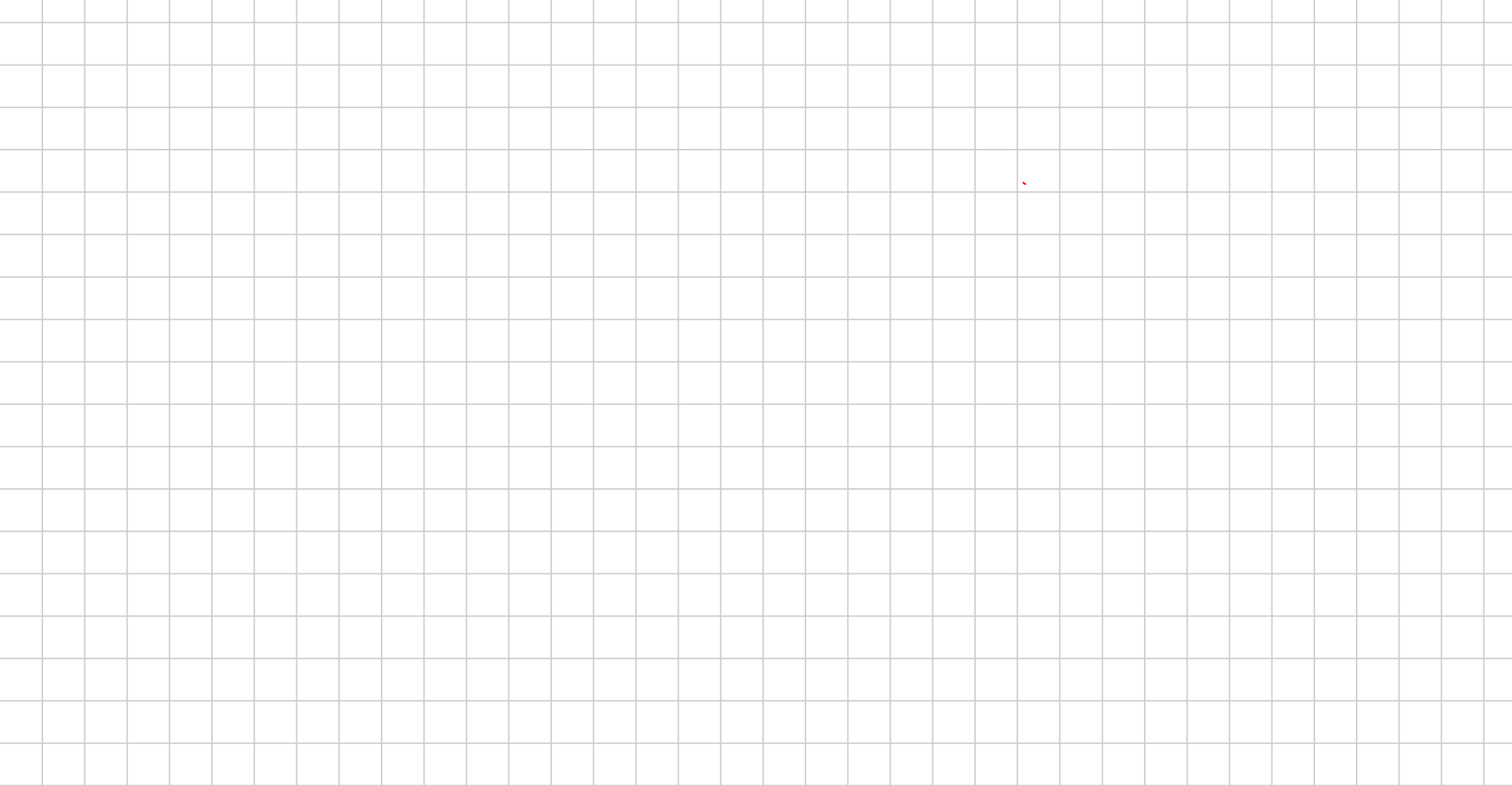

Titolo nota

26/01/2024



26/01/2024
L. Fucio

Hecke operators

$$SL_2(\mathbb{Z}) \curvearrowright \mathbb{H} = \{z \in \mathbb{C} \mid \Im z > 0\}$$

Def A **CONGRUENCE SUBGROUP** Γ of $SL_2(\mathbb{Z})$ is a subgroup that contains $\Gamma(N)$ for some $N \geq 1$

Note $\Gamma(N) = \{M \in SL_2(\mathbb{Z}) : M \equiv \text{Id} \pmod{N}\}$

$$\Gamma_1(N) = \left\{ M \in SL_2(\mathbb{Z}) : M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_0(N) = \left\{ M \in SL_2(\mathbb{Z}) : M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

Def A function $f: \mathbb{H} \rightarrow \hat{\mathbb{C}}$ is an **AUTOMORPHIC FUNCTION OF WEIGHT k FOR Γ** if it is meromorphic on \mathbb{H} and

satisfies $f(\gamma z) = (cz+d)^k f(z) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Moreover, $(cz+d)^{-k} f(z)$ should extend to a merom. function at the cusps.

Def. An autom. form $f: \mathbb{H} \rightarrow \mathbb{C}$ is a **MODULAR FORM** if it is holomorphic at the cusps. (I.e., $(cz+d)^{-k} f(z)$ is bounded as $\Im z \rightarrow \infty$)

Such an f is a **CUSP FORM** if $(cz+d)^{-k} f(\gamma z) \rightarrow 0$ as $\Im z \rightarrow \infty$

Notation $M_k(\Gamma) := \{ \text{mod forms weight } k \text{ for } \Gamma \}$

$$A_k(\Gamma) = \{\text{autom. " " } k \text{ for } \Gamma\}$$

Rmk We defined $X(\Gamma) := \mathbb{H}^* / \Gamma$. Then $A_0(\Gamma) = \mathbb{C}(X(\Gamma))$,

and more importantly

$$S_2(\Gamma) = H^0(X(\Gamma), \Omega_{X(\Gamma)}^1)$$

$$f(z) \longmapsto f(z) dz$$

Define $f[\gamma]_k := (cz+d)^{-k} f(\gamma z)$. Then for

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have that $f(z) dz$ is γ -invariant:

$$f(\gamma z) d(\gamma z) = (cz+d)^2 f(\gamma z) (cz+d)^{-2} dz$$

Moreover, if f is a cusp form, then $f(z) dz$ is regular at ∞ . Let's be more precise: if $\Gamma > \Gamma(N)$, then $f(z+N) = f(z) \Rightarrow f(z) = \tilde{f} \left(\underbrace{e^{2\pi i z/N}}_{q_N} \right)$.

In terms of q_N , $dq_N = \frac{2\pi i}{N} q_N dz$

$\Rightarrow dz = \frac{2\pi i}{N} \frac{dq_N}{q_N}$, so $f(z) dz$ stays

regular as $q_N \rightarrow 0$ iff $f(z) \rightarrow 0$ as $\text{Im} z \rightarrow \infty$. Same analysis for the other cusps.

Rmk Γ, Γ' congr. subgps, $\Gamma \triangleleft \Gamma'$. Then $\Gamma' \cong M_k(\Gamma)$

and $\Gamma' \cong S_k(\Gamma)$ via $\gamma \cdot f := f[\gamma]_k$. Indeed,

$\forall \delta \in \Gamma,$

$$(f[\gamma]_k)[\delta]_k = f([\gamma][\delta][\gamma^{-1}][\gamma])_k$$

$$= (f[\delta']_k)[\gamma]_k \stackrel{\uparrow}{=} f[\gamma]_k$$

$f \in M_k(\Gamma), \delta' \in \Gamma$

Hecke operators

Def $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. We define the **DIAMOND OPERATOR**

$$\langle d \rangle : S_k(\Gamma_1(N)) \longrightarrow S_k(\Gamma_1(N))$$

in the following way: let $\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ be any

matrix with $\tilde{d} \equiv d(N)$. We set

$$\langle d \rangle f := f[\gamma]_k$$

Rmk $\Gamma_1(N) \triangleleft \Gamma_0(N)$ and $\frac{\Gamma_0(N)}{\Gamma_1(N)} \cong (\mathbb{Z}/N\mathbb{Z})^\times$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d$$

This gives an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $S_k(\Gamma_1(N))$.

Fact $\dim_{\mathbb{C}} M_k(\Gamma) < +\infty$

Rmk Every fin-dim'l \mathbb{C} -rep of $(\mathbb{Z}/N\mathbb{Z})^\times$ is the \oplus of 1-dim'l eigenspaces. For every character

$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ we write $M_k(\Gamma_1(N), \chi)$
for the corresponding eigenspace

Rmk $S_k(\Gamma_0(N)) = S_k(\Gamma_1(N), 1)$

Def Let $\gamma \in GL_2(\mathbb{Q})^+$ ($\det \gamma > 0$). Define

$$f \circ [\gamma]_k := (\det \gamma)^{k/2} (cz+d)^{-k} f(\gamma z)$$

Ex. $\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ $f \circ [\gamma]_k = p^{k/2} f(pz)$

Double cosets

$$\Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) = \begin{cases} \bigsqcup_{\ell=0}^{p-1} \Gamma_1(N) \begin{pmatrix} 1 & \ell \\ 0 & p \end{pmatrix} & \text{if } p|N \\ \bigsqcup_{\ell=0}^{p-1} \Gamma_1(N) \begin{pmatrix} 1 & \ell \\ 0 & p \end{pmatrix} \cup \Gamma_1(N) \begin{pmatrix} a & b \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid N \end{cases}$$

Def. $T_p f = f \circ \left[\Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \right] =$

$$= \sum_{\ell=0}^{p-1} f \left[\begin{pmatrix} 1 & \ell \\ 0 & p \end{pmatrix} \right]_k + \underbrace{f \left[\begin{pmatrix} a & b \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right]_k}_{\text{if } p \nmid N}$$

(for PRIME values of p)

We also set $\langle d \rangle = 0$ for $(d, N) > 1$.

Prop. $\forall d \in \mathbb{Z} \quad \forall p \quad T_p \circ \langle d \rangle = \langle d \rangle \circ T_p$

$$\bullet \quad \forall p, q \quad T_p T_q = T_q T_p$$

Proof Matrix calculations

Def For $(m, n) = 1$ we set $T_{mn} = T_m T_n$

$$\text{For } n = p^{r+1}, \quad T_{p^{r+1}} = T_p T_{p^r} - p \langle p \rangle T_{p^{r-1}}.$$

Def The **HECKE ALGEBRA** is $\mathbb{Z} [T_n \mid n \geq 1]$. $\cong \mathbb{Z}$
contains $\langle d \rangle$ for all d

(Indeed, $T_{p^2} = (T_p)^2 - p \langle p \rangle$; take q another prime,
 $q \equiv p \pmod{N}$

$T_{q^2} = (T_q)^2 - q \langle p \rangle$. Hence, we have $p \langle p \rangle$
and $q \langle p \rangle$, so we have $\langle p \rangle$)

We can consider $\mathbb{T}_{\mathbb{Z}}$ as a sub-algebra of
 $\text{End}(S_k(\Gamma_1(N)))$

Jacobians

For X a curve over \mathbb{C} , $J(X) \cong \frac{H^0(X, \Omega^1)^{\vee}}{H_1(X, \mathbb{Z})}$.

If $X = X(\Gamma)$, $J(X(\Gamma)) = \frac{S_2(\Gamma)^{\vee}}{H_1(X, \mathbb{Z})}$

There is an action of $\pi_1 \mathbb{Z}$ on $S_2(\Gamma_1(N))$, hence on $S_2(\Gamma_1(N))^\vee$, by

$$T\varphi := \varphi \circ T \quad (\varphi \in S_2(\Gamma_1(N))^\vee)$$

This action induces an action on $\mathcal{J}(X_1(N))!$

The Mautz - Drinfeld theorem

02/02/2024
S. Boscardin

Cusps $\Gamma \subset SL_2(\mathbb{Z})$ a congruence subgroup, $\Gamma \ni \Gamma(m)$

$$Y_\Gamma := \mathbb{H} / \Gamma \quad X_\Gamma := \mathbb{H}^* / \Gamma$$

The set of cusps is $c(\Gamma) := X_\Gamma \setminus Y_\Gamma = \mathbb{P}^1(\mathbb{Q}) / \Gamma$.

Example ① $\Gamma = SL_2(\mathbb{Z})$, $c(\Gamma) = \{\infty\}$ (two justifications:

Γ acts transitively on $\mathbb{P}^1(\mathbb{Q})$; or $Y_\Gamma = \mathbb{A}^1$, $X_\Gamma = \mathbb{P}^1$,

hence $c(\Gamma) = \mathbb{P}^1 \setminus \mathbb{A}^1$)

② $\Gamma = \Gamma_0(n) = \left\{ M \in SL_2(\mathbb{Z}) \mid M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{n} \right\}$

If $n = p$, there are precisely two cusps, 0 and ∞ .

(Specifically, the orbit of $[x:y] \in \mathbb{P}^1(\mathbb{Q})$ - where

$x, y \in \mathbb{Z}, (x, y) = 1$ - contains $[0:1]$ if $p \nmid y$,
and it contains $[1:0]$ if $p \mid y$)

Thm (Manin-Drinfeld)

Let D be a divisor on X_Γ that is supported on the cusps and has degree 0. The class of D in $\text{Jac}(X_\Gamma)$ is torsion.

Equivalently: let c_1, \dots, c_n be cusps of X_Γ and let a_1, \dots, a_n be integers with $\sum a_i = 0$. There exists an integer $N \geq 0$ and $f \in \mathbb{C}(X_\Gamma)$ s.t.

$$\text{div } f = N(a_1 c_1 + \dots + a_n c_n)$$

Complements on Hecke operators & Manin symbols

$$T_p \curvearrowright S_2(\Gamma) \cong \Omega_{\text{hol}}^1(X_\Gamma), \quad T_p \curvearrowright S_2(\Gamma)^\vee$$

$$f(z) \longmapsto f(z) dz$$

$$\begin{array}{ccc} \text{Recall that } H_1(X_\Gamma, \mathbb{Z}) & \hookrightarrow & S_2(\Gamma)^\vee \cong H^0(X_\Gamma, \Omega^1)^\vee \\ \gamma & \longmapsto & \left(\omega \longmapsto \int_\gamma \omega \right) \end{array}$$

$$\text{and } \text{Jac}(X_\Gamma) \cong \frac{S_2(\Gamma)^\vee}{H_1(X_\Gamma, \mathbb{Z})}$$

Def Let M_2 be the ab. group generated by the symbols $\{\alpha, \beta\}$ for $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, modulo the (and $\{\alpha, \alpha\} = 0$)

relation $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0 \quad \forall \alpha, \beta, \gamma$

We also let $M_2(\Gamma) = M_2 / \sim$, where

$$\{\alpha, \beta\} \sim \{g\alpha, g\beta\} \quad \forall g \in \Gamma$$

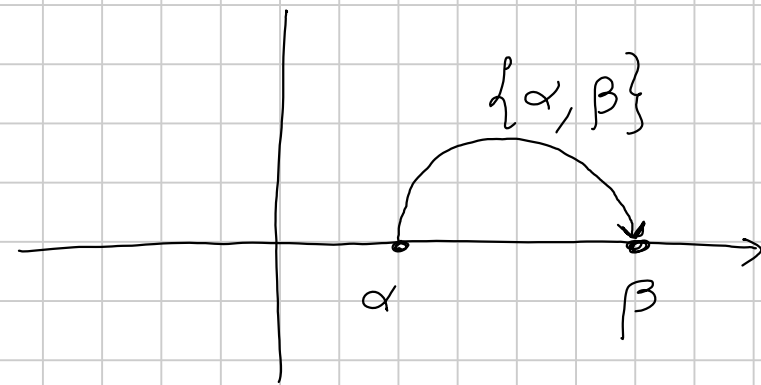
Interpretation We see $\{\alpha, \beta\}$ as "any path from

α to β in $\mathbb{H} \cup \{\alpha, \beta\}$:

There is a natural isomorphism

$$M_2(\Gamma) \xrightarrow{\sim} H_1(X_\Gamma, \text{cusps}, \mathbb{Z})$$

$$\cup \\ H_1(X_\Gamma, \mathbb{Z})$$



What's the image of $H_1(X_\Gamma, \mathbb{Z})$ inside $M_2(\Gamma)$?

Def $\delta : M_2(\Gamma) \longrightarrow \bigoplus_{c \in \text{cusps}} \mathbb{Z}c$

$$\{\alpha, \beta\} \longmapsto \bar{\alpha} - \bar{\beta}$$

Prop. $\ker \delta \cong H_1(X_\Gamma, \mathbb{Z})$

Fix now a level n .

We can define an action of T_p on $\{\alpha, \beta\}$ by setting

$$T_p \{\alpha, \beta\} = \sum_{\ell=0}^{p-1} \{A_\ell \alpha, A_\ell \beta\} \quad (\text{for } p \in \mathbb{N}),$$

where $A_\ell = \begin{pmatrix} p & \ell \\ 0 & 1 \end{pmatrix}$ for $\ell = 0, \dots, p-1$, $A_p = \begin{pmatrix} 1 & \\ & p \end{pmatrix}$

Prop The action just defined is compatible w/ the action on modular forms:

$$\int_{T_p \gamma} f(z) dz = \int_{\gamma} T_p f(z) dz$$

Proof (Manin-Drinfeld)

Step 1: We can assume $\Gamma = \Gamma(n)$. Indeed, if $\Gamma \supset \Gamma(n)$, there is a natural surjection $X_{\Gamma(n)} \xrightarrow{f} X_{\Gamma}$,
 $\{\text{cusps}\} \rightarrow \{\text{cusps}\}$

which extends to $f_* : \text{Jac}(X_{\Gamma(n)}) \xrightarrow{\cong} \text{Jac}(X_{\Gamma}) : f^*$

Let $D := \sum a_i c_i$ be a divisor of deg 0 supported on

the cusps of X_Γ . Then $f^*[D]$ is supported on the cusps of $X_{\Gamma(n)}$, hence is torsion by the special case of the thm; but then

$$f_* f^*[D] = (\deg f) \cdot [D]$$

is torsion.

Step 2: The theorem is true for $X(n) = X_{\Gamma(n)}$

Let $s_1, s_2 \in c(X(n))$. There is an action of T_p on

$H_1(X_\Gamma, \mathbb{Z})$. Take a prime $p \equiv 1 \pmod{n}$ and consider $(k = p+1)$

$$(T_p - k \text{ Id}) \{s_1, s_2\} =$$

$$= \sum_{\ell=0}^p \left[\{A_{\ell} s_1, A_{\ell} s_2\} - \{s_1, s_2\} \right] \in \ker \delta$$

This implies that $(T_p - \kappa \text{Id}) \{s_1, s_2\} \in H_1(X_{\Gamma}, \mathbb{Z})$

We can see T_p as a matrix in $M_{2g}(\mathbb{Z})$.

We know that the eigenvalues of T_p have size $p^{1/2}$,
so $(T_p - \kappa I)$ is invertible.

Multiplying by the classical adjoint of $T_p - \kappa I$ we get

$$\underbrace{\det(T_p - \kappa \text{Id})}_M \{s_1, s_2\} \in H_1(X_{\Gamma}, \mathbb{Z}), \text{ so}$$

$$\{s_1, s_2\} \in H_1(X_{\Gamma}, \mathbb{Q}).$$

This shows that $M \cdot [(s_1) - (s_2)] = 0$ in $\text{Jac}(X_\Gamma)$. \square

Cusps, again

$$\text{Let } A = \left\{ \pm \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\} = \text{Stab}(0)$$

$$A \backslash SL_2(\mathbb{Z}) / \Gamma \longleftrightarrow \text{cusps}$$

$$\overline{Y} \longleftrightarrow X$$

where $\gamma X = 0$

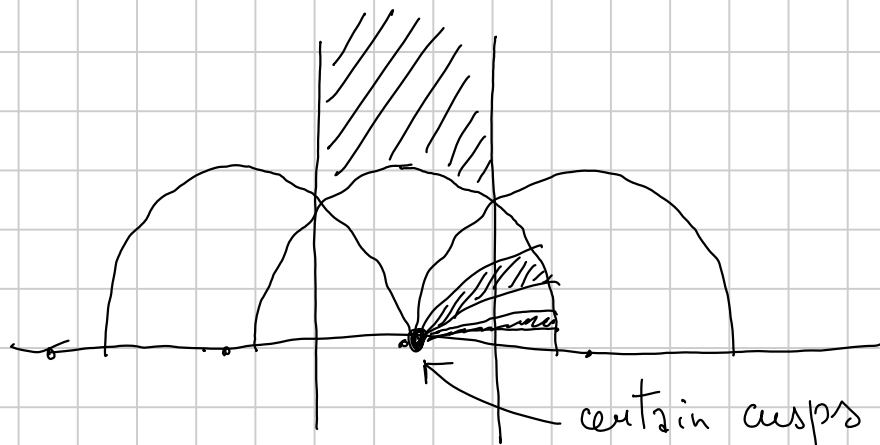
Note moreover that $A \backslash SL_2(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} \left\{ v \in (\mathbb{Z}/n\mathbb{Z})^2 : \text{ord } v = n \right\} / \pm \text{Id}$

(this is relevant when $\Gamma \supset \Gamma(m)$)

Ex $\Gamma = \Gamma_0(p)$ $(x, y) \cdot \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = (ax, bx + a^{-1}y)$

(∞)	$\{(0, *)\}$	$p-1$	1	# pts in the orbit
(0)	$\{(\neq 0, *)\}$	$p(p-1)$	w	

$A \cong SL_2(\mathbb{Z}) / \Gamma$



certain cusps are on the boundary of multiple

connected components in a fundamental domain

Let's find a function supported on these cusps.

Given $v \in (\mathbb{Q}/\mathbb{Z})^2$, let $v = (a, b)$ and

$$g_v(\tau) = q^{\frac{B(a)}{2}} \cdot e(a(b-1)) \cdot (1 - e(b)q^a) \prod_{n=1}^{\infty} \frac{(1 - e(b)q^{n+a})}{(1 - e(b)q^{n-a})}$$

$$B_2(x) = x^2 - x + \frac{1}{6}, \quad e(x) = \exp(2\pi i x), \quad q^x = \exp(2\pi i x \tau)$$

Moreover, $g_v(\gamma\tau) = g_{v\gamma}(\tau) \varepsilon(\gamma)$, $\varepsilon(\gamma) \in \mu_{12}$
 $\forall \gamma \in SL_2(\mathbb{Z})$

$\Rightarrow g_v^{12n} \in \mathcal{O}(\gamma(n))$ when $v \in \left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^2$

Let $u(\tau) = \prod_v g_v^{M_v}$, product over $v \in \left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^2$

Is this a reg. function on $Y(\Gamma)$, $\Gamma \supset \Gamma(n)$?

Applying the functional eqn, this happens iff

(i) $M_v = M_{\gamma v} \quad \forall \gamma \in \Gamma$

(ii) $\sum_v M_v \equiv 0 \pmod{12}$

(iii) $\sum_{v=(v_1, v_2)} M_v \cdot v_1^2 \equiv \sum_v M_v \cdot v_2^2 \equiv \sum_v M_v \cdot v_1 \cdot v_2 \equiv 0 \pmod{n}$

Ex $\Gamma = \Gamma_0(p)$. Take $M_v = M$ for $v = (0, *)$
 $M_v = 0$ for $v = (\neq 0, *)$

$$\operatorname{div}(u) = M \sum_{v \in \text{orbit}(\infty)} \operatorname{div}(g_v) = M \sum_{c \text{ cusp}} (c) w(c) \sum_{v \in (\infty)} B((vA_c)_1) / 2$$

where $A_c \infty = c$ and $(vA_c)_1 = 1^{\text{st}}$ coord.

$$\begin{aligned} \text{So } V_\infty(u) &= M \cdot \sum_{\substack{\uparrow \\ w(c)}} \frac{1}{2} \sum_{i=1}^{p-1} B\left(\left(\frac{1}{p}(0, i) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)_1\right) \\ &= M \cdot \frac{p-1}{2} B(0) = M \cdot \frac{p-1}{12} \end{aligned}$$

$$\left(A_c = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ for } c = \infty, \quad A_c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ for } c = 0 \right)$$

$$\text{and } V_0(u) = -V_\infty(u) = -M \frac{p-1}{12}.$$

$$\operatorname{div}(u) = M \frac{p-1}{12} \left((\infty) - (0) \right)$$

We need to choose M . The conditions are

$$(p-1)M \equiv 0 \pmod{12} \rightsquigarrow M = b \quad \frac{p-1}{12} = \frac{a}{6},$$

So $\text{div}(u) = a[(\infty) - (0)]$.

Rmk • $\Gamma = \Gamma_1(13)$: 12 cusps, G are defined over \mathbb{Q} .

There is an f such that

$$\text{div } f = 19 \sum_{i=1}^6 (-1)^i c_i$$

$\Rightarrow J_1(13)$ has a 19-torsion point!

• $\Gamma = \Gamma_0(p)$. Let $\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$.

Then η^{12} is a modular form for $SL_2(\mathbb{Z})$ of

weight 12. The function $\left(\frac{\eta(Nz)}{\eta(z)}\right)^{24} =: f$ satisfies

$\text{div}(f) = M \cdot ((\infty) - (0))$. It is invariant under

$\Gamma_0(N)$: if $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$

$$\eta(N\gamma z)^{24} = \eta\left(\frac{Naz + Nb}{Ncz + d}\right)^{24} = \eta\left(\frac{a(Nz) + Nb}{c(Nz) + d}\right)^{24}$$

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = +1 \quad = \left(\frac{1}{cNz + d}\right)^{12} \eta(Nz)$$



21/02/2024
P. Leonardini

Raynaud's unique prolongation theorem

Ref Finite flat group schemes (Tate)

Setting

$$\begin{array}{ccc} K & R = \mathcal{O}_K & \kappa = R/\pi \text{ res. field, } \pi = \text{uniformiser} \\ | & v(\pi) = 1, & v(p) = e \\ \mathbb{Q}_p & & \end{array}$$

We're interested in finite flat group schemes over R .

Facts In this setting, we have a connected-étale sequence, quotients, and if $\pi_K G$ is invertible in R , then $G \rightarrow \text{Spec } R$ is étale

Def (prolongation) Given $G_0 / \text{Spec } K$, a **PROLONGATION** $G \rightarrow \text{Spec } R$ is a finite flat gp scheme over R st. $G_{\text{Spec } K} \cong G_0$.

We say that G_0 has property UP (unique prolongation) if any two prolongations G_1, G_2 are isomorphic.

Thm (Raynaud) If $e < p-1$, every G_0 satisfies UP.

Ex For $K = \mathbb{Q}_p(\zeta_p)$, the scheme $(\mathbb{Z}/p\mathbb{Z})_K$ admits both $(\mathbb{Z}/p\mathbb{Z})_R$ and $(\mu_p)_R$ as prolongations, and they are not isomorphic.

Application E/K an ell. curve, $\mathcal{E}/\text{Spec } R$ (minimal reg. model),

$\bar{\mathcal{E}}/k$. We say that E has good red. if $v(\Delta_{\min}) = 0$.

If E has good red'n, $\mathcal{E}[m] \xrightarrow{\sim} \bar{\mathcal{E}}[m]$ when $p \nmid m$.

Raynaud's thm allows us to show: assume $e < p-1$. Then

reduction mod. π gives an injection $\mathbb{E}[u](R) \hookrightarrow \overline{\mathbb{E}[u]}(R)$.

More generally,

Prop. Let G be finite flat over R , $e < p-1$. Then $G(R) \hookrightarrow G_k(k)$.

Proof Let $\Gamma := G(R)$. Consider Γ as

$$\begin{array}{ccc} G_0 & \longrightarrow & \text{Spec } K \\ \downarrow & & \\ G & \longrightarrow & \end{array}$$

the constant group $\Gamma = \bigsqcup_{g \in \Gamma} \text{Spec } R$

We have an obvious morphism $\Gamma \xrightarrow{\Phi} G$.

$$G(\Gamma) = \text{Hom}(\Gamma, G) = \text{Hom}\left(\bigsqcup_{g \in \Gamma} \text{Spec}_g R, G\right) = \prod \text{Hom}(\text{Spec}_g R, G)$$

$$\begin{array}{c} \downarrow \\ \Phi \\ \downarrow \\ \text{Hom}(\text{Spec } R, G) \end{array}$$

Let $\overline{\Gamma} := \overline{\Phi(\Gamma)}$ be the Zariski closure. We have

$$\begin{array}{ccc} \Gamma_K & \xrightarrow{\sim} & \overline{\Gamma}_K & \longrightarrow & G_0 \\ \parallel & & \parallel & & \parallel \\ \pi \text{ Spec } K & & \pi \text{ Spec } K_i & & \end{array}$$

Since $\overline{\Gamma}_K \cong \Gamma_K$ and $\Gamma, \overline{\Gamma}$ are prolongations of Γ_K , this means $\overline{\Gamma} = \Gamma$, hence $\mathcal{O}_G \rightarrow \mathcal{O}_\Gamma$, and this implies $\Gamma_K \hookrightarrow G_K$. \square

Proof of Raynaud's theorem

Rmk $A \in A_0$: indeed, $R \subseteq K$ and

A/R is flat, so

$$A = R \otimes_R A \in K \otimes_R A = A_0.$$

Step 0 - define G^+ and G^-

By the remark, $A \in A_0$. Inclusion of coord rings gives an

$$\begin{array}{ccc} \text{Spec } A_0 = G_0 & \longrightarrow & \text{Spec } K \\ \downarrow & & \downarrow \\ \text{Spec } A = G & \xrightarrow{\text{flat}} & \text{Spec } R \end{array}$$

order relation on prolongations: $G_1 \geq G_2 \Leftrightarrow A_2 \leq A_1$.

Def. Let G^+ be a maximal element for this order (which exists, because $\text{rk}_R A$ is bounded, and given two prolongations $\text{Spec } A_1, \text{Spec } A_2$ we have $\text{Spec}(\langle A_1, A_2 \rangle)$)

• Let $G^- :=$ Cartier dual of the max of the duals of prolongations

Step 1 - reduction to simple G_0

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_0' & \longrightarrow & G_0 & \longrightarrow & G_0'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G/G' \longrightarrow 0 \\ 0 & \longrightarrow & H' & \longrightarrow & H & \longrightarrow & H/H' \longrightarrow 0 \end{array}$$

Assume G_0', G_0'' have UP. Let $G \leq H$ be two prolongations.

Then $H' \cong G'$, $H/H' \cong G/G'$, but unique prolong. shows that they are equal \Rightarrow the 5-lemma gives $G \cong H$.

By induction on the length of a Jordan-Hölder sequence, it's clear that it's enough to prove UP in the simple case

Step 2 - Raynaud's F-modules

Suppose $K = K^{nrc}$, the max. unramified extension.

$$\begin{array}{c} \text{Spec } \bar{K} \\ | \\ \text{Spec } K_{\text{tame}} \\ | \\ \text{Spec } K_{nrc} \end{array} \xleftarrow{\text{flat}} (G_0)_{\bar{K}} = \underbrace{\pi \text{ Spec (finite exts } \bar{K})}_{\text{in char } 0} = \pi \text{ Spec } \bar{K}$$

Spec K_{tame}

Spec K_{nrc}

$$\xleftarrow{\text{flat}} G_0$$

$\{\text{étale gp schemes } /k\} \leftrightarrow \{\text{finite groups with } G\text{-action}\}$

$$G = \text{Gal}(\bar{K}/K_{nrc})$$

Suppose $|G_0(\bar{K})| = p^r$. Write the usual sequence

$$\text{and } G_0 \text{ simple} \quad \left| \quad 1 \rightarrow P \rightarrow G \rightarrow G_{\text{tame}} \rightarrow 1; \right.$$

note that G_{tame} is abelian.

Let $H := \{x \in G(\bar{k}) \mid \sigma x = x \quad \forall \sigma \in P\} \triangleleft G(\bar{k})$.

It is not the trivial group: P acting on $G(\bar{k})$ has fixed pts.

(Note that $G_0(\bar{k}) = G_0(\bar{k})[p]$, and $G_0(\bar{k})[p]^P = H \neq \{e\}$).

By simplicity, $H = G(\bar{k})$, and the action of G factors via

G_{tame} . $\Rightarrow G_0(\bar{k})$ is a $\mathbb{Z}[G_{\text{tame}}]$ -simple module.

$\Rightarrow G_0(\bar{k}) \cong \mathbb{Z}[G_{\text{tame}}]/\mathfrak{M}$ — maximal ideal

$\Rightarrow G_0(\bar{k})$ "is" a field $F = \mathbb{F}_p = \mathbb{F}_q$

We have thus obtained a map $F \rightarrow \text{End}(G_0(\bar{k}))$, which
 $\simeq \hookrightarrow [\simeq]$

induces an action $F \rightarrow \text{End}(G_0)$

↳ since it commutes with the Gal action.

Rmk F acts on G^+ and G^- by uniqueness of the max.

Def (F -mod scheme) Let F be a ring. An F -mod scheme over R
is a commutative $\overset{\text{finite flat}}{\vee}$ gp scheme G together with a morphism
 $F \rightarrow \text{End}(G)$.

(Equivalently: G is a repr. functor to F -mod)

Def (Raynaud F -module scheme) In the context of the previous def, if F is a finite field of the same order as G , then G is called a Raynaud F -mod scheme.

Step 3 - characterisation of Raynaud's F -mod schemes

Let $F = \mathbb{F}_q = \mathbb{F}_{p^r}$, $\mu := \mu_{q-1}(\bar{K})$, $M = \text{Hom}(F^\times, \mu)$.

We extend every $\chi \in M$ to a function $\chi: F \rightarrow \bar{K}$.

Suppose $\mu \subseteq R$ (e.g., $R = \mathcal{O}_{K_{nr}}$). In this case, there are

$$(*) \quad F \xrightarrow{\chi} R \longrightarrow R/\pi R = k$$

$\xrightarrow{\quad \chi_0 = \text{hom. of fields} \quad}$

r characters ("fundam. characters of level r ")

χ_1, \dots, χ_n such that χ_0 is a hom of fields (see $(*)$)

These characters can be ordered so that $\chi_{i+1} = \chi_i^p$.

Thm (classification of Raynaud's F -mod schemes)

Let $(\chi_i)_{i \in I}$ be fundam. characters, assuming $\mu \subseteq R$.

(a) Let $\{\delta_i\}_{i \in I}$ be elements with $0 \leq v(\delta_i) \leq e \quad \forall i \in I$.

The algebra $R[x_i] / (x_i^p = \delta_i x_{i+1})_{i \in I}$ represents a finite flat gp scheme G ; there is a unique F -mod structure

on G st $[\rho] X_i = \gamma_i(\rho) \quad \forall i \in I, \quad \forall \rho \in F$

(b) Every Raynaud F -mod is isomorphic to one of this form.

(c) Suppose G, G' are Raynaud F -mods, defined by collections $\{\delta_i\}$ and $\{\delta_i'\}$. The homs $G' \rightarrow G$ correspond to $A \rightarrow A'$, where $a_i \in R$ satisfy

$$X_i \mapsto a_i X_i'$$

$$a_{i+1} \delta_i = a_i P \cdot \delta_i'$$

We assume this for the moment.

Final step - proof of Raynaud's theorem

We can reduce to the case $K = K_{nr}$. Indeed, suppose that $G^+ \not\cong G^-$ over R . As $\mathcal{O}_{K_{nr}} / \mathcal{O}_K$ is faithfully flat, we have $G^+ \not\cong G^-$ also over K_{nr} .

We can also assume that G_0 is simple (step 2), hence an \mathbb{F}_ℓ -module for some ℓ . If $\ell \neq p$, any prolongation is étale and we are done. Otherwise, ord $G_0 = p^r$, and G_0 is a Raynaud F -mod scheme. Consider $G^+ > G^-$.

We find $a_i \in R \setminus \{0\}$ st $a_i^p a_{i+1}^{-1} \delta_i' = \delta_i \quad \forall i \in I$.

Consider a_i st $v(a_i)$ is maximal.

$$v(a_i^p \delta_i') \geq p v(a_i)$$

$$p v(a_i) \leq v(a_i^p \delta_i') = v(\delta_i a_{i+1}) \leq e + v(a_{i+1}) \leq e + v(a_i)$$

$$\Rightarrow (p-1) v(a_i) \leq e < p-1 \Rightarrow v(a_i) = 0.$$

Thus, all a_i 's are units, and $G^- \hookrightarrow G^+$ is an isomorphism.

12/04/2024

The Eichler - Shimura relation

§ Recap

- Hecke correspondences: for $p \nmid N$,

$$\begin{array}{ccc}
 X_0(Np) & \longrightarrow & X_0(N) \\
 \downarrow & & \\
 X_0(N) & &
 \end{array}$$

$$\begin{array}{ccc}
 (E \xrightarrow{f} E', & G &) \xrightarrow{g} (E', \varphi(G)) \\
 \text{cyclic} & \text{cyclic} & \\
 \text{p-isogeny} & \text{subgp} & \\
 & \text{order } N & \\
 & \downarrow f & \\
 & (E, G) &
 \end{array}$$

Map on Jacobian:

$$f_* f^* = T_p : (E, G) \longmapsto \sum_{\substack{\varphi: E \rightarrow E' \\ \text{cyclic p-isog.}}} (E', \varphi(G))$$

- $H^1(X_0(N), \mathbb{C}) \cong S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$

Both objects are free of rank 2 over

$$\Pi_{\mathbb{C}} = \mathbb{Z}[T_p] \otimes \mathbb{C}$$

$\Rightarrow H^1(X_0(N), \mathbb{Q})$ is free of rank 2 over $\Pi_{\mathbb{Q}}$.

- Let $X/\overline{\mathbb{F}_p}$ and $F: X \longrightarrow X^{(p)}$ be the Frobenius.

$$[x_0: \dots: x_r] \mapsto [x_0^p: \dots: x_r^p]$$

If X is defined over \mathbb{F}_p , $F: X \longrightarrow X$

If X is an abelian variety,

$$\begin{array}{ccc}
 X & \xrightarrow{[p]} & X \\
 F \searrow & & \nearrow \\
 & X^{(p)} &
 \end{array}$$

Thm (Eichler - Shimura) p, N distinct primes

$$T_p = F + V \pmod{p},$$

as elements of $\text{End}(\mathcal{J}_0(N)_{\mathbb{F}_p})$.

Proof 1 (algebraic)

$$T_p(E, G) = \sum_{\substack{\varphi: E \rightarrow E' \\ p\text{-isogeny}}} (E', \varphi(G))$$

"The same" holds modulo p .

$$T_p(\tilde{E}, \tilde{G}) = \sum_{\substack{\varphi: \tilde{E} \rightarrow \tilde{E}' \\ p\text{-isog.}}} (\tilde{E}', \varphi(\tilde{G}))$$

Let E/\mathbb{Q}_p be a repr. for \tilde{E}/\mathbb{F}_p and consider

$$0 \rightarrow C_0 \rightarrow E[p] \rightarrow \tilde{E}[p] \rightarrow 0$$

Assume \tilde{E} is ordinary, so $\# C_0 = \# \tilde{E}[p] = p$

There are $p+1$ isogenies. One is special, namely that def'd by C_0 . If $\varphi: E \rightarrow E'$ is the quotient mod C_0 , then $\tilde{\varphi}: \tilde{E} \rightarrow \tilde{E}'$ is the Frobenius.

If instead φ has any other kernel, then $\tilde{\varphi}$ has kernel $\tilde{E}[p]$, and in particular it's separable.

$$\begin{array}{ccccc} \tilde{E} & \xrightarrow{\tilde{\varphi}} & \tilde{E}/\tilde{E}[p] & \xrightarrow{\varphi} & \tilde{E} \\ & & & \swarrow \sim & \\ & & [p] & & \end{array}$$

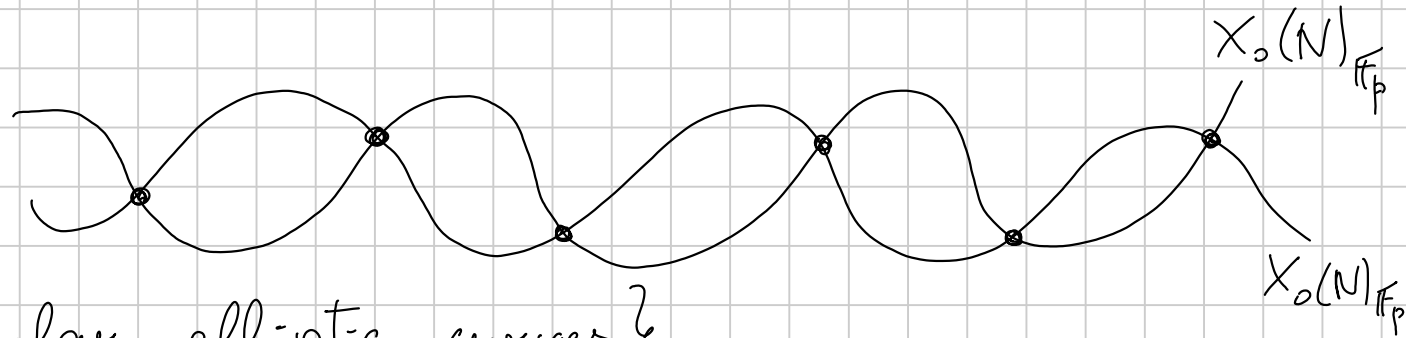
$\Rightarrow \deg \tilde{\varphi}^v = \text{deg} \tilde{\varphi}^v = p$, so $\tilde{\varphi}^v$ "is" the Frobenius.

$$\begin{aligned}
 \text{Hence: } T_p(\tilde{E}, \tilde{G}) &= \sum (\tilde{E}', \tilde{\varphi}(\tilde{G})) \\
 &= (\tilde{E}^{(p)}, \tilde{G}^{(p)}) + \sum_{E' \neq E/c_0} (\tilde{E}', \tilde{\varphi}(\tilde{G})) \\
 &= (\tilde{E}^{(p)}, \tilde{G}^{(p)}) + \underbrace{\sum_{E': (\tilde{E}')^{(p)} \cong E} (\tilde{E}', \tilde{\varphi}(\tilde{G}))}_{\text{this is a divisor whose image via Frobenius is } p \cdot (\tilde{E}, \tilde{G})} \\
 &= F(\tilde{E}, \tilde{G}) + V(\tilde{E}, \tilde{G})
 \end{aligned}$$

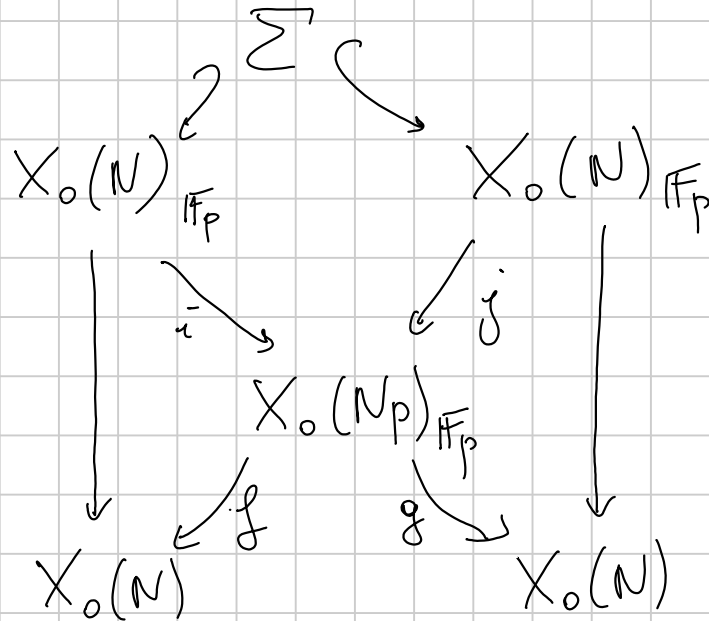
(+ details to avoid supersingular curves)

Proof 2

$$X_0(Np)_{\mathbb{F}_p} =$$



$$\Sigma = \{ \text{supersingular elliptic curves} \}$$



$$f_i = \text{id}$$

$$g_j = \text{id}$$

$$g_i = F$$

$$f_j = F$$

$$f^*(P) = i(P) + \sum_{y \in (fg)^{-1}(P)} j(y)$$

$$\Leftrightarrow y \in F^{-1}(P)$$

Applying g ,

$$g \circ i(P) + \sum_{y \in F^{-1}(P)} g \circ j(y) = F(P) + V(P) \quad \square$$

The Shimura construction, Galois representation

$$\begin{array}{ccc}
 V_{\ell}(\mathcal{J}_0(N)_{\mathbb{Q}}) & \xrightarrow{\sim} & V_{\ell}(\mathcal{J}_0(N)_{\mathbb{F}_p}) \\
 \uparrow & & \uparrow \\
 \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & & \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \\
 \psi & & \psi \\
 \text{Frob}_p & & \text{Frob}_p
 \end{array}$$

Moreover, $\Pi \simeq \mathcal{J}_0(N) \rightsquigarrow T_{\mathbb{Q}_\ell} \simeq V_\ell(\mathcal{J}_0(N))$

So $V_\ell(\mathcal{J}_0(N))$ is a module over $\Pi_{\mathbb{Q}_\ell}$, free of rank 2, and the action of Frob_p on $V_\ell(\mathcal{J}_0(N))$ is given by a 2×2 matrix with coeffs in $\Pi_{\mathbb{Q}_\ell}$.

Then
$$\begin{cases} \text{tr}(\rho_\ell(\text{Frob}_p) | V_\ell(\mathcal{J}_0(N))) = T_p \\ \det(\quad) = p \end{cases}$$

Proof $T_p = F + V, \quad FV = [p] \quad (\text{and } V = p \cdot F^{-1}).$

Hence $T_p = F + p \cdot F^{-1}$, and so $F^2 - T_p \cdot F + p = 0$.

Moreover, T_p is self-adjoint for the Weil pairing, because

$$T_p^v = (F+V)^v = F^v + V^v = V+F = T_p$$

$$\bullet \varphi: V_{\ell} \longrightarrow V_{\ell}^v \quad \varphi(Fx) = V\varphi(x)$$

$$x \longmapsto \langle x, \bullet \rangle$$

$$\bullet \text{ Hence, } \text{tr}(F|V_{\ell}) = \text{tr}(V|V_{\ell}^v) = \text{tr}^t \rho(V|V_{\ell}) = \text{tr} \rho(V|V_{\ell}),$$

$$\text{and finally } \text{tr}(\underbrace{T_p}_{2T_p}|V_{\ell}) = 2 \text{tr}(F|V_{\ell}).$$

□

The Shimura construction

Let $f \in S_2(\Gamma_0(N))^{\text{new}}$ be a normalised eigenform.

Consider

$$\begin{array}{ccc} \Pi_a & \longrightarrow & K_f \longrightarrow 0 \\ T & \longmapsto & \text{eigenvalue of } T \text{ on } f \end{array}$$

Recall that $T_p f = a_p(f)$, $a_p \in \overline{\mathbb{Z}}$

The kernel of $\pi_{\mathbb{Q}} \rightarrow K_f$ is denoted by I_f .

Def $A_f := \frac{J_0(N)}{I_f J_0(N)} \rightsquigarrow \sum_{T \in I_f} T \cdot J_0(N)$

Thm $\dim A_f = [K_f : \mathbb{Q}]$. We look at tangent space at 0:

$$\begin{aligned} T_0 A_f &= \frac{T_0 J_0(N)}{I_f T_0 J_0(N)} = T_0 J_0(N) \otimes_{\pi_{\mathbb{Q}}} (\pi_{\mathbb{Q}} / I_f) \\ &\simeq \pi_{\mathbb{Q}} \otimes_{\pi_{\mathbb{Q}}} (\pi_{\mathbb{Q}} / I_f) \simeq K_f \end{aligned}$$

Thm A_f has good red. away from N : $J_0(N)$ has good red. outside N , and then use Néron-Ogg-Shafarevich

We now describe the Gal rep of A_f .

1) $V_\ell(A_f)$ is free of rk 2 over $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$: to see this,

$$V_\ell A_f \cong \frac{V_\ell(J_0(N))}{I_f V_\ell(J_0(N))} \cong V_\ell(J_0(N)) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell/I_f$$

$$\cong \mathbb{T}_{\mathbb{Q}_\ell}^2 \otimes_{\mathbb{Q}_\ell} (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$$

$$2) \begin{matrix} \text{Tr}_{K_f} \\ \det_{K_f} \end{matrix} \rho_\ell(\text{Frob}_p | V_\ell(A_f)) = a_p(f)$$

$$\rho_\ell(\text{Frob}_p) = p$$

Indeed, the trace is T_p , but $T_p = a_p$ in $\mathbb{T}_{\mathbb{Q}} / I_f$.

Conclusion Given $f \in S_2(\Gamma_0(N))$ a normalised eigenform,

l prime, $\lambda | l$ in K_f . We constructed

$$\rho_{f,\lambda} : \Gamma_{\mathbb{Q}} \longrightarrow GL_2(K_{f,\lambda})$$

satisfying $\left\{ \begin{array}{l} \text{tr } \rho_{f,\lambda}(\text{Frob}_p) = a_p(f) \\ \det \rho_{f,\lambda}(\text{Frob}_p) = p \end{array} \right. \quad \forall p \nmid Nl.$

We get uniqueness if we require the representation to be semisimple