TEOREMA DI MAZUR

Note Title 13/10/2023

A. Gallese
13/10/2023

Introduzione

Teo $E/\mathbb{Q}$ curva ellittica. $E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/_{n}\mathbb{Z} & n = 1, 2, \dots, 10, 12 \\ \mathbb{Z}/_{2}\mathbb{Z} \times \mathbb{Z}/_{2n}\mathbb{Z} & n = 1, 2, 3, 4 \end{cases}$

Supponiamo di avere $E/\mathbb{Q}$ e $P \in E(\mathbb{Q})_{tors}$ di ordine > 3,

cioè $[2]P \neq O$, $[3]P \neq O$

Forma normale di Tate

Obiettivo: $E: y^2 + uxy + vy = x^3 + vx^2 \qquad P = (0, 0)$

Come al solito, mettiamo O_E in $[0 : 1 : 0]$.

Step 0: $y^2 + Axy + By = x^3 + Cx^2 + Dx + E$

Step 1: Sostituendo $x \rightsquigarrow x - x(P)$, $y \longrightarrow y - y(P)$

possiamo supporre $P = (0,0)$ e quindi il coeff. $E = 0$

Step 2: Sostituendo y con $y + tx$ otteniamo $(0,0) \mapsto (0,0)$ e

$$E \mapsto y^2 + 2tx + t^2x^2 + Axy + Atx^2 + By + \underbrace{Btx} = x^3 + Cx^2 + \underbrace{Dx}$$

Scelgo $t = D/B$ (se $B = 0$, il pto $(0,0)$ e' di 2-torsione)

e questo annulla il termine in x. Questo assicura che

la tg in $(0,0)$ sia $y = 0$

Step 3: Sostituendo $x \mapsto r^2 x$, $y \mapsto r^3 y$ e scegliendo $r = B/C$,

$(0,0) \mapsto (0,0)$ ed E diventa data da un'eqz. con

$B = C$. Notiamo che $C = 0 \iff [3](0,0) = O_E$.

Discriminante in forma di Tate Dovremmo imporre $\Delta \neq 0$; è un'espr. bruttissima, evitiamo.

Calcoliamo i multipli di P

$$[-2]P = \begin{cases} y=0 & \text{tangente} \\ x^3+vx^2=0 & E \end{cases} \rightsquigarrow [-2]P = (-v, 0)$$

$$\Rightarrow [2]P = (-v, v(u-1))$$

Per $[3]P$: la retta per P e $2P$ è $y = -(u-1)x$

$$\rightsquigarrow [3]P = (1-u, u-v-1)$$

$X_1(5)$ $\quad [5]P = 0$ "$\Leftrightarrow$" $x(2P) = x(3P) \Leftrightarrow \boxed{-v = 1-u}$

$\hookrightarrow \simeq Y_1(5)$

$$E_v: \; y^2 + (v+1)xy + vy = x^3 + vx^2$$

$$\Delta_E = -v^5 \cdot (v^2 + 11v - 1)$$

$$j : X_1(5) \longrightarrow X(1) \simeq \mathbb{P}^1$$
$$v \longmapsto j(E_v) = \text{funz. raz. di grado } 12$$

Oss. Perché 12? $E[5](\overline{\mathbb{Q}}) \simeq (\mathbb{Z}/5\mathbb{Z})^2$; ci sono 24 pti di ordine esattamente 5, ma sono identificati a coppie perché $(E, P) \simeq (E, [-1]P)$

Cosa succede quando cambio pto di 5-torsione?

$$\begin{array}{ccc} (E, P) & \longmapsto & (E, [2]P) \\ \downarrow & & \downarrow \\ (u, v) & & (u', v') \end{array}$$

$$[2]P = (-v,\ v(u-1))$$

Dovrei traslare $[2]P$ in $(0,0)$, poi raddrizzare la tg, e infine riscalare. Il risultato è

$$(u,v) = (v+1,\ v) \longmapsto (1 - 1/v,\ -1/v)$$

Se itero, ottengo $(1+v,\ v) \longleftrightarrow (E,\ [4]P) = (E,\ [-1]P) \simeq (E, P)$

7 - torsione

Uno calcola $[4]P = \left(\dfrac{-v(u-v-1)}{(1-u)^2},\ -\dfrac{v^2(2-3u+u^2+v)}{(-1+u)^3} \right)$

Imponendo $x([3]P) = x([4]P)$ troviamo un'eqz. per $X_1(7)$,

$$(1-u)^3 = -v(u-v-1)$$

Questa è una cubica singolare: $(1,0)$ è un pto doppio, e parametrizzando al solito modo $\begin{cases} u=t \\ v=s(t-1) \end{cases}$ le rette passanti per $(1,0)$ si trova una parametrizz. di $X_1(7)$:

$$s^2+t=1+s \Rightarrow u=t=1+s-s^2$$

$$v=s(t-1)=s(s-s^2)$$

$$=s^2(1-s)$$

$\Rightarrow \quad X_1(7)\simeq \mathbb{P}^1 \Rightarrow \exists$ infinite $E/\mathbb{Q}$ con un pto di 7-torsione.

$$E_s: \quad y^2+(1+s-s^2)xy+s^2(1-s)y=x^3+s^2(1-s)x^2$$

$$\Delta_{E_s} = s^7 (s-1)^7 (s^3 + 8s^2 + 5s + 1)$$

$$j : X_1(7) \longrightarrow X(1) \quad \text{ha grado } 24$$

11 - torsione

Dopo pacchi di conti e risoluzione delle singolarità,

$$X_1(11) \; : \; v^2 - v = u^3 - u^2$$

Che è una curva ellittica in forma normale di Tate, con parametri $(0,-1) \rightsquigarrow (0,0)$ è un pto di 5-torsione su $X_1(11)$! Si controlla che per i pti di 5-torsione la corrispondente curva in forma normale di Tate è singolare.

$\rightsquigarrow$ per ora non abbiamo trovato pti di 11-torsione su curve ellittiche su $\mathbb{Q}$.

Per Mordell-Weil, $X_1(11)(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$. Oggi ci calcoliamo T.

Teorema $E/\mathbb{Q}$ curva ellittica, N intero, $\underbrace{2 \nmid N}_{\text{superfluo}}$, p primo, $p \nmid \Delta_E$ e $p \nmid N$. Allora $E(\mathbb{Q})[N] \hookrightarrow \tilde{E}(\mathbb{F}_p)$

Applicazione Posso calcolare facilmente $\# \tilde{E}(\mathbb{F}_p)$. Nel nostro caso, $\# \tilde{E}(\mathbb{F}_3) = 5$ e $\# \tilde{E}(\mathbb{F}_7) = 10$, da cui $\# E(\mathbb{Q})_{tors} \mid 5$.

($E = X_1(11)$ nella riga qui sopra)

Dim finta del teorema

1) Estendendo il campo base, posso assumere $E[N](K) = E[N](\overline{\mathbb{Q}})$

ed $\# \tilde{E}[N](\mathcal{O}_K/\mathfrak{p}) = N^2$

2) So che $\# E[N](K) = N^2$ e $\# E[N](\mathcal{O}_K/\mathfrak{p}) = N^2$.

Basta dim che $E[N](K) \longrightarrow E[N](\mathcal{O}_K/\mathfrak{p})$ è surgettiva

3) Polinomi di divisione: $\psi_N(x,y)$ t.c. $\psi_N(x,y) \in \mathbb{Z}[x,y]$

$$[N](x,y) = \left(\frac{\phi_N}{\psi_N(x,y)^2}, \frac{\omega_N}{\psi_N(x,y)^3} \right)$$

In realtà, $\psi_N(x,y) \in \mathbb{Z}[x]$ o $y\,\mathbb{Z}[x]$, e

$$\psi_N(x) = 0 \quad \text{è} \quad E[N]$$

4) Vale $\deg \psi_N = \frac{N^2-1}{2}$

5) Ora è il lemma di Hensel: $\psi_N(x) = 0$ ha $\frac{N^2-1}{2}$ radici

Sia su K che su $\mathcal{O}_K/\mathfrak{p}$. Queste radici sono DISTINTE, altrimenti non ho abbastanza punti di N-torsione, per cui si sollevano <u>in modo unico</u> in caratteristica 0. Ma questa è proprio la tesi (dopo aver controllato che le coord y siano anch'esse distinte) $\square$

Dim un po' più formale $E[N]$ è étale su $\operatorname{Spec} \mathbb{Z}\left[\frac{1}{N\Delta_E}\right]$; e ora si ragiona come prima, ma è più comodo :)

20/10/2023
L. Furio

Sottogruppi che si realizzano come $E(\mathbb{Q})_{tors}$

Supponiamo che un gruppo della lista di Mazur non occorra infinite volte. Diciamo ad esempio che $H = \mathbb{Z}/5\mathbb{Z}$ si verifichi solo finite volte. Allora (a posteriori di Mazur) si deve verificare che (con finite eccezioni) ogni volta che $H \subseteq E(\mathbb{Q})_{tors}$ si ha $\mathbb{Z}/10\mathbb{Z} \subseteq E(\mathbb{Q})_{tors}$. Ma questo vuol dire

$$X_{10}(\mathbb{Q}) \longrightarrow X_5(\mathbb{Q})$$

surgettiva con finite eccezioni, che però è impossibile perché $\mathbb{P}^1 \simeq X_{10} \longrightarrow X_5 \simeq \mathbb{P}^1$ ha grado >1.

Hilbert

For $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, look at $y^2 = x \cdot g(x)$

$$y^2 + uxy + vy = x^3$$

Gruppi prodotto

Assumiamo $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ con $n \mid m$.

Vogliamo mostrare $n = 2$

Accoppiamento di Weil

Fissiamo n e supponiamo $\operatorname{char} K \nmid n$

Vogliamo definire $e_n : E[n] \times E[n] \longrightarrow \mu_n$

Fissiamo $T, S \in E[n]$. Ricordiamo $E(\bar{K}) \xrightarrow{\sim} \operatorname{Pic}^0(E)$

$$P \longmapsto [(P) - (\infty)]$$

$$\Rightarrow \quad n\left[(T)-(\infty)\right] = 0 \quad \Rightarrow \quad n(T) - n(\infty) = \operatorname{div} f$$

Consideriamo $\operatorname{div}\left(f\circ[n] \right) = n\left(\sum_{P:\, nP=T} (P) - \sum_{P\in E[n]} (P) \right)$

$$= n\left(\sum_{P\in E[n]} \left((P+P_0) - (P) \right) \right) \qquad \text{dove } nP_0 = T$$

D'altro canto, $\underset{\substack{\text{somma} \\ \text{in } E}}{\sum_{P\in E[n]}} (P+P_0) = \underset{\underset{\infty}{\parallel}}{n^2 P_0} + \sum_{P\in E[n]} P$

$$\Rightarrow \quad \sum_{P\in E[n]} \left((P+P_0) - (P) \right) = 0 \quad \text{in } E$$

$$\Rightarrow \quad \operatorname{div}\left(f\circ[n] \right) = \operatorname{div}\left(g^n \right) \Rightarrow \frac{f\circ[n]}{g^n} \text{ costante}$$

$\Rightarrow$ wlog, a meno di riscalare g, $f\circ[n] = g^n$

Ora definiamo $e_n(T, S) = \dfrac{g(X+S)}{g(X)}$

Notiamo che $\left(\dfrac{g(X+S)}{g(X)}\right)^n = \dfrac{(f \circ [n])(X+S)}{(f\circ[n])(X)} = \dfrac{f\circ[n](X)}{f\circ[n](X)} = 1,$

quindi $\dfrac{g(X+S)}{g(X)}$ è costante ed è una radice n-esima di 1.

Teo e_N è bilineare, alternante, Galois-equivariante, e non-degenere

- $\sigma(e_N(S,T)) = e_N(\sigma(S), \sigma(T)) \quad \forall \sigma \in Gal(\overline{K}/K)$
- $e_N(S,T) = e_N(T,S)^{-1}$
- $e_N(S_1+S_2, T) = e_N(S_1,T)\, e_N(S_2,T)$
- $e_N(S,T) = 1 \quad \forall T \in E[N] \Rightarrow S = 0$

Oss $\langle P, Q \rangle = E[N] \iff e_N(P,Q)$ genera μ_N

Applicazione $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$ con $n \mid m$

$\Rightarrow \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \subseteq E(\mathbb{Q})_{tors}$

$\Rightarrow E[n] \subseteq E(\mathbb{Q})_{tors}$

$\Rightarrow$ presa una base P, Q di $E[n]$, $\forall \sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$$\sigma(e_n(P,Q)) = e_n(\sigma P, \sigma Q) = e_n(P,Q)$$

$\Rightarrow e_n(P,Q) \in \mathbb{Q}$, ma è una radice primitiva n-esima, quindi $n \leq 2$.

Guardiamo i gruppi $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$.

(*) $E(\mathbb{Q})_{tors} \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ con $1 \le n \le 4$

Il caso $n=1$ è rognoso ($X(2)$ non è fine)

Se E soddisfa (*), allora dà un pto razionale sia su $X_1(2n)$ sia su $X(2)$ $\rightsquigarrow$ vorrei i pti su

$$\begin{tikzcd}
 & X_1(2n) \times_{X(1)} X(2) \arrow[dl] \arrow[dr] & \\
X_1(2n) \arrow[dr] & & X(2) \arrow[dl] \\
 & X(1) &
\end{tikzcd}$$

Consideriamo la seguente variante. Prendiamo un pto raz. di $X_1(2n)$, cioè $E/\mathbb{Q}$ con $P \in E[2n](\mathbb{Q})$

$\boxed{n=2}$ $E: \; y^2 + uxy + vy = x^3 + vx^2$ $\qquad P = (0,0)$

$$2P = (-v, \; v(u-1))$$

$$3P = (1-u, \; u-v-1)$$

$$4P = \left(\frac{-v(u-v-1)}{(1-u)^2}, \; \frac{-v(2-3u+u^2+v)}{(-1+u)^3} \right)$$

Ora $4P = 0 \iff u = 1$

La curva univ su $X_1(4)$ è $y^2 + xy + vy = x^3 + vx^2$,

o equivalentemente (a meno di traslazioni)

$(u=1)$ $$y^2 = x^3 + \frac{(u^2+4v)}{4}x^2 + \frac{uv}{2}x + \frac{v^2}{4}$$

Per $u=1$, $x=-v$ è soluzione, e

$$y^2 = (x+v)\left(x^2 + \frac{1}{4}x + \frac{v}{4}\right)$$

ha tutta la 2-tors def su $\mathbb{Q}$ sse $\frac{1}{16} - v = \square$. Questa è ancora $\mathbb{P}^1$!

$\boxed{m=3}$ $4P = -2P \longrightarrow x(4P) = x(2P)$

$$\Downarrow$$

$$-\frac{v(u-v-1)}{(1-u)^2} = -v$$

Due componenti: $v=0$ (che dà una curva singolare) e

$$u-v-1 = (1-u)^2$$

e cioè $\quad V = -u^2 + 3u - 2$

Stessi conti di prima $\rightsquigarrow$

$$y^2 = x^3 + \frac{-3u^2+12u-8}{4} x^2 + \frac{-u^3+3u^2-2u}{2} x + \frac{(u^2-3u+2)^2}{4}$$

e il pto $(-u+1, 0)$ è razionale

$$y^2 = (x+u-1)\left(x^2 + \frac{-3u^2+8u-4}{4} x + \frac{(u-1)(u-2)^2}{4}\right)$$

$$d^2 = \Delta = \left(\frac{-3u^2+8u-4}{2}\right)^2 - (u-1)(u-2)^2 = (u-2)^2\left[\left(\frac{3u-2}{2}\right)^2 - 4(u-1)\right]$$

che è ancora $\mathbb{P}^1$. Parametrizzando,

$$u = \frac{1}{54K} - \frac{4K}{3} + 8/9$$

E perché non $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$?

Lemma Se $E/\mathbb{Q}$ è t.c. $E(\mathbb{Q})_{tors} \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (risp. $\supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$), allora $\exists\, E'/\mathbb{Q}$ con isogenia $E \to E'$ di grado 2, tale che E' ammette un'isog. ciclica di grado 4 (risp. 8)

Dim. Scrivo $E[2] = \langle P, Q \rangle$

$$\begin{tikzcd}
 & E \arrow[dl, "f"'] \arrow[dr, "g"] & \\
E' := E/\langle P \rangle & & E/\langle Q \rangle
\end{tikzcd}$$

Allora $g \circ f^\vee$ è l'isog. cercata, perché $f^\vee(E'[2]) \subseteq \langle P \rangle$ e quindi $g \circ f^\vee$ non ammazza tutto $E'[2]$ $\square$

Cor No $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Dim Se sì, c'è $E' \sim E$ con una 20- o 24-isog. definita su $\mathbb{Q}$, che però non esiste perché sappiamo studiare $X_0(20)$, $X_0(24)$. $\square$

27/10/2023
S. Boscardin

Riduzioni di curve ellittiche su campi locali

K = campo locale completo rispetto a $|\cdot|$, R anello degli interi, $\mathfrak{m}$ = ideale mass. di R, $k = R/\mathfrak{m}$, E/K curv. ellittica

$$(*) \quad E: \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \qquad a_i \in K$$

Oss Il cambio di coord $x' = u^{-2}x$, $y' = u^{-3}y$ dà $a_i' = u^i a_i$, quindi possiamo supporre $a_i \in R$

Def. L'eqz. $(*)$ è *minimale* se $a_i \in R$ e $v(\Delta)$ is minimal among all such equations.

Rmk Δ is a polynomial with integer coeffs in the a_i (homog. of weighted degree 12), hence $a_i \in R \Rightarrow v(\Delta) \geq 0$

Def.

	wt
c_4	4
c_6	6
Δ	12
j	0

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \qquad j = \frac{c_4^3}{\Delta}$$

$$E: \quad y^2 = x^3 - 27c_4 x - 54 c_6$$

Lemma All Weierstrass eqns are obtained from one another via

$$(**) \begin{cases} x' = u^2 x + r \\ y' = u^3 y + u^2 s x + t \end{cases} \qquad r, s, t, u$$

Under this change of coords, $\Delta' = u^{-12} \Delta$

$\Rightarrow$ $v(\Delta)$ is well-def'd mod 12

Rmk A Weierstrass eqn is minimal $\iff v(\Delta) < 12$ or $v(c_4) < 4$
(For $\Rightarrow$, we assume char $k \neq 2,3$)

Def. Let $E: y^2 + a_1 xy + a_3 y = x^3 + \dots$ be a minimal Weierstr. eqn. The reduced curve $\tilde{E}/k$ is the curve with eqn

$$y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \dots \qquad \tilde{a}_i = a_i \bmod \mathfrak{m}$$

Any two minimal eqs give the same reduced curve: a change of variables (**) between two MINIMAL integral eqs has $r, s, t, u \in R$, $u \in R^\times$, and so gives a well-defined change of variables between the reduced curves.

There is a natural map $E(K) \longrightarrow \tilde{E}(k)$

$[x_0 : x_1 : x_2] \mapsto [\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2]$

$x_0, x_1, x_2 \in R$, not all in πR

Def $E_0(K) = \{ P \in E(K) : \tilde{P} \text{ is non-singular} \}$

$E_1(K) = \{ P \in E(K) : \tilde{P} = \tilde{\infty} \} \subseteq E_0(K) \subseteq E(K)$

Ex. sequence $0 \to E_1(K) \to E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0$

Hensel's lemma

If $(\alpha, \beta) \in \tilde{E}_{ns}(k)$, at least one derivative of the def. polyn. $F(x,y) = 0$ does not vanish; let's say $\frac{\partial F}{\partial x}(\alpha,\beta) \neq 0$

Then: fix $y_0 \in R$ st $\overline{y_0} = \beta$, and then use Hensel to solve $F(x, y_0) = 0$ (note that $F(\alpha, \tilde{y}_0) = 0$
$F'(\alpha, \tilde{y}_0) \neq 0$)

Structure of $E_1(K)$, formal groups

We study E around ∞. Suppose E is given by

$$E : \quad F(X, Y, Z) = 0$$

We would like to write $Y = F(X, Z)$ as a power series converging for $|X|$, $|Z|$ small.

Change of variables: $z = -X/Y$, $w = -1/Y$

$\rightsquigarrow$ E becomes $w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3 =: g(z,w)$

Now we iteratively replace w with and evaluate at $w=0$.

We get a seqn of elements in

$$\mathbb{Z}[a_1, \dots, a_6][[z]]$$

that converges to $w = w(z)$ [Since the seq. is Cauchy].

This power series satisfies $w(z) = f(z, w(z))$

$$\Rightarrow \quad \begin{matrix} x(z) = z/w(z) \\ \\ y(z) = -1/w(z) \end{matrix} \quad \in \quad 1/z^3\, \mathbb{Z}[a_i][[z]]$$

Def (Formal group) A FORMAL GROUP OVER R is a power series $\lambda(z_1, z_2) \in R[[z_1, z_2]]$ s.t.

1) $\lambda(z_1, \lambda(z_2, z_3)) = \lambda(\lambda(z_1, z_2), z_3)$

2) $\lambda(z_1, z_2) = \lambda(z_2, z_1)$

3) $\lambda(z_1, z_2) \equiv z_1 + z_2 \mod (z_1, z_2)^2$

4) $\lambda(z_1, 0) = z_1$

In our context, we get λ from

$$\left(x(z_1), y(z_1)\right) + \left(x(z_2), y(z_2)\right) = \left(x(\lambda(z_1, z_2)), y(\lambda(z_1, z_2))\right).$$

It looks like

$$\lambda(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - \ldots$$

We can then construct an actual group $\lambda(\mathfrak{m})$: the underlying set is $\mathfrak{M}$ and the operation is

$$x_1 \oplus x_2 = \lambda(x_1, x_2) \in \mathfrak{M}$$

Thm $E_1(K) \simeq \hat{E}(K) := \lambda(M)$

Pf $(x(z), y(z)) \longleftarrow\!\!| \; z$

$$\left(\frac{z}{w(z)}, -1/w(z)\right) = [z : -1 : w(z)] \equiv [0 : 1 : 0] \mod \mathfrak{M}$$

(To be more precise, $v(w(z)) = 3\,v(z)$ if $z \in \mathfrak{M}$)

In the other direction, $(x, y) \longmapsto -x/y$ $\square$

Def E/K has GOOD REDUCTION if $\tilde{E}$ is non-singular,
MULTIPLICATIVE REDUCTION if $\tilde{E}$ has a node, and
ADDITIVE REDUCTION if $\tilde{E}$ has a cusp.

Rmk Good red $\iff$ $v(\Delta_{min}) = 0$

Mult red $\iff$ $v(\Delta_{min}) > 0$ but $v(c_4) = 0$

Add red $\iff$ $v(\Delta_{min}) > 0$, $v(c_{4,min}) > 0$

In all cases, $\tilde{E}_{ns}$ is a group; specifically

- an elliptic curve, if E has good red.
- an algebraic torus, if E has mult. red
- $\mathbb{G}_a$, " " " add. red.

Def. E has POTENTIALLY GOOD REDUCTION if $\exists K'/K$ (finite field extn) st E/K' has good reduction.

Prop (a) If K'/K is unramified, then $E_{K'}$ has the same reduction type as E_K

(b) If E/K has mult / good red, then the same holds for $E_{K'}$

(c) $\exists K'/K$ st $E_{K'}$ has either good or multiplicative reduction

Prop. E has pot good reduction $\iff$ $j(E) \in R$

Proof $\boxed{\Rightarrow}$ Trivial: compute j using a min. eqn. Then

$j = (\text{integers}) / \Delta$, so $v(j) \geq 0$

$\boxed{\Leftarrow}$ Suppose char $k \neq 2$, $E: y^2 = x(x-1)(x-\lambda)$ over some extension, $\lambda \neq 0,1$. Then

$$(1-\lambda(1-\lambda))^3 - j \cdot \lambda^2(1-\lambda)^2 = 0$$

Assuming $v(j) \geq 0$, we obtain $\lambda \in R$, $\lambda \neq 0,1$ (111), and therefore E has good reduction. $\square$

Thm For every ell. curve E/K, the group $E(K)/E_0(K)$ is finite

Pf when k is finite

Note that k finite $\Leftrightarrow$ K locally cpt $\Leftrightarrow$ R compact.

Embed $E(K) \subset \mathbb{P}^2(K)$. Translations and $\pi : E(K) \to \tilde{E}(k)$ are continuous. Then $E(K)$ is the union of open sets of the form $\tau_p(E_0)$

Note that $E_0 = \bigcup_{p \text{ nonsing}} \pi^{-1}(\{p\})$ is open.

By compactness, $E(K) \subseteq \bigcup_{i=1}^{N} \tau_{p_i} E_0$ ◻

The Néron - Ogg - Shafarevich criterion

The following are equivalent:

(a) E has good reduction

(b) $E[m]$ is unramified $\forall m$ st $(m, \operatorname{char} k) = 1$

(c) the Tate module $T_\ell E$ is unramified for some prime $\ell \neq \operatorname{char} k$

(d) $E[m]$ is unramified for infinitely many integers m coprime to $\operatorname{char} k$

Def $T_\ell E = \varprojlim E[\ell^n]$

Def. $Gal(\bar{K}/K) \curvearrowright E[m]$ and on $T_\ell E$. We say that these modules are UNRAMIFIED if the inertia subgroup I acts trivially

Proof

a) $\Rightarrow$ b) We have to show that

$$\sigma(P) = P \quad \forall \sigma \in I, \quad \forall P \in E[m]$$

Recall that $E(R)_{\text{tors prime to } p} \hookrightarrow \tilde{E}(k)$ if $\tilde{E}$ is non-sing

Side note: proof of this injection

$$0 \to E_1(K) \to E(K) \to \tilde{E}(k) \to 0$$

$$\begin{array}{c} \wr\!\wr \\ \hat{E}(m) \end{array},$$

and one can show that $\hat{E}(\mathfrak{m})$ has no ℓ-torsion for any prime $\ell \neq \operatorname{char} k$

Now: $\sigma(P) - P \in E[m]$ reduces to $\sigma(\tilde{P}) - \tilde{P} = \tilde{P} - \tilde{P} = 0$.

By injectivity, $\sigma(P) = P$.

b) $\Rightarrow$ c) $\Rightarrow$ (d) easy

d) $\Rightarrow$ a) Let $K^{nr} = \overline{K}^{I}$ be the max. unramified ext^n.

Choose m s.t. (i) $(m, \operatorname{char} k) = 1$, (ii) $m > E(K^{nr}) / E_0(K^{nr})$

and (iii) $E[m]$ is unramified.

We have short exact sequences

$$(\star) \quad 0 \longrightarrow E_0(K^{nr}) \longrightarrow E(K^{nr}) \longrightarrow E(K^{nr})/E_0(K^{nr}) \longrightarrow 0$$

$$(\star\star) \quad 0 \longrightarrow E_1(K^{nr}) \longrightarrow E_0(K^{nr}) \longrightarrow \tilde{E}_{ns}(\bar{k}) \longrightarrow 0$$

By (iii), $\underset{(\mathbb{Z}/m\mathbb{Z})^2}{\underset{\|}{E[m]}} \subseteq E(K^{nr})$. From $(\star)$ it follows that

for some $\ell \mid m$ we have $E[\ell] \subseteq E_0(K^{nr})$.

Now $(\star\star)$ + the fact that there is no ℓ-torsion in $E_1(K^{nr})$

shows that $(\mathbb{Z}/\ell\mathbb{Z})^2 \subset \tilde{E}_{ns}(\bar{k}) = \underset{\text{or } \bar{k}}{\bar{k}^\times}$, contradiction if

$E_{K^{nr}}$ has bad red^n. Hence $E_{K^{nr}}$ has good red $\Rightarrow$ E_K also

has good red^n. $\square$

03/11/2023
R. Deferrari

Mordell - Weil

Thm K = nb field, E/K ell. curve. The group $E(K)$ is finitely generated

Thm (descent) A = ab. group, $m \in \mathbb{N}_{\geq 2}$. Suppose

(i) A/mA is finite

(ii) $\exists\ h : A \longrightarrow \mathbb{R}$ st

(a) $\forall Q \in A \quad \exists\ c_1 = c_1(Q)$ st $\forall P \in A$

$$h(P+Q) \leq 2h(P) + c_1$$

(b) $\exists\ c_2$ st $\forall P \in A \qquad h(mP) \geq m^2 h(P) - c_2$

(c) $\forall D \in \mathbb{R}, \quad \{P \in A \mid h(P) \leq D\}$ is finite

Then A is finitely generated

Proof Let $Q_1, \dots, Q_r$ be representatives of A/mA.

Every pt P in A is of the form $Q_i + mP'$. Define.

$P_0 = P, \qquad P_k = Q_{i_k} + m P_{k+1}$

The height of P_n satisfies:

$$h(P_n) \leq \frac{1}{m^2}\left(h(mP) + c_2\right) = \frac{1}{m^2}\left(h(P_{n-1} - Q_{i_{n-1}}) + C_2\right)$$

Let C_1 be $\max C_1(-Q_i)$. Then

$$h(P_{n-1} - Q_{i_{n-1}}) \leq 2h(P_{n-1}) + C_1,$$

so $h(P_n) \leq \frac{1}{m^2}\left(2h(P_{n-1}) + C_1 + C_2\right)$.

Iterating, $h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(\sum_{k=0}^{n-1}\left(\frac{2}{m^2}\right)^k\right)(C_1+C_2)$

$$\leq \left(\frac{2}{m^2}\right)^n h(P) + (C_1+C_2)\cdot\frac{1}{m^2-2}$$

In particular, for $n \gg 0$, $h(P_n) \leq 1 + \frac{C_1+C_2}{m^2-2} =: C_3+1$

On the other hand,

$$P = Q_{i_0} + mP_1 = Q_{i_0} + m(Q_{i_1} + mP_2) = \cdots$$

$$= \sum_{j=0}^{n-1} m^j Q_{i_j} + m^n P_n,$$

so every P is a combination of pts in the finite set

$$\{Q_i\} \cup \{P \mid h(P) \leq C_3 + 1\}$$ $\square$

Thm (weak Mordell-Weil) $E(K)/mE(K)$ is finite

Def. Let $G := \mathrm{Gal}(\overline{K}/K)$. A G-module M is called DISCRETE if $G \times M \longrightarrow M$ is continuous (where M has the discrete topology). Equivalently, $\forall m \in M$, $\mathrm{Stab}_G(m)$ is a discrete G-module

Examples $E(\overline{K})$, $\overline{K}$, $\overline{K}^\times$

Def M a G-Mod. We set $M^G = \{m \in M \mid g \cdot m = m \ \forall g \in G\}$

The map $M \longmapsto M^G$ is a left-exact functor

$$(-)^G : \mathrm{Mod}_G \longrightarrow \mathrm{Ab}$$

We then have derived functors $H^q(G, M)$. We'll use that

$$H^1(G, M) = \frac{\left\{ \varphi : G \to M \;\middle|\; \varphi(ab) \overset{\varphi \text{ continuous}}{=} \varphi(a) + a\,\varphi(b) \right\}}{\left\{ \varphi : G \to M \;\middle|\; \exists\, m \in M : \varphi(\sigma) = \sigma m - m \right\}}$$

Properties

- If the action of G on A is trivial, $H^1(G, A) \cong \mathrm{Hom}(G, A)$
- $0 \to A \to B \to C \to 0$ exact seq. of discrete G-modules

$$\Rightarrow \quad 0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C)$$

$$B \ni b \longmapsto c \qquad \delta(c)(\sigma) = \sigma b - b \in A$$

Def. $A \in G$-mod, $A' \in G'$-mod, $f: G' \to G$, $g: A \to A'$.

(f, g) is a COMPATIBLE PAIR if g is G'-equivariant for the G'-mod structure on A given by f.

We have
$$H^1(G, A) \longrightarrow H^1(G', A')$$
$$[\varphi] \longmapsto [g \circ \varphi \circ f]$$

Ex (1) $H \leq G \rightsquigarrow \mathrm{Res}: H^1(G, A) \longrightarrow H^1(H, A)$

(2) $N \trianglelefteq G \rightsquigarrow M^N$ is a G/N-mod and we have

$$G \longrightarrow G/N, \qquad M^N \hookrightarrow M$$

$$\rightsquigarrow \quad \mathrm{Inf}: H^1(G/N, M^N) \longrightarrow H^1(G, M)$$

Thm (Inflation - restriction)

$$0 \longrightarrow H^1(G/N, M^N) \longrightarrow H^1(G, M) \longrightarrow H^1(N, M)$$

is exact

Kummer theory

K a field, $\mu_m \subseteq K^\times$, char $K \nmid m$

Def. L/K "ab. ext of exponent m" means that $\mathrm{Gal}(L/K)$ is abelian and $\sigma^m = id$ $\forall \sigma \in \mathrm{Gal}(L/K)$.

Thm

$$\left\{ \begin{array}{c} L/K \text{ ab. of} \\ \text{exponent } m \end{array} \right\} \longleftrightarrow \left\{ \Delta \mid K^{\times m} \subseteq \Delta \subseteq K^\times \right\}$$

$$K(\Delta^{1/m}) \longleftarrow\!\shortmid \Delta$$

$$L \longmapsto L^{*m} \cap K^*$$

Sketch of proof

$$1 \longrightarrow \mu_m \longrightarrow L^* \xrightarrow{\ \wedge m\ } L^{*m} \longrightarrow 1$$

$$\Rightarrow \quad H^0(G, L^*) \longrightarrow H^0(G, L^{*m}) \longrightarrow H^1(G, \mu_m) \longrightarrow 0$$

$$K^* \longrightarrow L^{*m} \cap K^* \longrightarrow \mathrm{Hom}(G, \mu_m) \longrightarrow 0$$

$$\Rightarrow \quad \mathrm{Hom}(G, \mu_m) \cong \frac{K^* \cap L^{*m}}{K^*} =: \Delta$$

$\square$

Kummer sequence for elliptic curves

$$0 \longrightarrow E[m](\overline{K}) \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0$$

is an exact sequence of G-modules, where $G = \mathrm{Gal}(\overline{K}, K)$

$$\rightsquigarrow \quad E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(G, E[m](\overline{K}))$$

$$\Rightarrow \quad E(K)/mE(K) \hookrightarrow H^1(G, E[m](\overline{k}))$$

Lemma L/K finite Gal. extension of nb. fields. If Weak MW is true over L, it's true over K

Proof.

$$\begin{tikzcd}
 & \ker f \arrow[r, hook] \arrow[d, hook] & \frac{E(K)}{mE(K)} \arrow[r, "f"] \arrow[d, hook] \arrow[dr, phantom, "\circlearrowright"] & \frac{E(L)}{mE(L)} \arrow[d, hook] \\
0 \arrow[r] & \underbrace{H^1(G_{L/K}, E[m](L))}_{\text{finite}} \arrow[r] & H^1(G_K, E[m]) \arrow[r, "\mathrm{Res}"'] & H^1(G_L, E[m])
\end{tikzcd}$$

$\Rightarrow \ker f$ is finite $\square$

Let's assume that $E[m] \subseteq E(K)$; in particular,

$$0 \to E[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} \mathrm{Hom}(G_K, E[m])$$

In this way, δ defines a "Kummer pairing"

$$\langle \, , \, \rangle : E(K) \times G_K \longrightarrow E[m]$$
$$P \, , \, \sigma \longmapsto \delta(P)(\sigma) = \sigma(Q) - Q$$
$$mQ = P$$

The left- and right- kernels are

$$\ker\Big(E(K) \longrightarrow \mathrm{Hom}\big(G_K, E[m]\big)\Big) = mE(K) \quad (\text{Kummer})$$

and

$$\ker\Big(G_K \longrightarrow \mathrm{Hom}\big(E(K), E[m]\big)\Big) = \mathrm{Gal}\big(\overline{K}/L\big), \text{ where}$$

$L = K\left(\frac{1}{m}P \mid P \in E(K)\right)$ is a Gal ext. of K.

This induces a non-degenerate pairing

$$\langle \, , \, \rangle : \frac{E(K)}{mE(K)} \times G_{L/K} \longrightarrow E[m] \qquad (*)$$

In particular, $\left| \frac{E(K)}{mE(K)} \right| = |G_{L/K}|$ and it's enough to prove

that L/K is finite.

Def E/K ell. curve, $v \in M_K^0 \rightsquigarrow E_v/K_v$

We say that E has good/bad red at v iff E_v does

E has good red at all but finitely many places, because

$v(\Delta) = 0 \quad \tilde{\forall} v.$

Assume furthermore $v(m) = 0$. Then we've seen that

$$E[m] \hookrightarrow \tilde{E}_v(k_v)$$

Lemma $L = K([m]^{-1}E(k))$. Then

(1) L/k is abelian of exponent m: by $(*)$,

$$G_{L/k} \hookrightarrow \mathrm{Hom}\left(\frac{E(k)}{mE(k)}, E[m]\right)$$

(2) L/k is unramified outside a finite set of places S, namely $\{v \mid m\}$ and $\{v : E \text{ has bad red at } v\}$ (and the ∞ places)

Proof (1) done in the statement

(2) it suffices to show that, $\forall Q \in E(k)$ $\forall v \notin S$,

the extension $K(\frac{1}{m}Q)/K$ is unramified at v.

Let v' be a place of L over v.

Is it true that $I(v'|v)$ is trivial? Take a σ in $I(v'|v)$. Then $\sigma(Q)-Q \in E[m] \hookrightarrow \tilde{E}_v$, but σ acts trivially on $\tilde{E}_v$, so $\widetilde{\sigma(Q)-Q} = \sigma(\tilde{Q})-\tilde{Q}$

$= \tilde{Q}-\tilde{Q} = 0 \implies \sigma(Q) = Q$. $\square$

Prop Let K be a nb. field, S a finite set of places, L = max ab. ext^n of K unramified outside of S and of exponent m.

Then L/K is finite.

Proof
- 1^{st} reduction: can replace with a finite extn K'. We may therefore assume $\mu_m \in K^\times$.
- 2^{nd} reduction: we may enlarge S and assume that S contains all valuations dividing m and all ∞ places.
- Let $R_S = \{x \in K \mid v(x) \geq 0 \quad \forall v \notin S\}$
- Further enlarging S (add representatives for the finite group $Cl(K)$), R_S is a PID
- Now $L = K(\sqrt[m]{a} \mid a \in \Delta)$, and L/K is unramified at $v \notin S$ iff $v(a) \equiv 0 \mod m$. But then wlog $a \in R_S^\times$, and $R_S^\times / R_S^{\times m}$ is finite (Dirichlet's unit thm)

More precisely: let

$$T_S = \{ [a] \in K^\times / K^{\times m} \mid \mathrm{ord}_v(a) \equiv 0 \ (m) \}$$

Consider
$$\begin{aligned} R_S^\times &\twoheadrightarrow T_S \\ x &\longmapsto [x] \end{aligned}$$

* Surjectivity: $x R_S = I^m$ (look at valuations)

$\Rightarrow x = u \cdot b^m$ (R_S is a PID)

$\Rightarrow [x] = [u]$

* Kernel: if $[x] = [1]$, then $x = u^m$ and $u \in R_S^\times$, so $x \in R_S^{\times m}$

Thus, $T_S \simeq R_S^\times / R_S^{\times m}$ is finite

17/11/2023
D. Ranieri

Curves, Jacobians & Abelian varieties

Recall: $E(\overline{K}) \simeq \mathrm{Pic}^0(E)$

$$P \longmapsto [(P)-(\infty)]$$

Genus 2 and higher?

<u>Q1</u> Can we put an alg. gp structure on curves of $g>1$?

No! By Riemann-Roch.

If D is a divisor on a curve, $\deg D = d$, then

$$\ell(D) - \ell(K_C - D) = d-g+1$$

and $\deg K_C = 2g-2$

Fact Let G be an algebraic group. G is automatically smooth (our Gs are VARIETIES and in partic. reduced)

The canonical class is zero (Shafarevič, BAG)

$\Rightarrow \quad 2g-2 = \deg K_C = 0 \qquad$ (if $C = G$ is a group)

$\Rightarrow \quad g = 1$

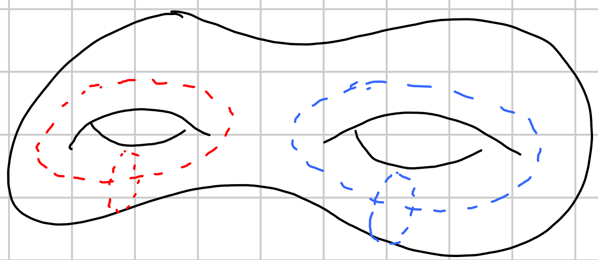
Q2. Is there a (nice) variety structure on $\mathrm{Pic}^0(C)$?

Motivation: complex case

Curves = Riemann surfaces

Functions = Holomorphic functions

Let C be a curve of genus g



$\mathrm{rk}_{\mathbb{Z}}\, H_1^{sing}(C, \mathbb{Z}) = 2g$

$g = \dim_{\mathbb{C}} H^0(C, \Omega^1_C)$

Let $\gamma_1, \dots, \gamma_g$ be a basis of $H^0(C, \Omega^1_C) \simeq \mathbb{C}^g$

$\omega_1, \dots, \omega_{2g}$ be a basis of $H_1^{\text{sing}}(C, \mathbb{Z})$

There is a map $H_1^{\text{sing}}(C, \mathbb{Z}) \hookrightarrow H^0(C, \Omega^1_C)^\vee$

$$\omega \longmapsto \left(\gamma \mapsto \int_\omega \gamma\right)$$

The img is a rank-$2g$ lattice, and we set

$$J(C) = \mathbb{C}^g / H_1^{\text{sing}}(C, \mathbb{Z})$$

One can prove that J is algebraic

(In general: $\mathbb{C}^g/\Lambda$ is " iff $\exists H$, Hermitian form on $\mathbb{C}^g$, s.t. $\Im H(\Lambda, \Lambda) \subset \mathbb{Z}$)

Thm (Abel-Jacobi)

① There is an analytic embedding $\mathcal{C} \hookrightarrow J$

② $\mathrm{Pic}^0(\mathcal{C}) \simeq J$ as groups

Goal

Given a curve $\mathcal{C}$ (smooth projective) of genus g, construct an $\underbrace{\text{abelian variety}}$ $\mathrm{Jac}\, \mathcal{C} / K = \bar{K}$ of dimension g such that

└ connected projective alg. group

1) as groups, $\mathrm{Jac}\, \mathcal{C} \simeq \mathrm{Pic}^0(\mathcal{C})$

2) $\exists\, j : \mathcal{C} \longrightarrow \mathrm{Jac}\, \mathcal{C}$, which is universal in the

following sense: $\forall$ morphism $C \longrightarrow A$ where A is an abelian variety, $\exists!\ \varphi$ s.t.

$$\begin{tikzcd} C \arrow[r] \arrow[d, hook] & A \\ \mathrm{Jac}\, C \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

commutes

(should fix base points...)

Recap on symmetric powers

V variety. $\underbrace{V \times V \times \dots \times V}_{n} = V^n$. $\mathrm{Sym}^n V := V^n / S_n$ parametrises unordered n-tuples of points on V.

(If $V = \mathrm{Spec}\, A$, $V^{\times n} = \mathrm{Spec}\, A^{\otimes n}$ and $\mathrm{Sym}^n V = \mathrm{Spec}\, (A^{\otimes n})^{S_n}$)

Thm (Hilbert) A a f.g. k-alg (even with $k \neq \overline{k}$), G a finite group acting on $A \Rightarrow A^G$ is fin. gen.

Pf. See Silverman-Hindry, Diophantine Geometry

Rmk If V is a smooth curve, $\mathrm{Sym}^n(V)$ is smooth

Weil's construction

$\mathrm{Sym}^g(C)$

By RR, on an ell. curve we have $\ell(D) - \ell(-D) = d$

$\Rightarrow$ D of degree one has $\ell(D) = 1$, and we use this to define $+$

Lemma $\exists\, U \subset \mathrm{Sym}^g(C) \times \mathrm{Sym}^g(C)$, open and non-empty, s.t. $\forall\, u_1 = P_1 + \dots + P_g \in U$, $u_2 = P_1' + \dots + P_g' \in U$

$$\ell(D_1 + D_2 - D_0) = 1 \qquad \forall D_1, D_2 \in U$$

(where we fix $D_0 \in \mathrm{Sym}^g(C)$)

$$\Rightarrow \quad D_1 + D_2 - D_0 \sim D_3$$

for a unique $D_3 \in \mathrm{Sym}^g(C)$.

Thm (Weil) For every rational group law X, there is a birational iso $(X, \cdot) \underset{\text{bir}}{\sim} (G, \cdot)$ where G is an actual alg. grp.

Chow's construction

Take $\mathrm{Sym}^n C$ with $n \gg 0$. If $D \in \mathrm{Sym}^n C$, then
$n > 2g-2$

$\ell(K_C - D) = 0$. This implies $\ell(D) = n-g-1$, so
$|D| \simeq \mathbb{P}^{n-g}$

Pretend that $\mathrm{Jac}\, C$ exists. Then, there should be a map

$$\begin{aligned} \mathrm{Sym}^n C &\longrightarrow \mathrm{Jac}\, C \\ P_1 + \dots + P_n &\longmapsto \left[\sum (P_i) - n(\infty) \right] \end{aligned}$$

Def. of the Jacobian

$J := \{$ complete linear systems of deg n on $C\}$

Fix ∞ (pt on $\mathcal{C}$), $D_0 = n \cdot (\infty)$

There is a group law on J:

$$|D_1| + |D_2| = |D_1 + D_2 - D_0|$$

(One checks that this doesn't depend on the representatives D_1, D_2)

Lemma Fix $\Delta \in \mathrm{Sym}^{n-g}(\mathcal{C})$. Then $\exists\, U_\Delta \hookrightarrow \mathrm{Sym}^n(\mathcal{C})$, $U_\Delta \neq \phi$, st $\forall D \in U_\Delta$ we have $\ell(D - \Delta) = 1$. Moreover, the U_Δ cover $\mathrm{Sym}^n(\mathcal{C})$

$$\begin{tikzcd}
 & \mathrm{Sym}^n(C) \arrow[d, two heads, "\pi"] & D \arrow[d, mapsto] \\
\mathrm{Sym}^g(C) \arrow[ur, "t_\Delta"] \arrow[r, hook, "f_\Delta"'] & J & |D|
\end{tikzcd}$$

Let $V_\Delta = (t_\Delta)^{-1}$. Then $V_\Delta = \{D : \ell(D) = 1\}$, and f_Δ is an injection $|D+\Delta| = |D' + \Delta| \Rightarrow D \sim D' \Rightarrow D = D'$

We can use the f_Δ to equip J w/ an alg. variety

Rmk π is a morphism, $\mathrm{Sym}^n C$ is projective $\Rightarrow$ J projective

One should check that addition is a morphism.

$$\begin{tikzcd}
C^n \times C^n \arrow[r] \arrow[d] & C^{2n} \arrow[r] & \mathrm{Sym}^{2n}(C) \arrow[d] \\
\mathrm{Sym}^n C \times \mathrm{Sym}^n C \arrow[urr] \arrow[rr] \arrow[d] & & J \\
J \times J \arrow[urr] & &
\end{tikzcd}$$

Rmk In principle, the constr. depends on n ... but it doesn't.

Properties

① $\mathrm{Pic}^0(J) \longrightarrow J$. Fix D_0 of degree n

$$[D] \longmapsto |D + D_0|$$

surj: $|D - D_0| \longmapsto |D|$

inj : $[D] \longmapsto [0] \Rightarrow |D_0| = |D + D_0|$

$\Rightarrow D_0 \sim D + D_0 \Rightarrow D \sim 0.$

② Fix $P_0 \in \mathcal{C}$ (first time we need $k = \overline{k}$!)

$j : C \hookrightarrow J$ is a morphism (factors

$P \longmapsto |P + (n-1) P_0|$ via $C \to \mathrm{Sym}^n C \to J$)

Let $W_r = \underbrace{j(C) + \dots + j(C)}_{r \text{ times}}$; formally,

$W_r = \mathrm{im}\left(C^r \xrightarrow{j^r} J^r \xrightarrow{+} J\right).$

Rmk

1. $\dim W_r \leq r$
2. $W_r = \text{image } C^r$ is irreducible
3. by an easy induction,

$$\dim W_{r+1} = \begin{cases} \dim W_r + 1 \\ \dim W_r \end{cases}$$

4. by dim of fibres, $\dim J = (n) - (n-g) = g$.
5. Let r_0 be the least r st $\dim W_{r+1} = \dim W_r$. Then (by induction) it's constant from there on.

$$\left(W_{r+2} = W_{r+1} + j(C) = W_r + j(C) = W_{r+1} \right)$$

(6) $W_0 \subsetneq W_1 \subsetneq W_2 \subsetneq \dots \subsetneq W_{r_0} = W_{r_0+1} = W_{r_0+2} = \dots$

(7) But $\mathrm{Sym}^n \twoheadrightarrow J$, so eventually $W_r = J$. Hence $\dim W_{r_0} = g$, and therefore $r_0 = g$.

Cor $j: C \to W_1$ is a surj. map of irred. curves with connected fibres $\Rightarrow$ j is an embedding.

Fact 1-Differential forms on C correspond bijectively to 1-diff. forms on $\mathrm{Jac}(C)$

Thm W_{r-1} is an irreducible divisor on $\mathrm{Jac}(C)$, called the Θ divisor. The pair $(\mathrm{Jac}\, C, \Theta)$ determines C (Torelli)

24/11/2023
A. Landi

§1. Modular curves over $\mathbb{C}$

Fact E an elliptic curve $/\mathbb{C}$. There exists a lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ (conversely, $\mathbb{C}/\Lambda$ is always an elliptic curve). One can take $\Lambda = H_1(E, \mathbb{Z}) \subset H^0(E, \omega_E)^\vee$

Cor (i) $\mathrm{Hom}(E_1, E_2) = \{\alpha \in \mathbb{C} \mid \alpha(\Lambda_1) \subset \Lambda_2\}$

$$\begin{tikzcd} \mathbb{C} \arrow[r, dashed, "\tilde{\varphi}"] \arrow[d] \arrow[dr] & \mathbb{C} \arrow[d] \\ E_1 \arrow[r, "\varphi"'] & E_2 \end{tikzcd}$$

$d\tilde{\varphi}$ definisce una funzione olom. su E_1 $\Rightarrow$ $d\tilde{\varphi} = $ costante

$\Rightarrow \tilde{\varphi}(z) = \alpha z + c$,

ma $\tilde{\varphi}(0) = 0 \Rightarrow c = 0$

(ii) $\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$

$\Lambda = \langle 1, \tau \rangle$ (up to homothety)

$\alpha \cdot 1 = a + b\tau$

$a, b, c, d \in \mathbb{Z}$

$\alpha \cdot \tau = c + d\tau$

Either $b = 0$, or $b\tau^2 + (a-d)\tau - c = 0$

$\Rightarrow$ $\tau \in K$, imag. quadr. field, and also $\alpha \in K$.

$$\Rightarrow \quad \mathrm{End}(E) \simeq \begin{cases} \mathbb{Z} \\ \mathcal{O}, \text{ an order in } K, \quad K = \mathbb{Q}(\sqrt{-d}) \end{cases}$$

$$\Rightarrow \quad \mathrm{Aut}(E) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} & \Longleftrightarrow \quad E \simeq \mathbb{C}/\mathbb{Z}[i] =: E_i \\ \mathbb{Z}/6\mathbb{Z} & \Longleftrightarrow \quad E \simeq \mathbb{C}/\mathbb{Z}[\zeta_3] =: E_\rho \end{cases}$$

Def. • $\mathcal{H} = \{ \tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0 \} \subset \mathbb{C}$

• $Y(1) := \{$ isom. classes of ell. curves $/ \mathbb{C} \}$

There is a natural map

$$\begin{aligned} \mathcal{H} &\longrightarrow Y(1) \\ \tau &\longmapsto E_\tau := \mathbb{C} / \langle 1, \tau \rangle \end{aligned}$$

• $\Gamma(1) := SL_2(\mathbb{Z}) \curvearrowright \mathcal{H}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

Prop.

$$\begin{tikzcd} \mathcal{H} \arrow[r] \arrow[d] & Y(1) \\ \mathcal{H}/\Gamma(1) \arrow[ur, "\sim"] & \end{tikzcd}$$

Proof. Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $\langle a\tau + b, c\tau + d \rangle = \langle 1, \tau \rangle$

$\wr$ homoth

$\langle 1, \frac{a\tau+b}{c\tau+d} \rangle$, so

$E_\tau \simeq E_{\gamma \cdot \tau}$. Conversely, given $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ with

$\Lambda_\tau = \alpha(\Lambda_{\tau'})$, write $\Lambda_\tau = \langle 1, \tau \rangle$, $\Lambda_{\tau'} = \langle 1, \tau' \rangle$

$$\Rightarrow \quad \begin{aligned} 1 &= \alpha(c\tau' + d) \\ \tau &= \alpha(a\tau' + b) \end{aligned} \quad \Rightarrow \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}). \qquad \square$$

Def

- $Y_1(N) := \left\{ (E, P) \;\middle|\; \begin{array}{l} E/\mathbb{C} \text{ ell. cur} \\ P \in E(\mathbb{C}) \text{ has order } N \end{array} \right\} / \text{iso}$

- $Y_0(N) := \left\{ (E, G) \;\middle|\; \begin{array}{l} E/\mathbb{C} \text{ ell. crv.} \\ G \text{ cyclic, } |G| = N \end{array} \right\}$

- $Y(N) := \left\{ (E, P, Q) \;\middle|\; \begin{array}{l} E/\mathbb{C} \text{ ell. curve} \\ P, Q \text{ basis of } E[N] \end{array} \right\}$

- $\mathcal{H} \xrightarrow{\varphi_1} Y_1(N)$, $\tau \longmapsto \left(E_\tau, \frac{1}{N} + \Lambda_\tau\right)$ | $\mathcal{H} \xrightarrow{\varphi_0} Y_0(N)$, $\tau \longmapsto \left(E_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle\right)$

$$\varphi : \quad \mathcal{H} \xrightarrow{\varphi} Y(N)$$
$$\tau \longmapsto \left(E_\tau, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\right)$$

- $\Gamma_1(N) = \left\{ \gamma \in \Gamma(1) \;\middle|\; \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (N) \right\}$
- $\Gamma_0(N) = \left\{ \gamma \in \Gamma(1) \;\middle|\; \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (N) \right\}$
- $\Gamma(N) = \ker\left(\Gamma(1) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z}) \right)$

Rmk $Y(N) \longrightarrow Y_1(N) \longrightarrow Y_0(N) \longrightarrow Y(1)$

Prop. φ_1, φ_0 are onto, and $\varphi_1, \varphi_0, \varphi$ factor via the action of $\Gamma_1(N)$, $\Gamma_0(N)$, $\Gamma(N)$

Proof Checks... $\square$

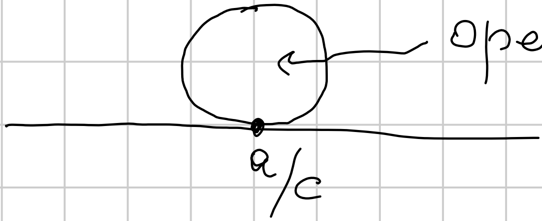
Def $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$

Rmk $\mathrm{Stab}_{\Gamma(1)}(\infty) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ $\quad \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix}$

Topology on $\mathcal{H}^*$

Neighbourhoods of ∞ : $U_r = \{ \operatorname{Im} \tau > r \} \cup \{\infty\}$

" " $\frac{a}{c}$:

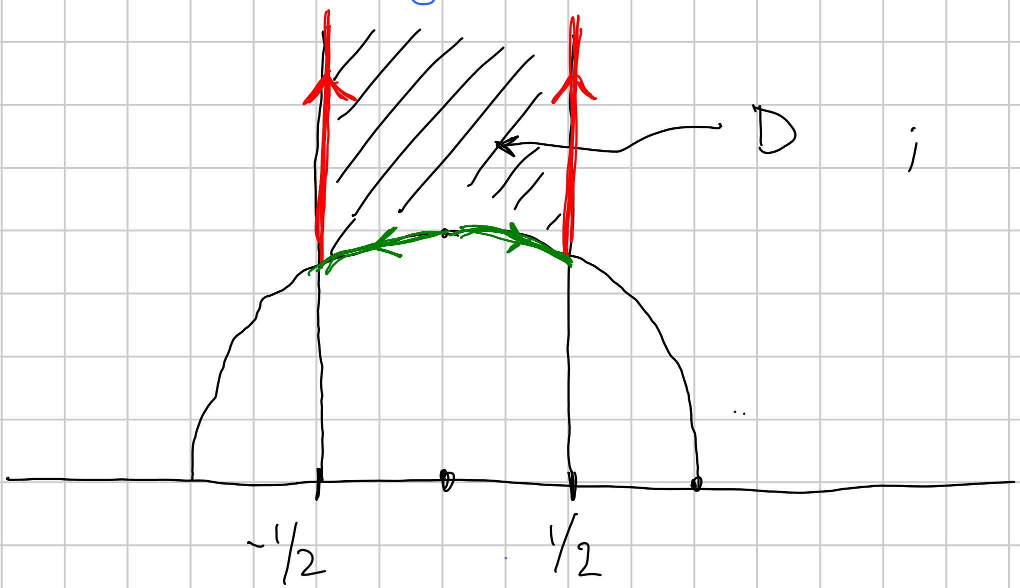


open disk $\cup \left\{ \frac{a}{c} \right\}$

Def. $X_1(N), \; X_0(N), \; X(N) := \mathcal{H}^*/\Gamma_1(N), \; \mathcal{H}^*/\Gamma_0(N),$

$\mathcal{H}^*/\Gamma(N)$

Fundamental domain for $\Gamma(1)$



D ; $D^* = D \cup \{\infty\}$

Prop. $\mathcal{H}^*$ is connected and D^* is compact

Prop. The modular curves are compact, connected, T_2, the action of $\Gamma(1)$ is properly discont. & open.

Proof Everything follows from the fact that the action is properly discontinuous. Fix $V_1 \ni x$, $V_2 \ni y$

$$\operatorname{Im}\left(\frac{az+b}{cz+d}\right) = \operatorname{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \frac{\operatorname{Im} z}{|cz+d|^2}.$$

This shows that $s(\gamma) := \sup\{\operatorname{Im}(\gamma \cdot z) \mid z \in V_1\} \leq$

$\leq \sup\left\{ \frac{\text{const}}{|cz+d|^2} \,\middle|\, z \in V_1 \right\}$ is finite. Thus, there are only finitely many transforms of V_1 that may intersect V_2 ... restrict V_1 $\square$

Prop Let $z \in \mathbb{H}$. There is an isom $\Gamma(1)_z \xrightarrow{\sim} \operatorname{Aut} E_z$

Proof Given $\gamma \in \Gamma(1)_z$, define $g : \Lambda_z \longrightarrow \Lambda_z$.

$$z \longmapsto az+b$$
$$1 \longmapsto cz+d$$

$$g \text{ is } \mathbb{C} \text{ linear} \iff z\, \underset{\substack{\| \\ z\cdot(cz+d)}}{g(1)} = \underset{\substack{\| \\ az+b}}{g(z)} \iff \gamma \cdot z = z$$

$\square$

Def. $z \in \mathbb{H}$ is elliptic for $\underset{\text{finite index}}{\Gamma \subset \Gamma(1)}$ if $\overline{\Gamma}_z := \Gamma_z / \{\pm 1\} \cap \Gamma_z$ is non-trivial.

Holom. structure on $X(\Gamma)$

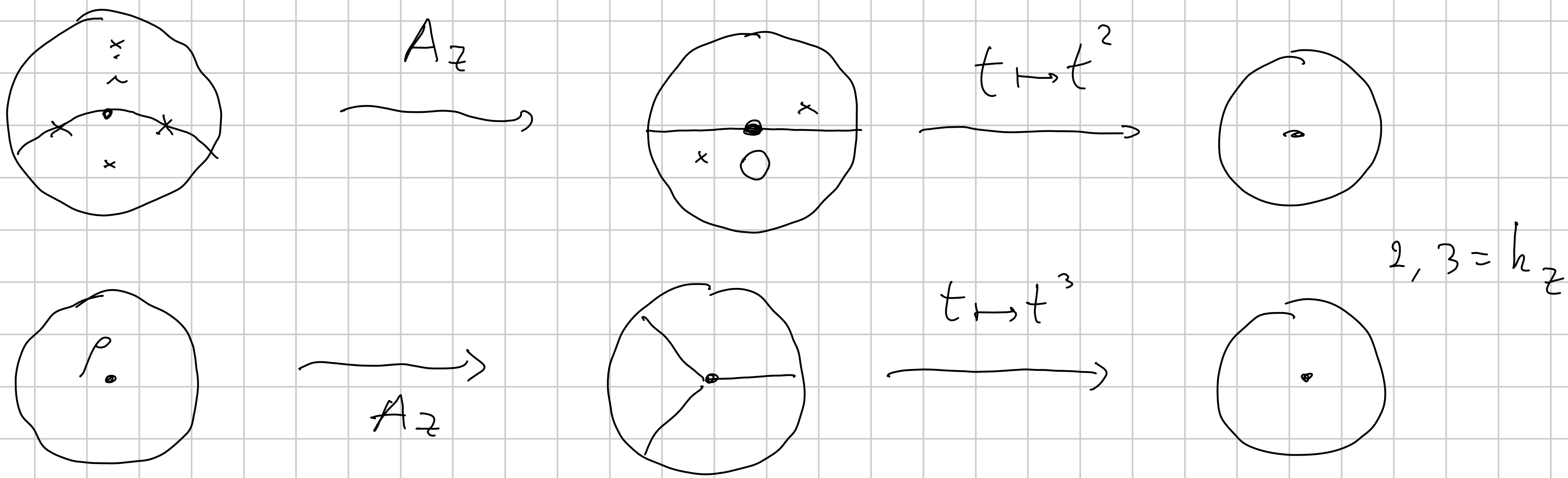
- Let $z \in \mathcal{H}$ not elliptic, $z \in U$ s.t. $\gamma z \neq z \Rightarrow \gamma U \cap U = \emptyset$.

Then $\pi : \mathcal{H}^* \longrightarrow X(\Gamma)$ induces $\pi : U \xrightarrow{\sim} \pi(U)$,
and we use (the inverse of) this as a chart.

- $z \in \mathcal{H}$ elliptic, $h_z := \# \Gamma_z > 1$

$$A_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix} \qquad A_\tau \cdot \tau = 0, \quad A_\tau \cdot \bar{\tau} = \infty$$

$$\left(A_\tau \Gamma A_\tau^{-1}\right)_0 = A_\tau \Gamma_z A_\tau^{-1}$$



- Around the cusp ∞, the chart is $\begin{array}{l} \tau \overset{\varphi}{\longmapsto} e^{2\pi i \tau / h_z} \\ \infty \longmapsto 0 \end{array}$,

where $h_z = [\overline{\Gamma(1)}_\infty : \overline{\Gamma}_\infty]$

Around $\frac{a}{c} = \delta(\infty)$, take $\varphi \circ \delta^{-1}$

Prop. $g = g(X_\Gamma)$, $X_\Gamma := \mathcal{H}^* / \Gamma$

$$g = 1 + \frac{d}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where $d = [\overline{\Gamma(1)} : \overline{\Gamma}]$, $\nu_2 = \#$ orbits elliptic pts order 2

$\nu_3 = \#$ orbits elliptic pts order 3, $\nu_\infty = \#$ cusps.

Proof

$$\begin{array}{c} X \\ \downarrow \\ X_\Gamma \end{array} \qquad i, \rho, \infty$$

Riemann-Hurwitz gives

$$2-2g = 2d + \sum (e_p - 1)$$

If $\pi(x) = i$,

$$\sum_{\pi(p)=i} (e_p - 1) = \frac{d - \nu_2}{2}$$

$$\sum_{\pi(p)=\rho} (e_p - 1) = \frac{d - \nu_3}{3}$$

$$\sum_{\pi(p)=\infty} (e_p - 1) = d - \# \pi^{-1}(\infty) = d - \nu_\infty$$

Functorial definitions

Let S be a base scheme, $\mathcal{E} \longrightarrow S$ an elliptic scheme, $N \geq 2$. A $\Gamma(N)$-structure is the choice of two pts $P, Q \in \mathcal{E}(S)[N]$ s.t.

$$(P, Q) : \left(\mathbb{Z}/N\mathbb{Z}\right)^2 \longrightarrow \mathcal{E}[N]$$

is an isomorphism.

$$F_{\Gamma(N)}(S) = \{ \mathcal{E}/S + \Gamma(N)\text{-structure} \}$$

$$F_{\Gamma(1)}(S) = \{ \mathcal{E}/S \}$$

Prop. K campo, $G_K = \mathrm{Gal}(K^s/K)$. There is a natural bijection $\{\text{twisted forms of } E\} \longleftrightarrow H^1(G_K, \mathrm{Aut}(E_{\bar{K}}))$

Sketch $E'_{K^s} \xrightarrow[\sim]{\varphi} E_{K^s} \rightsquigarrow$

$$G_K \longrightarrow \mathrm{Aut}(E_{K^s})$$
$$\sigma \longmapsto {}^{\sigma}\varphi \circ \varphi^{-1}$$

is a 1-cocycle: take its cohomology class.

Fix $N \geq 3$

Automorphisms: $(E, P, Q) \xrightarrow{\sim} (E, P, Q)$ is a map

$$\varphi : E \xrightarrow{\sim} E, \quad \varphi(P) = P, \quad \varphi(Q) = Q$$

$\Rightarrow$ φ fixes ≥ 5 pts $\Rightarrow$ $\varphi = \mathrm{id}$.

01/12/2023
A. Landi &
L. Morstabilini

Recap

- Def. and construction of mod. curves over $\mathbb{C}$

  $Y(1) = \mathcal{H} / SL_2(\mathbb{Z})$

- We asked whether $F_{\Gamma(N)}(S) = \{(E \to S, e_P, e_Q)\} / \text{iso}$ is representable

- We showed that, for $N \geq 3$, every autom. of an ell. curve E fixing a $\Gamma(N)$-structure is the identity.

- Corollary: $F_{\Gamma(N)}$ is a sheaf for the étale topology
  Zar

Weierstrass forms

Prop. $(\pi : E \to S, e)$ elliptic scheme. Zariski-locally over S, E is in Weierstrass point.

$$\left(\forall s \in S \quad \exists \text{ nbd } \operatorname{Spec} A \ni s \text{ s.t. } E_{\operatorname{Spec} A} = \operatorname{Proj}\left(\frac{A[x,y,z]}{(y^2 z - \dots)} \right) \right)$$

Rmk Over a field, one uses Riemann-Roch

Proof $L^\vee = \mathcal{O}_E(-e(S)) \rightsquigarrow 0 \to L^\vee \to \mathcal{O}_E \to e_* \mathcal{O}_S \to 0$

Tensoring by $L^{\otimes n+1}$, $\quad 0 \to L^n \to L^{n+1} \to e_* \mathcal{O}_S \otimes L^{n+1} \to 0$

Wlog S is affine, s geometric point,

$$h^0(E_s, L_s^{\otimes n}) = n, \quad h^1(E_s, L_s^{\otimes n}) = 0$$

Since $h^1(E_s, L_s^{\otimes n}) = h^0(E_s, (L_s^\vee)^{\otimes n}) = 0$ by Serre duality.

Standard results show that $\pi_* L^{\otimes n}$ is a locally free sheaf, of rank $h^0(\operatorname{Spec} \bar{s}, \pi_* L^{\otimes n}) = h^0(E_{\bar{s}}, L^{\otimes n}) = n$.

It also follows $R^1 \pi_* L^{\otimes n} \underset{\uparrow}{=} 0$, which gives

cohomology and base-change

$$0 \to \pi_* L^n \longrightarrow L_* L^{n+1} \longrightarrow Q \longrightarrow 0$$

Take a nbd so that these locally free sheaves are free:

if $S = \operatorname{Spec} A$, $(*)\ 0 \to A^n \longrightarrow A^{n+1} \longrightarrow Q \longrightarrow 0$

We show Q loc free $\Leftrightarrow$ flat $(\Rightarrow)$

$\mathrm{Tor}^1(N, Q) = 0$ for all fin. gen. A-mod N.

By functoriality of the construction, $(*)$ is preserved under base-change. Let $A' = A \oplus N \ni \begin{pmatrix} a & n \\ 0 & a \end{pmatrix}$; it's an A-algebra.

Pulling back to A' shows that $\mathrm{Tor}^1(A', Q) = 0$

$$= \mathrm{Tor}^1(A, Q) \oplus \mathrm{Tor}^1(N, Q)$$

So assume $\pi_* L^{n+1} / \pi_* L^n$ is free $\forall n \leq 5$.

Then take $1 \in H^0(L)$, $\langle 1, x \rangle = H^0(L^2)$, $\langle 1, x, y \rangle = H^0(L^3)$ and since L^{n+1}/L^n is free multiplication works as expected.

Now $[1:x:y] : E \longrightarrow \mathbb{P}^2_S$, and we check that this is a closed embedding (reduce to fibres)

$$\begin{tikzcd} E \arrow[r, hook] \arrow[dr, "\varphi"'] & \mathbb{P}^2_S \\ & V \arrow[u, phantom, "\cup"] \end{tikzcd}$$

$0 \to I \to \mathcal{O}_V \to \varphi_* \mathcal{O}_E \to 0$

but on fibres I is zero.

Thm Let $R = \dfrac{\mathbb{Z}[\frac{1}{3}, B, C, \frac{1}{\Delta}]}{(B^3 - (B+C)^3)}$ and $Y(3) := \operatorname{Spec} R$.

Then $Y(3)$ represents $F_{\Gamma(3)}$.

Proof It's a local problem, so assume $(\pi : E \to S, e_0, e_P, e_Q)$ is in Weierstrass form for $S = \operatorname{Spec} A$

$$y^2 + a_1 xy + a_3 y = h(x)$$

Note that x has a pole of order 2 along $e_0(S)$

y " " " " " 3 " "

Let $L_P = \mathcal{O}_E(-e_P(S))$, $L_0 = \mathcal{O}_E(-e_0(S))$

Consider $L_P^{\otimes 3} \otimes (L_0^\vee)^{\otimes 3}$, which is trivial on the fibers (since $3e_P = e_0$) and hence locally trivial.

Let's pretend that A is a field. Then

$$3(P) - 3(0) = \operatorname{div} f,$$

but $1, x, y$ span $H^0(\mathcal{O}(3(\infty)))$, so $f = ay + bx + c$

Wlog $a=1$,

$$y^2 + a_1 xy + a_3 y = (x - x(P))^3 \quad \text{(triple zero at } P)$$

Up to translation, $y^2 + a_1 xy + a_3 y = x^3$ and $P = (0,0)$

We have $3(Q) - 3(O) = \operatorname{div}(y - Ax - B)$.

Claim: A is invertible ($\Leftrightarrow A \neq 0$: it suffices to look at fibres)

Suppose $A=0$. Then $y - B$ has a triple zero, and

$$\begin{cases} y - B = 0 \\ y^2 + a_1 xy + a_3 y = x^3 \end{cases} \Leftrightarrow \begin{cases} y = B \\ B^2 + a_1 Bx + a_3 B = x^3, \end{cases}$$

so we should have $x^3 - (B^2 + a_1 Bx + a_3 B) = (x - x(Q))^3$

Comparing coeffs of x^2 gives $x(Q)=0$, but $x(P)=0$, contradiction. using

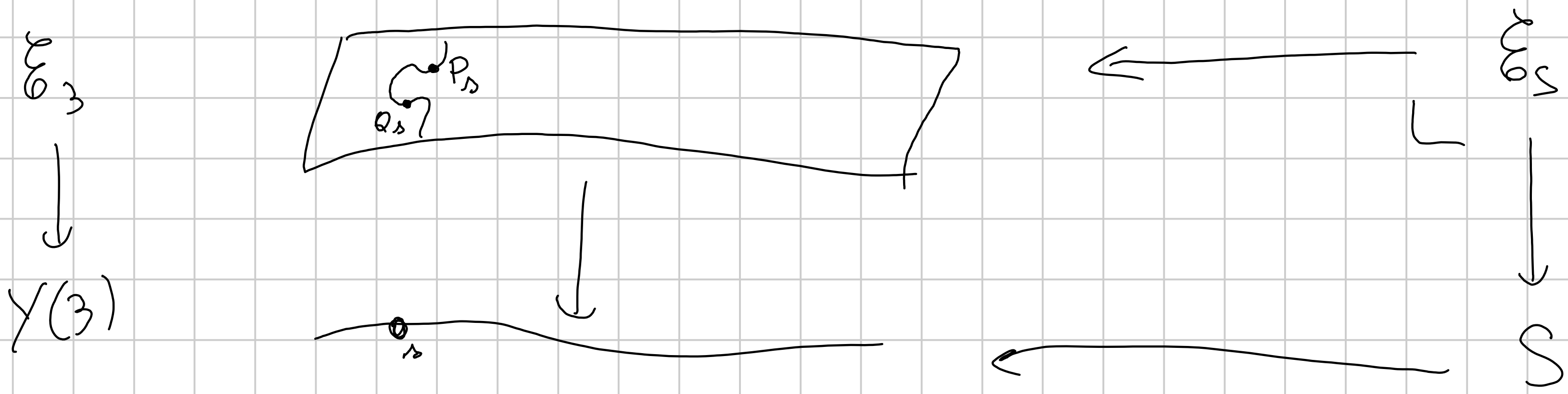
Make change of variable st $A=1$, namely y/A^3, x/A^2.

Then $y-x-B$ has triple zero at Q; computing, we find
$$X^3 - \left((x+B)^2 + a_1 x(x+B) + a_3(x+B) \right) = (x-C)^3, \quad C = x(Q)$$

$$\iff \begin{cases} 3C = a_1 + 1 \\ -3C^2 = 2B + a_1 B + a_3 \\ C^2 = B^2 + a_3 B \end{cases} \implies (B+C)^3 = C^3.$$

So the ell. curve is $P=(0,0)$, $Q=(C, B+C)$ and an explicit eqn. $\square$

From $Y(3)$ to $Y(N)$



$$\langle P_s, Q_s \rangle = \mathcal{E}_{3,s}[3]$$

This is universal: if $\mathcal{E}_S \longrightarrow S$ is a family w/ basis of 3-torsion, then it comes from pull-back from $\mathcal{E}_3 \longrightarrow Y(3)$.

Thm $\exists\, Y(N)$ representing $F_{\Gamma(N)}$ $\forall N \geq 3$ over $\mathbb{Z}[1/N]$

- $(N,3) = 1 \implies Y(3N)$
- quotient by grp action $\rightsquigarrow Y(N)$

Reminder: the Weil pairing

$$e_N : E[N] \times E[N] \longrightarrow \mu_N$$

- bilinear
- $e_N(x,x) = 1$
- $e_N(x,y) = 1 \quad \forall y \in E[N] \Rightarrow x = 0$

It can also be defined in families:

$$\begin{array}{c} E \\ \downarrow \\ \operatorname{Spec} R \end{array} \qquad e_N : E[N] \times E[N] \longrightarrow \mu_{N,R}$$

Fix S and $\mathcal{E}_S \longrightarrow S$ a family of ell. curves $/S$.

$$F_{\mathcal{E}/S}(T \to S) = \{ \Gamma(N)\text{-structures on } (\mathcal{E}_S)_T \}$$

Prop. $F_{\mathcal{E}/S}$ is representable by a finite étale scheme over S

Proof Let

$$\begin{tikzcd} S' = \mathcal{E}_S[N] \times \mathcal{E}_S[N] \arrow[r, "e_N"] \arrow[d, "\text{étale}"'] & \mu_{N,S} \\ S \end{tikzcd}$$

Take $S'' = e_N^{-1}(\mu_{N,S}^{prim})$. A map $T \to S''$ is the same as two sections $T \longrightarrow (\mathcal{E}_S)_T[N]$ whose Weil pairing is a primitive root of 1, so these two sections form a basis $\square$

Let $\mathcal{E}_T \longrightarrow T \longrightarrow S$ be the scheme representing $\mathcal{F}_{\mathcal{E}/S}$.

Thm Assume $(N, 3) = 1$. Then $F_{\Gamma(3N)}$ is representable by a smooth affine scheme over $\mathbb{Z}[1/3N]$ (or $\mathbb{Q}$ ...)

Proof Use the proposition for the family $\mathcal{E}_3 \longrightarrow Y(3)$.
The functor $S' \longmapsto \{ \Gamma(N)\text{-structures on } \mathcal{E}_{3,S} \}$ is representable. Consider the representing scheme T.

$$\begin{array}{ccc} \mathcal{E}_3 & \longrightarrow & Y(3) \\ & & \uparrow \text{finite ét} \\ & & T \end{array}$$

Since $Y(3)$ is smooth and affine, T is smooth and affine

We claim that T is $Y_1(3N)$.

How $(S', T) \overset{?}{\longleftrightarrow}$ $\Gamma(N)$-structures on ell. curves over S'

by the univ property of $Y(3)$ applied to φ

$$\begin{tikzcd}
(\mathcal{E}_3)_{S'} \arrow[r] \arrow[d] & \mathcal{E}_{3,T} \arrow[r] & \mathcal{E}_3 \arrow[d] \\
S' \arrow[r] \arrow[rr, bend left, "\text{composition } \varphi"] & T \arrow[r] & Y(3)
\end{tikzcd}$$

start with this

On the other hand, $(\mathcal{E}_3)_{S'} = \left(\mathcal{E}_3 \times_{Y(3)} T\right) \times_T S'$, so the map $S' \longrightarrow T$ also gives a $\Gamma(N)$-structure on

$$(\mathcal{E}_T)_{S'} = (\mathcal{E}_3)_{S'}$$

$\rightsquigarrow$ from a map $S' \longrightarrow T$ we get a $\Gamma(3)$- and a $\Gamma(N)$-structure on $\mathcal{E}_{S'}$, that is, a $\Gamma(3N)$-structure

Thm $Y(3N) / GL_2(\mathbb{Z}/3\mathbb{Z})$ represents $Y(N)$, is smooth and affine over $\mathbb{Z}[1/3N]$

Prop $G := GL_2(\mathbb{Z}/3\mathbb{Z})$ acts freely on $Y(3N)$ (equiv., $F_{\Gamma(3N)}$) and the (sheaf) quotient $F_{\Gamma(3N)}/G$ is $\simeq F_{\Gamma(N)}$

Proof E/S' with $(\underbrace{(P,Q)}_{3\text{-tors}}, \underbrace{(P',Q')}_{N\text{-tors}})$, $g \in G$, such that

$$g\left(E, (P,Q), (P',Q')\right) \cong \left(E, (P,Q), (P',Q')\right)$$

In partic., g gives an iso of E that is the identity on $E[N]$, but the only such is the identity. Thus, the action is free.

Surjectivity: $\mathcal{F}_{\Gamma(3N)} \longrightarrow \mathcal{F}_{\Gamma(N)}$ ... well, in the étale topology it's pretty trivial.

$$E \in \mathcal{F}_{\Gamma(N)}(S)$$

$\square$