \quad \subseteq K = ff(\mathbb{Z}[\alpha]) = \mathbb{Q}(\alpha)$.

$\mathbb{Z}[\alpha]$ a root of $f(x)$.

$Y_1^{(b,c)}(N)$.

(25 pts of order 5). $Y_0^{(b,c)}(N)$ sub gp of order 5.

$Y_1^{(b,c)}(N) \to$ moduli curve!

$Y_1^{(b,c)}(5)$ no points ~~of order 5~~ over $\mathbb{Q}$.

* In Literature. definition of 2 curves $Y_1(N)/K \subseteq X_1(N)/K$.

$\tilde{Y}_1^{(b,c)}(N) \xrightarrow{\sim} Y_1(N)$ over K., but this should be true!

Que. For the curve $Y_1^{(b,c)}(N)$, do they have singularities.

* Can this be proved?

Set all pair $(E/K, P \in E(K))$, of P exact order n, up to isomorphism.

$(E/K, P) \sim (E'/K, P')$

iff. $\exists\ \varphi: E \to E'$, s.t. K-isomorphism. st. $\varphi(P) = P'$.

$$E \longrightarrow E$$
$$p \longmapsto -p,$$

up to HW exercise, we have a map.

$$S \longrightarrow Y_1^{(b,c)}(N)(k).$$

Is this injective and bijective.

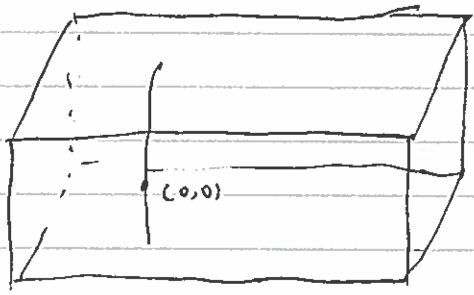
2th/oct/18 We-Tue.

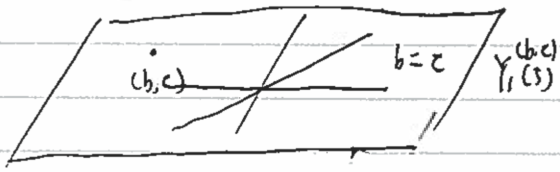
$n \geq 4$, $Y_1^{(b,c)}(N)/k$

$\left.\begin{array}{l} E/k \\ p \in E(k) \\ \mathrm{ord}(p) \neq 2,3 \end{array}\right\} \rightsquigarrow (b_0, c_0) \in k^2$ $p \mapsto (0,0)$

$y^2 + (1-c)xy - by = x^3 - bx^2$ $\Delta(b,c) \in \mathbb{Z}[b,c]$

* ($b=0$, No term of deg 1, ⇒ singular.





$E(b,c)|_{Y_1(5)}$ (Surface)

↓ ↑ section (0,0)'

$Y_1^{(b,c)}(5) \subseteq X_1^{(b,c)} \cong \mathbb{P}^1$

Surface

↓ fibers are almost everywhere elliptic curves.

$\mathbb{P}^1$

★ or we get a elliptic curve over function field $k(Y_1^{(b,c)}(N))$ with a rational pt of order N.

★ $S = \{$ all point E/k, $p \in E(k)$ of order $N \} / \sim$

isomorphism. $(E/k, p) \xrightarrow{\varphi} (E/k, p')$ $\varphi: E \longrightarrow E$ isomor over k ($\varphi(\infty) = \infty$.

s.t. $\varphi(p) = p'$.

Ex. $(E/k, p) \sim (E/k, -1[p])$

$$S \xrightarrow{\text{bijection}} Y_1^{(b,c)}(N)(k).$$

$(E/K, P) \longrightarrow (b_0, c_0)$ giving $(E(b_0, c_0),\ p_0 = (0,0))$

$$\wr\!\uparrow$$

$$(E, P).$$

well-defined

$$(E/k, P) \xrightarrow{\sim} (E(b_0, c_0), (0,0))$$

$$\uparrow S$$

isomorph. ↘ $(E'/k, p')$

* How do we describe all elliptic curves?

$S =$ All elliptic curve E/k, up to isomorphism of elliptic curve.

we want map $S \xrightarrow{\varphi_i} \bar{k}$ $i = 1, \ldots$

φ_1 is ~~two~~ some "invariant" on S.

Then, we have

$$S \longrightarrow \bar{k}^n$$

$$s \longmapsto (\varphi_1(s), \ldots, \varphi_n(s))$$

Is the Image in some algebraic ~~variety~~ subvariety of $\bar{k}^n$? (Ques).

*

↗ (Fine module spa

(Best case) S is a bijection with $V(k)$ and this holds for all extension over k.

* ☆ Suppose answer to Que is yes, then we can define by equations with coeff in k

* For S as above, such V/k does not exist, But such V/k exist with weaker property $\bar{S} = \{E/\bar{k}$ elliptic curve, up to iso$\} \xrightarrow{\sim} V(\bar{k})$.

We have the word V/k (coarse moduli space).

(Recall) * For W.E. E/k, we define b_i, c_i, Δ,

$$\left.\begin{matrix} b_i \\ c_i \\ \Delta \end{matrix}\right\} \in \mathbb{Z}[a_1, \ldots, a_6].$$

we show that change of variable, produce a new W.E.

$x' = \lambda^2 x + r$ $\quad \lambda \in k^*$,

$y' = \lambda^3 y + sx + t$

So we see that $\dfrac{\alpha c_4^3 + \beta c_6^2}{\gamma c_4^3 + \delta c_6^2}$ is invariant when defined.

$\Delta = \dfrac{c_4^3 - c_6^2}{1728} \in \mathbb{Z}[a_1, \dots, a_6]$.

* (Traditional choice):

$j(E/k) = j(a_1, \dots, a_6) = \dfrac{1728\, c_4^3}{c_4^3 - c_6^2}$ j invariant.

Thm. Let $\bar{S}$ = set of elliptic curve over $\bar{k}$, up to iso

Then $j \quad \bar{S} \longrightarrow \mathbb{A}^1(\bar{k}) = \bar{k}$

$E/\bar{k} \longmapsto j(E/\bar{k})$.

is a bijection.

(E_1/k, E_2/k may not be iso $\Rightarrow$ $E_1/\bar{k}$, may iso $E_2/\bar{k}$, $\Rightarrow$

* $S = \{$set of elliptic curve over $k\}/\sim$.

is not injective

$\hookrightarrow S \xrightarrow{j} \mathbb{A}^1(k)$

Eg. (i) $y^2 = f(x)$, (Char $k \neq 2$)

Let $L = k(\sqrt{d})$ $d \in k$, square free.

(ii) $dy^2 = f(x)$. E_d/k new elliptic curve.

become Isomorphic be to E/k over L.

But In general, it is not iso to E/k over k.

(E_d is called a quadratic twist)

Pf of the Thm:

Surjectivity: Given $j_0 \in \bar{k}$, then the curve $E(j_0)/\bar{k}$ given by

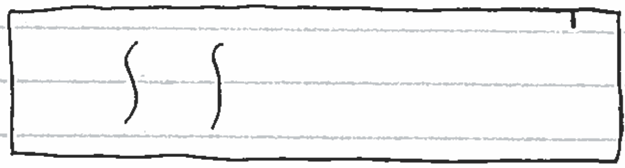
$y^2 + xy = x^3 - \dfrac{36}{j_0 - 1728}x - \dfrac{1}{j_0 - 1728}$

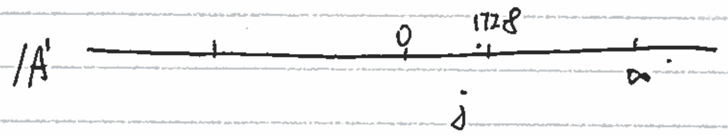
has $j(E(j_0)) = j_0$, $\forall j_0 \neq 0, 1728$

$j_0 = 0$: consider $y^2 + y = x^3$, $\Delta = -27$

$j_0 = 1728$ consider $y^2 = x^3 + x$, $\Delta = -64$

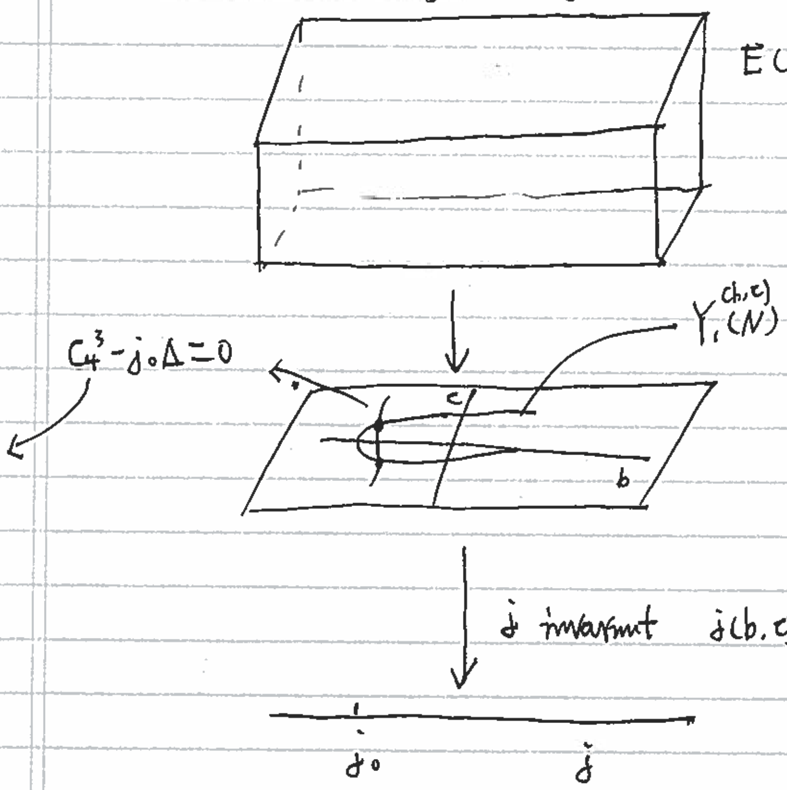
Rk. The proof gives a family of elliptic curve over $\mathbb{A}^1 \setminus \{0, 1728\}$.





function field is $k(j)$.

Ques: What is the minimum number of pts need to be removed in order to get a ~~smooth family~~ of elliptic curve.
(non-constant) (non-isotrivial) (trivial after extension)
(Not exist one family works for all)



it has deg 12.

j invariant $j(b,c) = \dfrac{C_4^3(b,c)}{\Delta(b,c)}$

How many pts on $Y_1^{(b,c)}(N)(\bar{k}) \cap \{j = j_0\}$.

pair $E/\bar{k}$, p of order N $p \in E(\bar{k})$ and $j(E/\bar{k}) = j_0$.

and

4th/oct/18 Thr

E/k

$\hookrightarrow k(E[3])$ $\qquad\qquad$ $\mathbb{Q}(E(3))$

$\qquad\qquad | \qquad\qquad\qquad\qquad | \quad \searrow$ discriminant $\in \mathbb{Z}$

$\qquad\qquad k \qquad\qquad\qquad\qquad \mathbb{Q}$

$3 \mid \mathrm{disc}(\mathbb{Q}(E(3))/\mathbb{Q})$ all have 3-torsion on $\mathbb{Q}$.

$E(3)\,\mathbb{Q} \supset \mathbb{Z}/3\mathbb{Z}$

Thm: E/k be elliptic curve, Let $N \geq 1$, $(\mathrm{char}(k), N) = 1$,
Then $E[N](k) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\Rightarrow k$ contain the N-th root of unity.

$k(E[N])$
$|$
$k(\zeta_N)$
$|$
k

$\{p \mid p \mid \Delta_{\mathbb{Q}(E(3))}\}$
$\qquad \parallel$
$\{3\} \cup \{p \mid p \mid \Delta(E)\}$

[J. E. Cremona / Algorithm of Modular Elliptic Curve]

E.x. $(Y_1^{(b,c)}(V))$ $\qquad\qquad 2^6 \qquad -2^6 7^3$

John Cremona.

rank / Torsion of size / sign of discr /.

(Arithmetic Moduli of Elliptic Curve (Katz)

Recall: E_j (Give EC with j Given)

$\downarrow$

$\mathbb{A}^1 \setminus \{0, 1728\}$

$j = 0$, $\quad y^2 + y = x^3$ $\qquad \Delta = -27$

$j = 1728$, $\quad y^2 = x^3 + x$, $\qquad \Delta = -64$.

* $j = 0, 1728$ are the only EC with extra automor. (except inv)

* $y^2 = x^3 + Ax \Rightarrow j = 1728 \qquad \forall A \neq 0$

$y^2 = x^3 + B \Rightarrow j = 0$, $\qquad \forall B \neq 0$.

check $y^2 + y = x^3 \xrightarrow{\mathrm{char} \neq 2} y^2 = x^3 + \frac{1}{4}$ $\longrightarrow$ [illegible]

[illegible]

$y^2 = x^3 + Ax$ $\quad x \mapsto -x$ ~~ix~~, $y \mapsto iy$ $\}$ order 4 if ~~order~~ char(k) $\neq 2$.

$-y^2 = -x^3 - Ax$.

This is Automorp in $\bar{k}$.

Recall: We have a morphism.

$Y_1^{(b,c)}(N) \longrightarrow \mathbb{A}^1$.

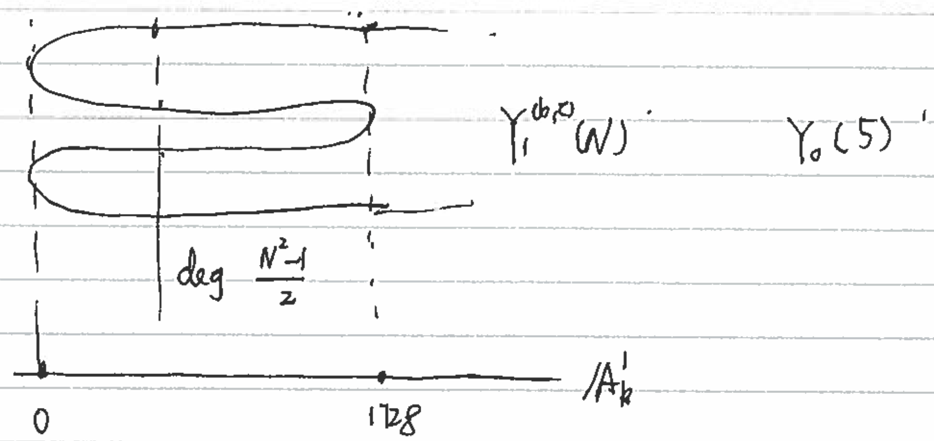
j invariant $\longrightarrow$ N^2 pt there.

E/k, $P \in E[N](k)$ of order N $\longrightarrow j(E/k)$

Assume N is prime, coprime to char(k)

So there are N^2-1 pts of exact order N

~~except~~ expect that deg is $\frac{N^2-1}{2}$.



morphis is ramified at 0, 1728 (and at ∞ when projectified)

9th / Oct / 18 Tue.

* Toward understanding the info in Cremona's table.

* N = conductor of E for $E/\mathbb{Q}$, $N \in \mathbb{N}$,

$N = \prod_{p \text{ prime}} p^{n_p}$

$\longrightarrow N_E$

* Symbol. I, II, III, IV, IV^*,

Kodaira's symbol for the reduction modulo p of the elliptic curve.

reduction at p is I $\quad n_p := 0 \quad$ (good reduction)

Reduction at p is I_n $\quad n_p := 1$, $\quad$ (multiplicative red)
$n \geq 1$

Other reduction: $n_p \geq 2$ if $p \neq 2, 3$, n_p in this case is 2. (addit red)

* C_p. Tamagawa number

order of the component group $\Phi_p(\mathbb{Z}/p\mathbb{Z})$

* Shimura - Taniyama - Weil conjecture for $E/\mathbb{Q}$

There exist a non-constant morphism over $\mathbb{Q}$

$X_1(N_E) \longrightarrow E$

$/\mathbb{Q}$ (moduli curve)

$\longrightarrow$ (good reduction except prime p that divide N_E)

* In general, for E/k, $\Delta_{E/k}$ is not something we have defined.

But: for each W.E. for E/k, we get Δ(W.E./k)

Over $\mathbb{Z}$, we can define $\Delta_{E/\mathbb{Q}} = \prod_{\text{prime}} p^{\nu_p}$

where ν_p = minimal exponent of p appearing among all W.E. * $E/\mathbb{Q}$ which have $a_1, \dots a_6 \in \mathbb{Z}$

In char $\neq 2, 3$, ν_p is between 1 – 12.

* Over PID ($\mathbb{Z}$), it is possible to find a single W.E. for $E/\mathbb{Q}$,

s.t. Δ(W.E.) = $\Delta_{E/\mathbb{Q}}$ $\longrightarrow$ minimal discriminant

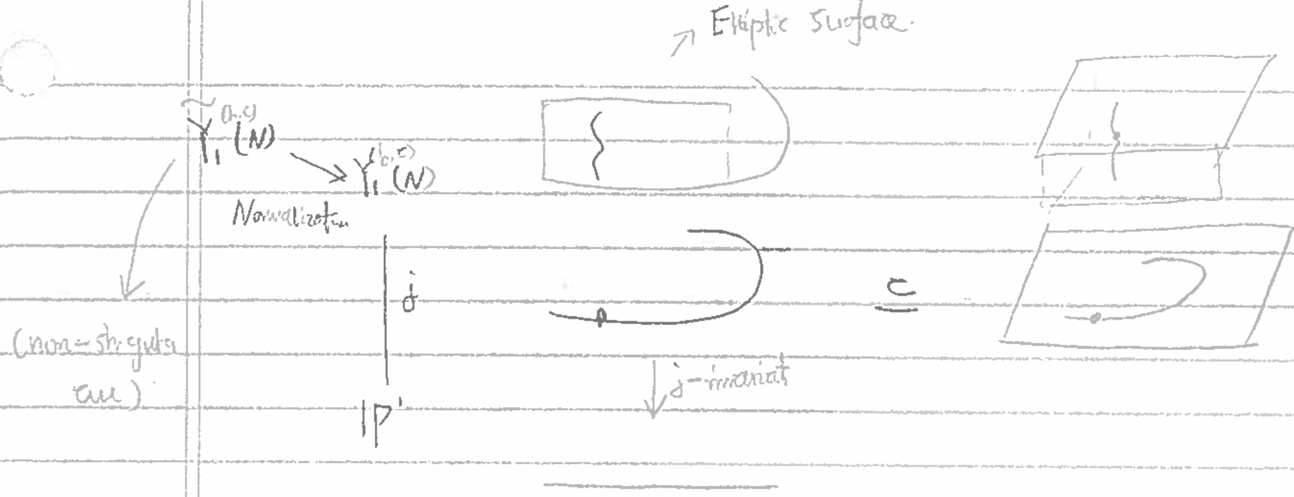
* All curves in Cremona's table create the minimal $\Delta_{E/\mathbb{Q}}$

Fact. $N_E \mid \Delta_{E/\mathbb{Q}} \longrightarrow$ minimal discriminant

and they have the exact same prime factors.

Recall. $Y_1^{(h.c)}(N)$

$\mid$
δ



Equation of

equated $[-2]P = [N-2](P)$

or

So that P has order N

(Remove: when N is not prime any component where P has order smaller than N)

E.g. $\boxed{N=7}$

Equation: $bc - c^3 = b^2$ ($\Delta(b,c) \neq 0$)

Singular at $(0,0)$ — field of fraction.

* $B = k[b,c]/(bc-c^3-b^2) \subseteq$ normalization $\subseteq ff(B)$

$\frac{b}{c}$, since $\left(\frac{b}{c}\right)^2 + -\frac{b}{c} + c = 0$

$\frac{b}{c}$ is integral over B

$B \subseteq B[\frac{b}{c}] \simeq k[c,\frac{b}{c}]/\left(\left(\frac{b}{c}\right)^2 - \frac{b}{c} + c\right) \subseteq ff(B)$

$\simeq k[\frac{b}{c}]$. → parabola $\simeq$ affine line.

* $y^2 - (1-c)xy - by = x^3 - bx^2$ over $bc - c^3 - b^2 = 0$

set $t = \frac{b}{c}$

$(t, c) \longmapsto (b = tc,\ c)$

$y^2 - (1 - t(t-1))xy - t(t-t^2)y = x^3 - t(t-t^2)x^2$

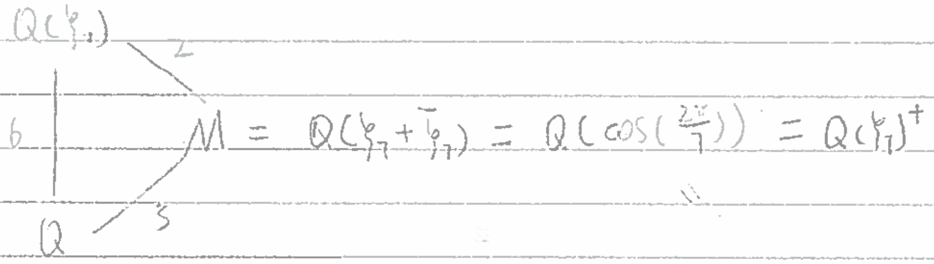
* Disc't in t,

$\Delta = t^7 (t-1)^7 \underbrace{(t^3 - 8t^2 + 5t + 1)}$

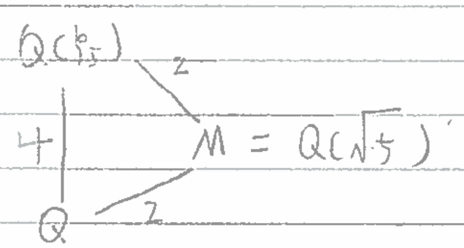
deg 3, with deg disc of power 7

N	poly deg	poly disc	field
5	2	5	$Q(\sqrt{5})$
7	3	7	$Q(\zeta_7)^+$

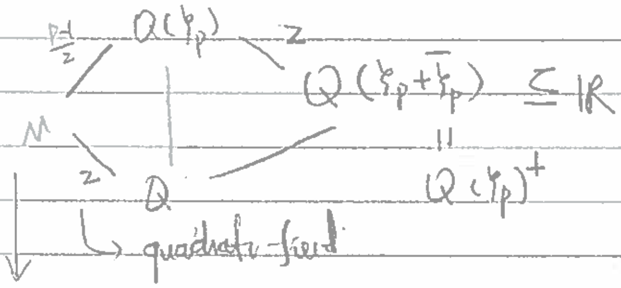
→ give disc't to recog the field



(☆) Galois group is
(Only ramification at 7)

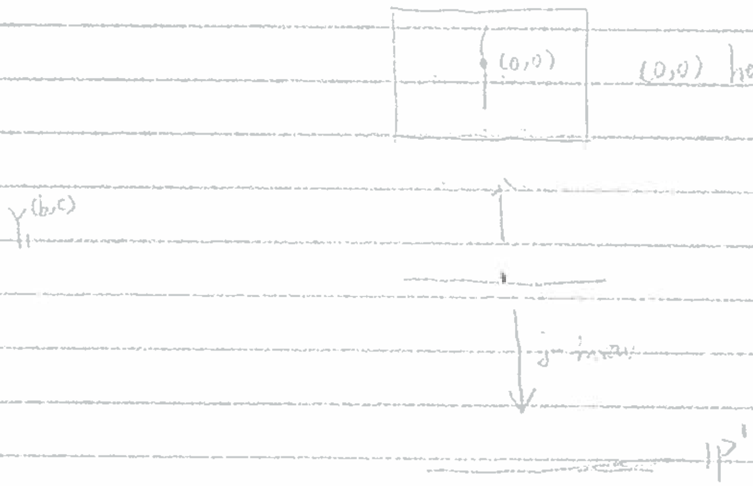


cos 5



* Consider a K with char $K = p$ and the curve $Y_1^{(b,c)}(p)$.

(0,0) has exact order p.



no point of order p is supersingular

Only finite many elliptic curve has no pts of order p

We have two remark.

① The number of of j-invariant of supersingular must be finite

② all these j-invariant must be alge over $\mathbb{F}_p$ (In fact in $\mathbb{F}_{p^2}$)

16th/Oct/18 Tue.

$\mathcal{E}$ - family $\qquad y^2+(1-c)xy-by = x^3-bx^2$

$\downarrow \qquad\qquad\qquad \downarrow$

$Y_1^{(b,c)}(N) \subseteq (b,c)$ plane.

Say $N=p$ prime.

If Tate normal form is over $p/p\mathbb{Z}$,

$P=(0,0)$, $[2]P = \ldots$ are all pts.

with coordinate in rational fcn in b & c, with coeff in $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z}(b,c) = \text{f.f } \mathbb{Z}/p\mathbb{Z}[b,c]$.

To get an equation for $Y_1^{(b,c)}(p)$, in (b,c) plane

We start by equaling

$[-2]P = [p-2]P$ or $[-\frac{p-1}{2}]P = [\frac{p+1}{2}]P$ we have $[p]P = \text{"}\infty\text{"}$

☆ From this, we get a plane curve (the equation) with coeff in $\mathbb{Z}/p\mathbb{Z}$

$Y_1^{(b,c)}(p) \subset$ plane curve $\subset (b,c)$ plane.

↪ (may not fixed) $\qquad$ ↓ j invariant

$\mathbb{P}^1$

$N=5p$ $\qquad$ ↪ component with order 5 / p / $5p$

* Assume two different pts in $Y_1^{(b,c)}(p)$, we have diff j-inv, these pts lie on the same connected component in $Y_1^{(b,c)}(p)$, then the j invariant map

$$Y_1^{(b,c)}(p)(\bar{k}) \longrightarrow \mathbb{P}^1(\bar{k})$$

only misses finite many pts in $\mathbb{P}^1(\bar{k})$

If there exist an elliptic curve E/k, with $E[p](\bar{k}) = (0)$, then the j-invariant is not in the image of above j map.

Moreover, it is in $\mathbb{F}_p$, because the map is defined in $\mathbb{F}_p$.

Rk. The curve $Y_1^{(b,c)}(N)$ comes with a natural automorphisms.

On the level of pts

$Y_1^{(b,c)}(N)(k) = \{ E/k, P \in E(k) \text{ of order } N \} / \text{isom}$

$\{f(a,b)=0\} = Y_1^{(b,c)}(N)(k)$ b → g(b,c), c → h(b,c)

↓ ↓ W_m

$\{f(a,b)=0\} = Y_1^{(b,c)}(N)(k)$

We want $f(g(b,c), h(b,c)) = 0$

☆ Done the exercise,

$(E(k), P \in E(k)) \longrightarrow E_{(b,c)}, (0,0)$ in normal form

↓ (b,c)

$E(k), {}^{\tau}PE \longrightarrow (b', c')$ } same $(b,c) = (b', c')$

☆ Take $(E_{(b,c)}, (0,0)$ pt$) \longrightarrow (b,c)$

$(E_{(b,c)}, [2](0,0)$ pt$) \longrightarrow (b', c')$ pt

$b' = g(b,c)$, $c' = h(b,c)$

Assume 2 coprime to N

expect to have a $(b,c) \longmapsto (g(b,c), h(b,c))$

to produce a map $Y_1^{(b,c)}(N) \longrightarrow Y_1^{(b,c)}(N)$

☆ When N is prime, there are $\frac{N-1}{2}$ possible distinct W_m.

In this case, the set $\langle W_m,\ m$ coprime to $N \rangle \simeq \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$

$Y_1^{(b,c)}(N)$ $(E, p$ of order $N)$

↓ ← deg $\frac{N-1}{2}$

$Y^{(b,c)}(N)/W_m$ $(E,$ Subgroup of order N no generator specified$)$

Subgroup is $\langle p \rangle = \langle W_m(p) : \text{if } \gcd(m,N)=1 \rangle$

We have

$\frac{N-1}{2}$ $Y_1^{(b,c)}(N)$ (E, p) $(E[N](\bar{k})$ has N^2 pts$)$

$Y_0(N)$ deg $\frac{N^2-1}{2}$

↓ ↓

$$Y_1(N) \xrightarrow{\frac{N-1}{2}} Y_0(N) \xrightarrow{\deg N+1} \mathbb{P}^1, \qquad Y_1(N) \xrightarrow{j\text{-invariant}} \mathbb{P}^1$$

$\mathbb{P}^1 \leftarrow j(E)$

$\{E,$ subgroup of order N $\cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ in $E[N](\bar{k})\}/\text{iso}$

Only identify p & $-p$ here (Assume)

☆ The j-invariant map $X_1(N) \longrightarrow \mathbb{P}^1$, is ramified at $j=0$, $j=1728$ & $j=$"∞"

☆ Case $j=0$, $y^2=x^3+1$, in char $\neq 2,3$.

with auto: $\sigma: x \longmapsto \zeta_3 x$ $\quad$ $\zeta_3^2+\zeta_3+1=0$ cubic root of unity

$y \longmapsto -y$

σ has order 6 (→ orbit of σ^3)

Fix pt of σ, ∞ and no other

of σ^2, $(0,1)$, & $(0,-1)$ — they are the two pts of exact order 3

of σ^3, $(-\zeta_3,0)$, $(-\zeta_3^2,0)$, $(-1,0)$. → orbit of σ)

↳ pts of order 2.

Ex. $(0,1)$ & $(0,-1)$ are 2 pts of order 3 ☆

☆ Consider E

$\downarrow$ ← deg 6, since almost all pts has 6 distinct pts.

$E/\langle\sigma\rangle$ $\qquad |\langle\sigma\rangle|=6$.

Small orbit $\begin{cases} \{(0,-1), (0,1)\} \\ (-\zeta_3,0), (-\zeta_3^2,0), (-1,0) \end{cases}$

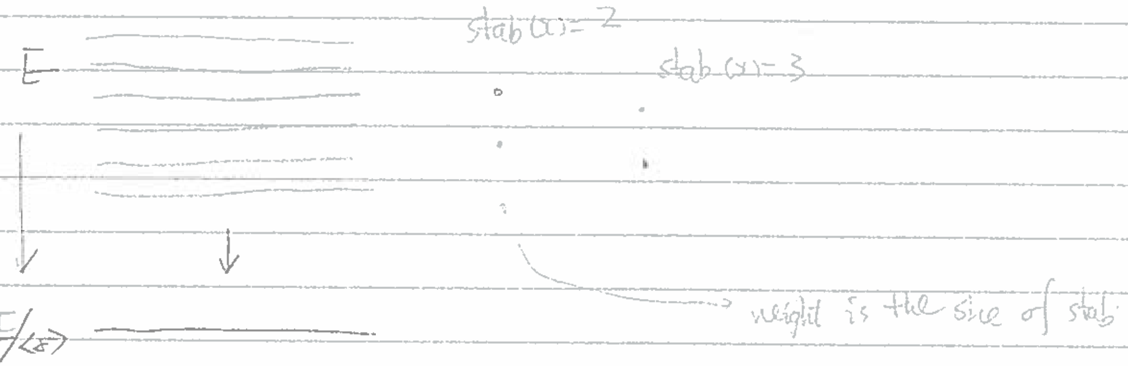
If G act X, $x \in X$

then $\mathrm{stab}(x) = \{g \in G \mid g(x)=x\}$

$\mathrm{Stab}(\ldots$

Riem–Hur form (in char $\neq 2,3$) coprime to the deg

$2g(E)-2 = \deg(2g(E/\langle\sigma\rangle)-2) +$ correcting term



Correcting term $= \sum_{x\in E(k)} (|stab(x)|-1)$

$2\cdot 1-2=0$

$= 6\cdot(2g(E/\langle\sigma\rangle)-2) + 3\cdot 1 + 2\cdot 2 + 5\ (\infty)$ (12)

$g(E/\langle\sigma\rangle)=0$

$(E_{j(E)=0},\ p)$ $N>3$

$\wr\!\!\mid$

$(E,\ \sigma(p))$

14th/Oct/18 Thr

Recall: $Y_1^{(b,c)}(N)$ → $Y_0^{(b,c)}(N) = Y_1^{(b,c)}(N) / \langle W_m, \gcd(m,N)=1 \rangle$ → $\mathbb{P}^1$

(E/k, $p \in E(N)(k)$ exact order N) → (E/k, subgp generated by p) → j(E)

if N prime: first map $\deg \frac{N-1}{2}$, second map $\deg N+1$; composite $\deg \frac{N^2-1}{2}$ = num# of pts of exact order N in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$

Question: W_m is defined as follows:

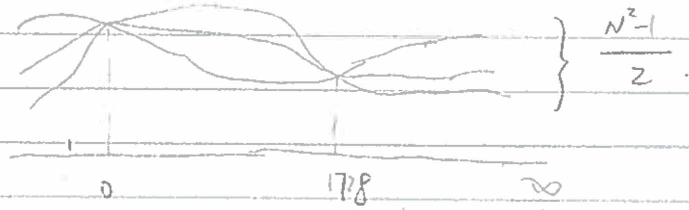
start $y^2 + (1-c)xy - by = x^3 - bx^2$ $\quad p = (0,0)$

Then consider the same curve $E(b,c)$ with pt with pts $[m]P$

Find the normal form of the pair $(E_{b,c}, [m]P)$, it corresp to $(b',c') = (g(b,c), h(b,c))$

☆ Does this map from (b,c) plane to itself has any interesting property

☆ Ramification: $Y_1(b,c)$ → $\mathbb{P}^1$



$Y_1^{(b,c)}(N)(k) \simeq \{ E/k, \; p \in E(N)(k), \; p$ exact order $N \} / \sim$

$(E, p) \simeq (E', p')$

if $\exists \sigma : E \to E$ isom with $\sigma(p) = p'$

at $j=0$ & $j=1728$, we have more automorphs than just $[-1]$

$j=0$, Aut group is $\mathbb{Z}/6\mathbb{Z}$
$j=1728$, Aut group is $\mathbb{Z}/4\mathbb{Z}$ } over $\bar{k}$

☆ None of automorphism fix a torsion pt of order >3

over $j=0$, $\frac{N^2-1}{6}$ pts (and not $\frac{N^2-1}{2}$ pts

$j=1728$, $\frac{N^2-1}{4}$ pts

☆ Another research question:

Pick a favorite field k, which has a separable extension L/k, with $d := [L:k] > 1$

For instance, $L = \mathbb{Q}(\zeta_{17})$, so $d = 16$,

Qus: Find smooth curve X/k of low positive genus with a new point over L.

If X/k is given by $f(x,y) = 0$, $f(x,y) \in k[x,y]$

then $(a,b) \in Z_f(L)$ is a new pt. of $k(a,b) = L$.

☆ For $L = \mathbb{Q}(\zeta_{17})$, I do not know how to find an elliptic curve with a new pt over L.

☆ For $L = \mathbb{Q}(\zeta_{31})$

- should be easy to find an elliptic curve
- $g = 2, 3, 4$ open
- $g = 5$ 1 example.
- $g \geq 6$ (with Q. Liu) there are infinitely examples (for each g)

☆☆ Reduction of elliptic curve.

Thm. Let $X/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 1$. Then exist, for each prime p, a uniquely defined curve, $X_p/\mathbb{F}_p$, and the reduction map and a reduction map $X(\mathbb{Q}) \longrightarrow X_p(\mathbb{F}_p)$.

☆ [The curve $X_p/\mathbb{F}_p$ is the special fiber at p of the minimal regular model of X over $\mathbb{Z}$.]

This theorem involves a lot of Algeb Geo.

☆ We are going to study the reduction of elliptic curves using Wierstrass eq.

! △ A curve can have many different equations which produce different reductions.

Ex. $y^2 = x^3 + p^2$ (W. E.) (over $\mathbb{Q}$)

So mod p: $y^2 = x^3$ which is <

☆ But the same elliptic curve over $\mathbb{Q}$ is also given by: $Y^2 = pX^3 + 1$

$$\begin{cases} Y = \frac{y}{p} \\ X = \frac{x}{p} \end{cases}$$

$\Downarrow$ mod p

$Y^2 = 1$

If $p \neq 2$, then the red is two lines

☆ For elliptic curve, we have two other canonical reductions

(1) is in the above thm

(2) A special fiber of the Néron model $\mathcal{E}$ of $E/\mathbb{Q}$ at p.

(b) red is a group homo. / (c), $\mathcal{E}_p/\mathbb{F}_p$ is smooth.

☆ Using only Weierstrass equation, we can do the following

- Define a finite index subgp $E^0(\mathbb{Q}) \subseteq E(\mathbb{Q})$
- Define a curve $\widetilde{E}_p/\mathbb{F}_p$ with a group structure
- Define a group homomorphism $E^0(\mathbb{Q}) \longrightarrow \widetilde{E}_p(\mathbb{F}_p)$.

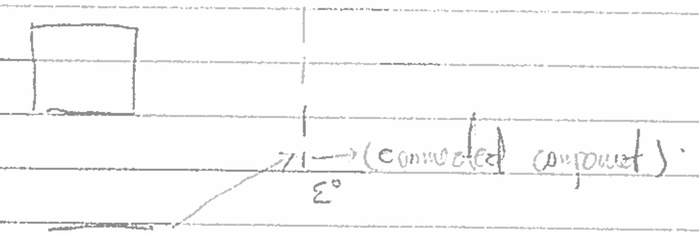
☆ How this relate to Néron model reduction?

$$\begin{array}{ccccc} E(\mathbb{Q}) & \longrightarrow & \mathcal{E}_p(\mathbb{F}_p) & \longrightarrow & \text{(may disconnected)} \\ \text{|U} & & \text{|U} & & \\ E^0(\mathbb{Q}) & \longrightarrow & \text{Its image} & \longrightarrow & \text{Connected component of } 0 \text{ in } \mathcal{E}_p(\mathbb{F}_p) \end{array}$$

(Silverman I)

Let $\mathcal{E}_p^0/\mathbb{F}_p$ denote the connected component of the identity. Then

Fact: $\text{red}(E^0(\mathbb{Q})) \subseteq \mathcal{E}_p^0(\mathbb{F}_p)$, and $\widetilde{E}_p \simeq \mathcal{E}_p(\mathbb{F}_p)$ over $\mathbb{F}_p$.



E.g. Let G/k given by $x^2 - dy^2 = 1$ (not elliptic curve).

$G(k) \longrightarrow (k(\sqrt{d})^*, \cdot)$

$(x, y) \longmapsto x + \sqrt{d}\, y$ $\quad G(k) =$ set of norm 1 elements in $k(\sqrt{d})$

$(x,y)\cdot(x',y') := (xx' + dyy',\ xy' + x'y)$. identity $(1,0)$.

Inverse $(x,y) \longmapsto (x,-y)$.

K dvR, with uniformizer π, → field of fractions

Say O_K is PID with ff$(O_K) = K$. Say $d = \pi \cdot d'$ with (π) prime ideal

Then the reduction G_π/k is defined by $x^2 - dy^2 = 1 \mod \pi$.

where residue field $k = O_K/(\pi)$

Say $\text{char}(k) \neq 2$, so $x^2 = 1 \Rightarrow (x-1)(x+1) = 0 \Rightarrow$ two lines.

We have reduction map $G(O_K) \xrightarrow{\text{mod } \pi} G_\pi(k)$ is a group homomorphism

$(x,y) \longmapsto (\bar{x}, \bar{y})$, $\quad x = -1$

$(1,0)$ goes to two lines

$$\begin{array}{ccc} G(O_K) & \longrightarrow & G_\pi(k) \\ \downarrow & & \\ (\bar{1},\bar{0}) & & \end{array}$$

$x = 1$ → connected component of $(\bar{1},\bar{0})$, G_π^0

Ex. $\to G_\pi^0(k) \to G_\pi(k) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$