Note Title 26/01/2024

26/01/2024
L. Furio

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 subgp that contains $\Gamma(N)$ for some $N \geq 1$

Note

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

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

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

Def A function $f : \mathbb{H} \longrightarrow \hat{\mathbb{C}}$ 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 $f : \mathbb{H} \longrightarrow \mathbb{C}$ is a MODULAR FORM if it is holomorphic at the cusps. (I.e., $(cz+d)^{-k} f(z)$ is bounded as $\operatorname{Im} z \longrightarrow \infty$)

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

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

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

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

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 $f(z+N) = f(z) \Rightarrow f(z) = \tilde{f}\big(\underbrace{e^{2\pi i z/N}}_{q_N}\big)$.

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 $q_N \to 0$ iff $f(z) \to 0$ as $\mathrm{Im}\, z \to \infty$. Same analysis for the other cusps.

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

and $\Gamma' \circlearrowright S_k(\Gamma)$ via $\gamma \bullet f := f[\gamma]_k$. Indeed, $\forall \delta \in \Gamma'$,

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

$$= (f[\delta']_k)[\gamma]_k \underset{\substack{\uparrow \\ f \in M_k(\Gamma),\ \delta' \in \Gamma}}{=} f[\gamma]_k$$

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 $\dfrac{\Gamma_0(N)}{\Gamma_1(N)} \simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$

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

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

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

Rmk Every fin-dim'l $\mathbb{C}$-rep of $\left(\mathbb{Z}/N\mathbb{Z}\right)^\times$ 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 $\quad S_k(\Gamma_0(N)) = S_k(\Gamma_1(N), 1)$

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

Double cosets

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

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

- $\forall p, q$ $T_p T_q = T_q T_p$

Proof Matrix calculations

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

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

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

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

$T_{q^2} = (T_q)^2 - q\langle p\rangle$. 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

$$\mathrm{End}(S_k(\Gamma_1(N)))$$

Jacobians

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

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

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

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

This action induces an action on $J(X_1(N))$!

The Manin-Drinfeld theorem

02/02/2024
S. Boscardin

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

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

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: $\Gamma \curvearrowright$ 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 $\Gamma = \Gamma_0(n) = \left\{ M \in SL_2(\mathbb{Z}) \;\middle|\; M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod n \right\}$

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 $\mathrm{Jac}(X_\Gamma)$ is torsion.

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

$$\operatorname{div} f = N(a_1 c_1 + \ldots + a_n c_n)$$

Complements on Hecke operators & Manin symbols

$$T_p \curvearrowright S_2(\Gamma) \simeq \Omega^1_{hol}(X_\Gamma), \qquad T_p \curvearrowright S_2(\Gamma)^\vee$$

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

Recall that $H_1(X_\Gamma, \mathbb{Z}) \hookrightarrow S_2(\Gamma)^\vee \simeq H^0(X_\Gamma, \Omega^1)^\vee$

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

and $\mathrm{Jac}(X_\Gamma) \simeq \dfrac{S_2(\Gamma)^\vee}{H_1(X_\Gamma, \mathbb{Z})}$

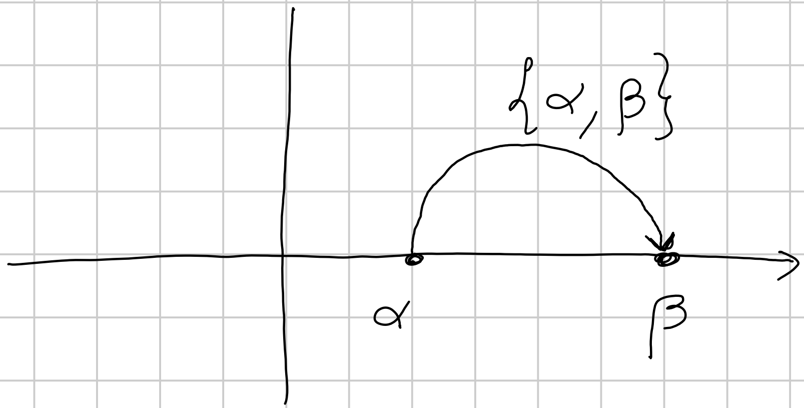
Def Let M_2 be the ab. group generated by the symbols $\{\alpha, \beta\}$ for $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, modulo the (and $\{\alpha, \alpha\} = 0$)

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

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

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

Fix now a level n.

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

$$T_p\{\alpha, \beta\} = \sum_{\ell=0}^{p} \{A_\ell \alpha, A_\ell \beta\} \qquad (\text{for } p \nmid N),$$

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 $X_{\Gamma(n)} \xrightarrow{f} X_\Gamma$,

$$\{\text{cusps}\} \longrightarrow \{\text{cusps}\}$$

which extends to $f_* : \mathrm{Jac}(X_{\Gamma(n)}) \rightleftarrows \mathrm{Jac}(X_\Gamma) : f^*$

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.

<u>Step 2</u>: 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 $p \equiv 1 \; (n)$ and consider ($k = p+1$)

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

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

This implies that $(T_p - k\,\mathrm{Id})\{s_1, s_2\} \in \underbrace{H_1(X_\Gamma, \mathbb{Z})}_{\cong\, \mathbb{Z}^{2g}}$

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 $(T_p - kI)$ is invertible.

Multiplying by the classical adjoint of $T_p - kI$ we get

$$\underbrace{\det(T_p - k\,\mathrm{Id})}_{M} \{s_1, s_2\} \in H_1(X_\Gamma, \mathbb{Z}), \text{ so}$$

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

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

Cusps, again

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

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

$$\bar{\gamma} \longleftrightarrow x$$

where $\gamma x = 0$

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

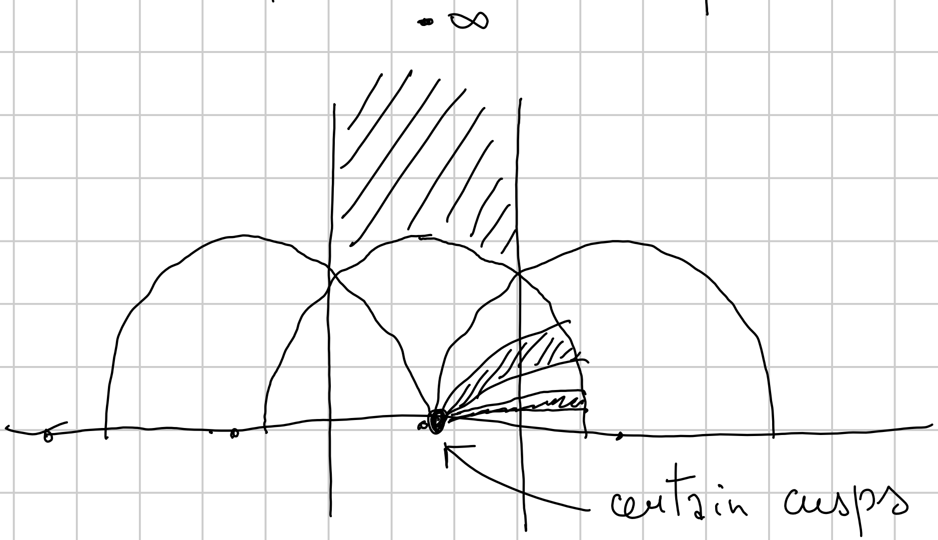
(this is relevant when $\Gamma \supset \Gamma(n)$)

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
(0)	$\{(\neq 0, *)\}$	$p(p-1)$	w

\# pts in the orbit

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



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

$$g_v(\tau) = q^{B_2(a)/2} \cdot e\big(a(b-1)\big) \cdot \left(1 - e(b)\, q^a\right) \prod_{n=1}^{\infty} \left(1 - e(b)\, q^{n+a}\right)\left(1 - e(b)\, q^{n-a}\right)$$

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

Moreover, $g_v(\gamma\tau) = g_{v\gamma}(\tau)\, \varepsilon(\gamma)$, $\quad \varepsilon(\gamma) \in \mu_{12}$

$\forall \gamma \in SL_2(\mathbb{Z})$

$$\Rightarrow \quad g_v^{12n} \in \mathcal{O}(Y(n)) \quad \text{when } v \in \left(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^2$$

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) $\sum_v M_v \equiv 0 \ (12)$

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

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

$M_v = 0$ for $v = (\neq 0, *)$

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

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

So
$$v_\infty(u) = M \cdot \sum \underbrace{1}_{w(c)} \cdot \frac{1}{2} \sum_{i=1}^{p-1} B\left(\left(\frac{1}{p}(0,i)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)_1\right)$$

$$= M \cdot \frac{p-1}{2} B(0) = M \cdot \frac{p-1}{12}$$

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

and $v_0(u) = -v_\infty(u) = -M \frac{p-1}{12}$.

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

We need to choose M. The conditions are

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

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

Rmk • $\Gamma = \Gamma_1(13)$: 12 cusps, 6 are defined over $\mathbb{Q}$.

There is an f such that

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

$\Rightarrow J_1(13)$ 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

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

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

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

$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = +1$

$$= \left(\frac{1}{cNz+d}\right)^{12} \eta(Nz)$$

Raynaud's unique prolongation theorem

21/02/2024
P. Leonardini

Ref Finite flat group schemes (Tate)

Setting K $R = \mathcal{O}_K$ $\kappa = R/\pi$ res. field, π = uniformiser

$$\begin{array}{c} K \\ | \\ \mathbb{Q}_p \end{array} \qquad v(\pi) = 1, \quad v(p) = e$$

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

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

Def (prolongation) Given $G_0 / \operatorname{Spec} K$, a PROLONGATION $G \to \operatorname{Spec} R$ is a finite flat gp scheme over R st. $G_{\operatorname{Spec} K} \simeq G_0$.

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, $\mathcal{E}/\operatorname{Spec} R$ (minimal reg. model), $\overline{\mathcal{E}}/k$. We say that E has good red. if $v(\Delta_{min}) = 0$.

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

Raynaud's thm allows us to show: assume $e < p-1$. Then reduction mod. π gives an injection $\mathcal{E}[m](R) \hookrightarrow \bar{\mathcal{E}}[m](R)$.

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

$$\begin{tikzcd} G_0 \arrow[r] \arrow[d] & \operatorname{Spec} K \\ G \arrow[r] & {} \end{tikzcd}$$

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

$$G(\Gamma) = \operatorname{Hom}(\Gamma, G) = \operatorname{Hom}\Big(\bigsqcup_{g\in\Gamma} \operatorname{Spec}_g R, G\Big) = \prod \operatorname{Hom}(\operatorname{Spec}_g R, G)$$

$$\Phi \in G(\Gamma), \qquad (g : \operatorname{Spec} R \to G) \in \operatorname{Hom}(\operatorname{Spec}_g R, G)$$

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

$$\begin{array}{ccccc} \Gamma_K & \xrightarrow{\sim} & \overline{\Gamma}_K & \longrightarrow & G_0 \\ \parallel & & & & \parallel \\ \prod \operatorname{Spec} K & & & & \prod \operatorname{Spec} K_i \end{array}$$

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

Proof of Raynaud's theorem

Rmk $A \subseteq A_0$: indeed, $R \subseteq K$ and A/R is flat, so

$$\begin{tikzcd} \operatorname{Spec} A_0 = G_0 \arrow[r] \arrow[d] & \operatorname{Spec} K \arrow[d] \\ \operatorname{Spec} A = G \arrow[r, "flat"'] & \operatorname{Spec} R \end{tikzcd}$$

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

Step 0 - define G^+ and G^-

By the remark, $A \subseteq A_0$. Inclusion of coord rings gives an order relation on prolongations: $G_1 \geq G_2 \iff A_2 \leq A_1$.

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

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

Step 1 - reduction to simple G_0

$$\begin{tikzcd}
0 \arrow[r] & G_0' \arrow[r] \arrow[d] & G_0 \arrow[r] \arrow[d] & G_0'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & G' \arrow[r] & G \arrow[r] & G/G' \arrow[r] & 0 \\
0 \arrow[r] & H' \arrow[r] & H \arrow[r] & H/H' \arrow[r] & 0
\end{tikzcd}$$

Assume G_0', G_0'' have UP. Let $G \leq H$ be two prolongations. Then $H' \geq G'$, $H/H' \geq G/G'$, but unique prolong. shows that they are equal $\Rightarrow$ the 5-lemma gives $G \simeq H$.

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

$$\begin{tikzcd} \operatorname{Spec} \overline{K} \arrow[d, dash] & & (G_0)_{\overline{K}} \arrow[ll, "\text{flat}"'] \\ \operatorname{Spec} K_{tame} \arrow[d, dash] & & \\ \operatorname{Spec} K_{nr} & & G_0 \arrow[ll, "\text{flat}"] \end{tikzcd}$$

$$(G_0)_{\overline{K}} = \underbrace{\prod \operatorname{Spec}(\text{finite exts } \overline{K}) = \prod \operatorname{Spec} \overline{K}}_{\text{in char } 0.}$$

$$\{\text{étale gp schemes}/K\} \longleftrightarrow \left\{\begin{array}{l}\text{finite groups}\\ \text{with } \mathcal{G}\text{-action}\end{array}\right\}$$

$$\mathcal{G} = \operatorname{Gal}(\overline{K}/K_{nr})$$

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

and G_0 simple

$$1 \to P \to \mathcal{G} \to \mathcal{G}_{tame} \to 1;$$

note that $\mathcal{G}_{tame}$ is abelian.

Let $H := \{ x \in G(\overline{K}) \mid \sigma x = x \ \ \forall \sigma \in P \} \lhd G(\overline{K})$.

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

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

By simplicity, $H = G(\overline{K})$, and the action of $\mathcal{G}$ factors via $\mathcal{G}_{tame}$.

$\Rightarrow G_0(\overline{k})$ is a $\mathbb{Z}[\mathcal{G}_{tame}]$ - simple module.
abelian

$\Rightarrow G_0(\overline{k}) \simeq \mathbb{Z}[\mathcal{G}_{tame}]/\mathfrak{m}$ — maximal ideal

$\Rightarrow G_0(\overline{k})$ "is" a field $F = \mathbb{F}_{p^r} = \mathbb{F}_q$

We have thus obtained a map $F \longrightarrow \mathrm{End}(G_0(\bar{K}))$, which

$s \longmapsto [s]$

induces an action $F \longrightarrow \mathrm{End}(G_0)$

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 finite flat gp scheme G together with a morphism

$$F \longrightarrow \mathrm{End}(G).$$

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

We extend every $\chi \in M$ to a function $\chi : F \longrightarrow \overline{K}$.
$0 \longmapsto 0$

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

$$(*) \quad \begin{tikzcd} F \arrow[r, "\chi"] \arrow[rr, bend right, "\chi_0"'] & R \arrow[r] & R/\pi R = k \end{tikzcd}$$

χ_0 = hom. of fields

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

$\chi_1, \ldots, \chi_r$ 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 $[s]\, X_i = \chi_i(s) \quad \forall i \in I, \ \forall s \in F$

(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 $G' \longrightarrow G$ correspond to $\begin{array}{l} A \longrightarrow A' \\ X_i \longmapsto a_i X_i' \end{array}$ where $a_i \in R$ satisfy

$$a_{i+1} \delta_i = a_i^p \cdot \delta_i'.$$

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 $G^+ \underset{\neq}{>} G^-$ over R. As $\mathcal{O}_{K_{nr}} / \mathcal{O}_K$ is faithfully flat, we have $G^+ \underset{\neq}{>} G^-$ also over K_{nr}.

We can also assume that G_0 is simple (step 2), hence an $\mathbb{F}_\ell$-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.

The Eichler - Shimura relation

12/04/2024

§ Recap

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

$$\begin{tikzcd} X_0(Np) \arrow[r] \arrow[d] & X_0(N) \\ X_0(N) & \end{tikzcd}$$

$$\begin{tikzcd} \Big(\underset{\text{cyclic } p\text{-isogeny}}{E \xrightarrow{\varphi} E'}, \underset{\text{cyclic subgp order } N}{G} \Big) \arrow[r, mapsto, "g"] \arrow[d, mapsto, "f"] & (E', \varphi(G)) \\ (E, G) & \end{tikzcd}$$

Map on Jacobian:

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

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

  Both objects are free of rank 2 over

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

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

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

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

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

If X is an abelian variety,

$$\begin{tikzcd} X \arrow[rr, "{[p]}"] \arrow[dr, "F"'] & & X \\ & X^{(p)} \arrow[ur, "V"'] & \end{tikzcd}$$

Thm (Eichler–Shimura) p, N distinct primes

$$T_p = F + V \quad \text{mod } p,$$

as elements of $\mathrm{End}(J_0(N)_{\mathbb{F}_p})$.

Proof 1 (algebraic)

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

"The same" holds modulo p.

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

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

$$0 \to C_0 \longrightarrow E[p] \longrightarrow \tilde{E}[p] \longrightarrow 0$$

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 $\varphi : E \longrightarrow E'$ is the quotient mod C_0, then $\tilde{\varphi} : \tilde{E} \longrightarrow \tilde{E}'$ is the Frobenius.

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

$$\begin{tikzcd} \tilde{E} \arrow[r, "\tilde{\varphi}"] \arrow[rr, bend right, "{[p]}"'] & \tilde{E}/\tilde{E}[p] \arrow[r, "\tilde{\varphi}^{\vee}"] & \tilde{E} \end{tikzcd}$$

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

Hence: $$T_p(\tilde{E}, \tilde{G}) = \sum (\tilde{E}', \tilde{\varphi}(\tilde{G}))$$

$$= (\tilde{E}^{(p)}, \tilde{G}^{(p)}) + \sum_{E' \neq E/C_0} (\tilde{E}', \tilde{\varphi}(\tilde{G}))$$

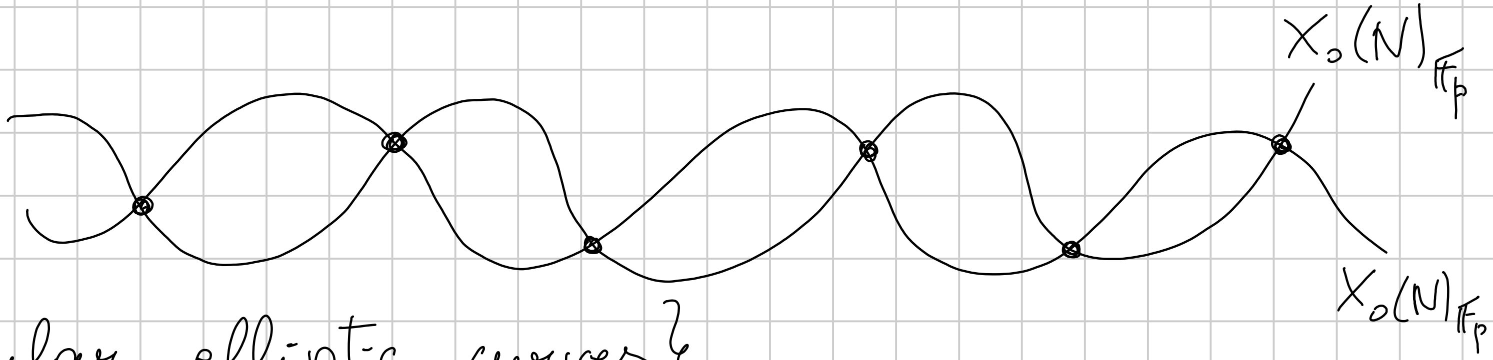
$$= (\tilde{E}^{(p)}, \tilde{G}^{(p)}) + \underbrace{\sum_{E' :\, (\tilde{E}')^{(p)} \cong E} (\tilde{E}', \tilde{\varphi}(\tilde{G}))}_{\text{This is a divisor whose image via Frobenius is } p \cdot (\tilde{E}, \tilde{G})}$$

$$= F(\tilde{E}, \tilde{G}) + V(\tilde{E}, \tilde{G})$$

(+ details to avoid supersingular curves)

Proof 2

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



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

$$\begin{tikzcd}
 & \Sigma \arrow[dl, hook'] \arrow[dr, hook] & \\
X_0(N)_{\mathbb{F}_p} \arrow[dr, "i"] \arrow[dd] & & X_0(N)_{\mathbb{F}_p} \arrow[dl, "j"'] \arrow[dd] \\
 & X_0(Np)_{\mathbb{F}_p} \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X_0(N) & & X_0(N)
\end{tikzcd}$$

$fi = id$

$gj = id$

$gi = F$

$fj = F$

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

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

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

The Shimura construction, Galois representation

$$\begin{array}{ccc} V_\ell(J_0(N)_{\mathbb{Q}}) & \xrightarrow{\sim} & V_\ell(J_0(N)_{\mathbb{F}_p}) \\ \circlearrowleft & & \circlearrowleft \\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & & \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \\ \cup & & \cup \\ \mathrm{Frob}_p & & \mathrm{Frob}_p \end{array}$$

Moreover, $\mathbb{T} \curvearrowright J_0(N) \rightsquigarrow \mathbb{T}_{\mathbb{Q}_\ell} \curvearrowright V_\ell(J_0(N))$

So $V_\ell(J_0(N))$ is a module over $\mathbb{T}_{\mathbb{Q}_\ell}$, free of rk 2, and the action of Frob_p on $V_\ell(J_0(N))$ is given by a 2×2 matrix with coeffs in $\mathbb{T}_{\mathbb{Q}_\ell}$.

Thm
$$\begin{cases} \mathrm{Tr}\left(\rho_\ell(\mathrm{Frob}_p) \mid V_\ell(J_0(N))\right) = T_p \\ \det\left(\qquad\qquad\qquad\qquad \right) = p \end{cases}$$

Proof $T_p = F + V$, $\quad FV = [p] \quad$ (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

$$T_p^\vee = (F+V)^\vee = F^\vee + V^\vee = V + F = T_p$$

- $\varphi : V_\ell \longrightarrow V_\ell^\vee \qquad \varphi(Fx) = V\varphi(x)$

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

- Hence, $\mathrm{tr}(F|V_\ell) = \mathrm{tr}(V|V_\ell^\vee) = \mathrm{tr}\ {}^t\rho(V|V_\ell) = \mathrm{tr}\ \rho(V|V_\ell)$,

  and finally $\underset{\substack{\parallel \\ 2T_p}}{\mathrm{tr}(T_p|V_\ell)} = 2\,\mathrm{tr}(F|V_\ell)$.

$\square$

The Shimura construction

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

Consider $\mathbb{T}_\mathbb{Q} \longrightarrow K_f \longrightarrow 0$

$T \longmapsto$ eigenvalue of T on f

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

The kernel of $\mathbb{T}_{\mathbb{Q}} \twoheadrightarrow K_f$ is denoted by I_f.

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

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

$$T_0 A_f = \frac{T_0 J_0(N)}{I_f T_0 J_0(N)} = T_0 J_0(N) \otimes_{\mathbb{T}_{\mathbb{Q}}} (\mathbb{T}_{\mathbb{Q}}/I_f)$$

$$\simeq \mathbb{T}_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} (\mathbb{T}_{\mathbb{Q}}/I_f) \simeq K_f$$

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,

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

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

2) $\mathrm{Tr}_{K_f}\ \rho_\ell(\mathrm{Frob}_p \mid V_\ell(A_f)) = a_p(f)$

$\det_{K_f}\ \rho_\ell(\qquad\qquad) = p$

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, $\lambda \mid \ell$ in K_f. We constructed

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

satisfying $\begin{cases} \operatorname{tr} \rho_{f,\lambda}(\mathrm{Frob}_p) = a_p(f) \\ \det \rho_{f,\lambda}(\mathrm{Frob}_p) = p \end{cases}$ $\forall p \nmid N\ell$.

We get uniqueness if we require the representation to be semisimple

10/05/2024
L. Furio

Thm A $N > 7$ prime, $f : X_0(N) \longrightarrow A$ st

- A has good red away from N
- $f(0) \neq f(\infty)$
- $\# A(\mathbb{Q}) < +\infty$.

Then no ell. curve defined over $\mathbb{Q}$ has a rational N-torsion pt

Thm B $A/\mathbb{Q}$ ab. var., $N \neq p$ primes, $N > 2$. Suppose:

- A has good red away from N
- A has totally toric red. at N
- the Jordan-Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are all trivial or cyclotomic

Then $\# A(\mathbb{Q}) < +\infty$

~ o ~

Combining these results we get:

Cor $N > 7$, $p \neq N$ primes. Suppose $\exists A/\mathbb{Q}$ with $f : X_0(N) \to A$ st

1) A has good red away from N

2) A has totally toric red at N

3) $f(0) \neq f(\infty)$

4) $JH(p)$: $A[p]$ has JH constituents that are all $\mathbb{Z}/p\mathbb{Z}$ or μ_p

Then no ell. curve $/\mathbb{Q}$ has a rational N-torsion pt.

We want to show that the conditions of this thm are satisfied for all primes $N > 7$. Note that all maps $X_0(N)$ factor via

$$\begin{tikzcd} X_0(N) \arrow[rr, "f"] \arrow[dr, hook] & & A \\ & J_0(N) \arrow[ur, "g"'] & \end{tikzcd}$$

so we might as well replace A with $g(J_0(N))$, so we can look for quotients of $J_0(N)$.

Since $J_0(N)$ has good red away from N (we have more or less proved this) and totally toric red at N (postponed), conditions 1) and 2) are automatic.

Properties of $[0]-[\infty]$

$[0]-[\infty] \in J_0(N)$ is torsion of order dividing $N-1$.

(and it's nontrivial)

Proof If $(0)-(\infty) = \mathrm{div}(f)$, $f : X_0(N) \xrightarrow{\sim} \mathbb{P}^1$, contradiction.

Moreover, $\mathrm{div}\left(\frac{\Delta(z)}{\Delta(Nz)}\right) = (N-1)\left([0]-[\infty]\right)$. More precisely,

- $\Delta(z)$ is a mod form of wt 12, non-vanishing on Δ and having a simple zero at ∞
- $\Delta(Nz)$ is a mod form of wt 12 for $\Gamma_0(N)$, with similar properties

The ratio $\Delta(z)/\Delta(Nz)$ hence descends to $X_0(N)$.

Moreover, for $q = e^{2\pi i z}$, $\Delta(z) = q + \cdots$, $\Delta(Nz) = q^N + \cdots$,

hence $\dfrac{\Delta(z)}{\Delta(Nz)} = q^{-(N-1)} + \cdots$ has a pole of order $N-1$

at ∞. The only other possible pole/zero is at the other

cusp, namely zero, and hence

$$\operatorname{div}\left(\frac{\Delta(z)}{\Delta(Nz)}\right) = (N-1)\left([0]-[\infty]\right)$$

$\square$

Thm Let $\ell \nmid N$ be a prime. $T_\ell\left([0]-[\infty]\right) = (\ell+1)\left([0]-[\infty]\right)$

Proof Recall the Hecke correspondence

$$\begin{tikzcd}
 & X_0(\ell N) \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X_0(N) & & X_0(N)
\end{tikzcd}$$

$[E, C_N \oplus C_\ell]$

$[E, C_N]$ $\qquad$ $\left[E/C_\ell, \dfrac{C_N \oplus C_\ell}{C_\ell}\right]$

* $X_0(N\ell)$ has 4 cusps, $\{ \underbrace{(x,}_{X_0(N)}\underbrace{y)}_{X_0(\ell)} \mid x, y \in \{0, \infty\}\}$

* $f(x,y) = g(x,y) = x$

To see this, lift f, g to $\mathbb{H}$. Then $f = \mathrm{id}$ and $g = [\ell]$, which implies the claim (cusps are elements of $\mathbb{P}^1(\mathbb{Q})$, up to the $\Gamma_0(N)$ - equivalence. For f there's nothing to prove.

For g, note that the 4 cusps are

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} N \\ \ell \end{pmatrix} \quad \begin{pmatrix} \ell \\ N \end{pmatrix},$$

and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \ell \\ 0 \end{pmatrix}, \begin{pmatrix} \ell N \\ \ell \end{pmatrix}, \begin{pmatrix} \ell^2 \\ N \end{pmatrix}$ are equivalent mod N

to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ respectively).

* f has ramification index ℓ at $(*, 0)$
1 at $(0, *)$

$$X_0(N\ell) \longrightarrow X_0(N) \longrightarrow X(1)$$

Ramif. indices at cusps for $X_0(M) \longrightarrow X(1)$ are the indices of $\mathrm{Stab}_{\overline{\Gamma_0(M)}}(\text{cusp})$, so

$$e_{(*,0)} = [\mathrm{Stab}_{(*,0)}\Gamma_0(N) : \mathrm{Stab}_{(*,0)}\Gamma_0(N\ell)],$$

and it's an exercise:

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \overset{?}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ in } \mathbb{P}^1(\mathbb{Q}) \Rightarrow b=0$$

ℓ cases for c

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} a & b \\ N\ell c & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \overset{?}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow b=0$$

Anyway: computations. While Lorenzo explains, I'll write the proof I have in mind:

$$f^{-1}[0] = a(0,0) + b(0,\infty)$$

with $a+b = \deg f = \ell+1$, hence

$$g_* f^* [0] = (\ell+1)[0].$$

Similarly for $[\infty]$.

Construction of the Eisenstein quotient

Looking for: $J_0(N) \longrightarrow A$ with $[0]-[\infty] \neq 0$ in A and A satisfies $JH(p)$. Write

$$J_0(N) \sim \prod A_f \qquad A_f = \frac{J_0(N)}{I_f\, J_0(N)}$$

Let $S = \{ f : A_f \text{ satisfies } JH(p) \}$ and

$$I = \bigcap_{f \in S} I_f \ ;$$

then $A := \dfrac{J_0(N)}{I\, J_0(N)}$ satisfies $JH(p)$. We need $S \neq \emptyset$, or equivalently $A \neq 0$.

We show this by proving that $[0]-[\infty] \neq 0$ in A. Let p be a prime, $p \mid \mathrm{ord}([0]-[\infty])$ in $J_0(N)$. (hence $p \mid N-1$)

⚠ For the rest of this lecture, we ASSUME $\dim A_f = 1$ $\forall f \in S_2(\Gamma_0(N))$

Lemma $f \in S \iff a_\ell(f) - (\ell+1) \equiv 0 \pmod p$ $\forall \ell \neq p$.

Proof $\boxed{\Rightarrow}$ Let $\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ be the Gal rep of A_f, with

$\{\chi_1, \chi_2\} = \{1, \chi\}$. Hence $\mathrm{tr}\, \rho_{A_f, p} \equiv 1+\chi \mod p$,

and $\mathrm{tr}(\mathrm{Frob}_\ell \mid A[p]) \equiv 1 + \chi(\mathrm{Frob}_\ell) \equiv 1+\ell \pmod p$

$\boxed{\Leftarrow}$ Chebotarev, no doubt. Now we think about how. Yes, it's clear:

ρ_p^{ss} — semi-simplification and $1 \oplus \chi$ have the same trace for every Frobenius. By density, ρ_p^{ss} and $1 \oplus \chi$ have the same character. Hence $\rho_p^{ss} \simeq 1 \oplus \chi$, which implies that we have $JH(p)$.

↳ the char. determines a semisimple representation

$\square$

Def $\mathfrak{a} := (p, T_\ell - (\ell+1))$ ideal of $\mathbb{T}_\mathbb{Z}$, the Eisenstein ideal

Lemma $\mathbb{T}/\mathfrak{a} \simeq \mathbb{F}_p$, hence $\mathfrak{a}$ is maximal

Proof $\mathbb{T}/(p, T_\ell - (\ell+1)) \simeq \dfrac{\mathbb{F}_p[T_n]}{(T_\ell - (\ell+1))}$ is a quotient of $\mathbb{F}_p$.

(To show that the quotient is $\neq 0$, we need to

Know $S \neq 0$, in the case $\dim A_f = 1$ $\forall f$, this can be done by hand, but I can't reconstruct the argument in real time. We certainly need to use the p-torsion pt)

Lemma The following are equivalent:

1 * $f \in S$

2 * $I_f \subseteq \mathfrak{a}$

3 * $\mathfrak{a} \longrightarrow \mathbb{T}/I_f$ is not (1)

Proof 2 $\iff$ 3 by maximality, 1 $\iff$ 2 by one of the previous lemmas. $\square$