* Big Galois representations

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

*A graduate student seminar talk at TIFR. The author is partially supported by the NSF grant: DMS 1464106.

§1. Notation

To describe the cyclotomic ordinary big p-adic Hecke algebra, we introduce some notation. Fix

- A prime p (we assume p is odd for simplicity);
- a positive integer N prime to p;
- two field embeddings $\mathbb{C} \hookleftarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$;
- $\Gamma = 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^{\times}$.

Consider $\mathfrak{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$ and

$$\Gamma_1(Np^r) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \middle| d - 1 \equiv c \equiv 0 \mod N \right\}.$$

Take the open curve $Y_r(\mathbb{C}) := Y_1(Np^r)(\mathbb{C}) = \Gamma_1(Np^r)\backslash\mathfrak{H}$ and the compactified one $X_r(\mathbb{C}) := X_1(Np^r)(\mathbb{C}) = \Gamma_1(Np^r)\backslash(\mathfrak{H} \sqcup \mathbf{P}^1(\mathbb{Q}))$.

§2. Classification.

The curve $Y_{r/\mathbb{Q}} := Y_1(Np^r)_{/\mathbb{Q}}$ classifies elliptic curves E with an embedding $\phi : \mu_{Np^r} \hookrightarrow E[p^r] = \mathrm{Ker}(p^r : E \to E)$. Choosing a primitive root of unity $\zeta_{Np^r} \in \mu_{Np^r}$, we identify $\mathbb{Z}/Np^r\mathbb{Z}$ with $\mu_{p^r}(\mathbb{C})$ by $m \mapsto \zeta_{Np^r}^m$. This is plain for $z \in \Gamma_1(Np^r)\backslash\mathfrak{H}$ is mapped to $(\mathbb{C}/2\pi i(\mathbb{Z}+\mathbb{Z}z) \overset{\exp}{=} \mathbb{C}^\times/q^{\mathbb{Z}}, \mu_{Np^r}(\mathbb{C}) \subset \mathbb{C}^\times)$ ($q = \exp(2\pi i z)$).

The completed curve $X_{r/\mathbb{Q}} := X_1(Np^r)$ is the normalization of $\mathbf{P}^1(j)$ in the function field of $Y_{r/\mathbb{Q}}$.

Let $R_i = \mathbb{Z}_{(p)}[\mu_{p^i}]$ and $K_i = \mathbb{Q}[\mu_{p^i}]$ ($i = 1, 2, \ldots, \infty$). We fix an isomorphism $\mathbb{Z}_p(1) = \varprojlim_r \mu_{p^r}(R_\infty)$ choosing a coherent sequence of primitive roots of unity $\zeta_{p^r} \in \mu_{p^r}(R_r)$ such that $\zeta_{p^{r+1}}^p = \zeta_{p^r}$ for all r, and therefore, R_i has a specific primitive root of unity denoted by ζ_{p^i}. We suppose $\zeta_{Np^r} = \zeta_N\zeta_{p^r}$. Write R for R_i and K for its quotient field.

§3. Diamond operators

The group $z \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ acts on $X_{r/\mathbb{Q}}$ by $\phi(\zeta) \mapsto \phi(\zeta^z)$, as $\mathrm{Aut}(\mu_{Np^r}) \cong (\mathbb{Z}/Np^r\mathbb{Z})^\times$.

Thus $\Gamma = 1+p\mathbb{Z}_p = \gamma^{\mathbb{Z}_p}$ ($\gamma = 1+p$) acts on X_r (and its Jacobian $J_{r/\mathbb{Q}}$) through its image in $(\mathbb{Z}/Np^r\mathbb{Z})^\times$.

For $s > r \geq 0$, we define another modular curve $Y^r_{s/\mathbb{Q}}$ by the quotient of Y_s by $(1+p^r\mathbb{Z}_p)/(1+p^s\mathbb{Z}_p) \subset (\mathbb{Z}/Np^s\mathbb{Z})^\times$ and define $X^r_{s/R}$ to be the normalization of $\mathbf{P}(j)_{/R}$ in the function field $K(Y^r_{s/\mathbb{Q}})$.

$X^r_{s/\mathbb{Q}}(\mathbb{C})$ is given by $\Gamma^r_s \backslash (\mathfrak{H} \sqcup \mathbf{P}^1(\mathbb{Q}))$ for $\Gamma^r_s = \Gamma_1(Np^r) \cap \Gamma_0(p^s)$ ($s > r \geq 0$).

§4. Hecke operators

$\mathfrak{H} \ni z \mapsto z/p$ induces a projection $\pi' : X^r_{r+1} \to X_r$. Then for a prime divisor $[P]$ on X_r and for the natural projection $\pi : X^r_{r+1} \twoheadrightarrow X_r$, the map $[P] \mapsto \sum_{Q \in \pi^{-1}(P)} [\pi'(Q)]$ give a Hecke operator $U(p) \in \mathrm{End}(J_r)$.

For each congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, we define the modular curve $X(\Gamma)(\mathbb{C}) = \Gamma \backslash (\mathfrak{H} \sqcup \mathbf{P}^1(\mathbb{Q}))$. In this setting, we always assume $\Gamma = \Gamma_1(Np^r) \cap \Gamma_0(l^m)$ for a prime l, and then $X(\Gamma)$ is canonically defined over $\mathbb{Q}$.

Write N_l for the l-primary part of N. Similarly for the two projections $\pi_l, \pi'_l : X(\Gamma_0(lN_l) \cap \Gamma_1(Np^r)) \rightrightarrows X_r$ gives rise to the Hecke operator $T(l) \in \mathrm{End}(J_{r/\mathbb{Q}})$. Writing $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} \Gamma = \bigsqcup_\alpha \Gamma\alpha$, lifting P to $z \in \mathfrak{H}$, $T(l)$ sends a divisor $[z]$ to $\sum_\alpha [\alpha(z)]$ in J_r.

§5. U-isomorphisms.

For $\mathbb{Z}[U]$-modules M and M', we call a $\mathbb{Z}[U]$-linear map $f : M \to M'$ a U-injection (resp. a U-surjection) if Ker(f) is killed by a power of U (resp. Coker(f) is killed by a power of U).

If f is an U-injection and U-surjection, we call f is a U-isomorphism.

In other words, f is a U-injection (resp. a U-surjection, a U-isomorphism) if after tensor with $\mathbb{Z}[U, U^{-1}]$, it becomes an injection (resp. a surjection, an isomorphism). In terms of U-isomorphisms, we describe briefly the facts we study.

§6. Coset identity.

We have the following coset identity:

$$\Gamma_s^r\backslash\Gamma_s^r \begin{pmatrix} 1 & 0 \\ 0 & p^{s-r} \end{pmatrix} \Gamma_1(Np^r) = \left\{ \begin{pmatrix} 1 & a \\ 0 & p^{s-r} \end{pmatrix} \middle| a \mod p^{s-r} \right\}$$
$$= \Gamma_1(Np^r)\backslash\Gamma_1(Np^r) \begin{pmatrix} 1 & 0 \\ 0 & p^{s-r} \end{pmatrix} \Gamma_1(Np^r).$$

Write $U_r^s(p^{s-r}) : J_r^s \to J_r$ for the Hecke operator of $\Gamma_r^s \alpha_{s-r} \Gamma_1(Np^r)$ for $\alpha_m = \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix}$.

The Hecke operator of this coset is induced by the correspondence of divisors

$$\mathrm{Div}(X(\Gamma)) \ni [z] \mapsto \sum_a \left[\frac{z+a}{p^{s-r}} \right] \in \mathrm{Div}(X(\Gamma'))$$

for $(\Gamma, \Gamma') = (\Gamma_s^r, \Gamma_1(Np^r))$ and $(\Gamma_1(Np^r), \Gamma_1(Np^r))$.

§7. $U(p)$-isomorphism.

The above coset identity implies the following commutative diagram from the above identity, first over $\mathbb{C}$, then over $\mathbb{Q}$:

$$\begin{array}{ccc} J_{r/K} & \xrightarrow{\pi^*} & J^r_{s/K} \\ \downarrow u & \swarrow u' & \downarrow u'' \\ J_{r/K} & \xrightarrow{\pi^*} & J^r_{s/K}, \end{array} \qquad (1)$$

where the middle u' is given by $U^s_r(p^{s-r})$ and u and u'' are $U(p^{s-r})$. Here $\pi^*([P]) = \sum_{Q\in\pi^{-1}(P)}[Q]$. Thus

$$\pi^* : J_{r/K} \to J^r_{s/K} \text{ is a } U(p)\text{-isomorphism} \qquad \text{(u)}$$

(for the projection $\pi : X^r_s \to X_r$).

§8. Jacobians

For a curve $X_{/\overline{k}}$ over an algebraically closed field, each meromorphic function $f : X \to \mathbf{P}^1(\overline{k})$ gives divisor $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)[P]$ for the order $\mathrm{ord}_P(f)$ of poles and zeros of f at P.

Then $J(X) = \mathrm{Div}^0(X)/P(X)$, where $P(X) = \{\mathrm{div}(f) | f \in \overline{k}(X)\}$ and $\mathrm{Div}^0(X) = \{D = \sum_P m_P[P] | \deg(D) = \sum_P m_P = 0\}$.

Cover $X(\mathbb{C}) = \bigcup_i U_i$ by a simply connected open sets U_i, a divisor D restricted to U_i is of the form $D \cap U_i = \mathrm{div}(f_i)$ for a meromorphic function $f_i : U_i \to \mathbf{P}^1(\mathbb{C})$. Then $(f_i/f_j \in \mathcal{O}_X^\times(U_i \cap U_j))_{i,j}$ is a Čech 1-cocycle; so, $\mathrm{Div}(X)/P(X) \cong \check{H}^1(X, \mathcal{O}_X^\times)$. From the exact sequence of sheaf cohomology $0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{\exp(2\pi i\ )} \mathcal{O}_X^\times \to 0$ we have a long sequence

$$0 \to H^1(X, \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^\times) \xrightarrow{\deg} H^2(X, \mathbb{Z}) = \mathbb{Z}.$$

Thus $J(X)(\mathbb{C}) = H^1(X, \mathcal{O}_X)/H^1(X, \mathbb{Z})$.

§9. Hodge sequence.

By the Hodge sequence

$$0 \to H^0(X, \Omega_{X/\mathbb{C}}) \to H^1_{DR}(X, \mathbb{C}) \to H^1(X, \mathcal{O}_X) \to 0,$$

we have $H^1(X, \mathcal{O}_X) \cong H^1(X, \mathbb{R})$ as real vector space; so,

$$J(X)(\mathbb{C}) \cong H^1(X, \mathbb{R})/H^1(X, \mathbb{Z})$$

as a topological group. This combined wirh the exact sequence

$$0 \to H^1(X, \mathbb{Z}) \to H^1(X, \mathbb{R}) \to H^1(X, \mathbf{T}) \xrightarrow{\text{deg}} H^2(X, \mathbb{Z}) = \mathbb{Z},$$

we have $J(X)(\mathbb{C}) \hookrightarrow H^1(X, \mathbf{T})$ for $\mathbf{T} = \mathbb{R}/\mathbb{Z}$.

§10. Inflation-Restriction.

Since $\Gamma_s^r \triangleright \Gamma_1(Np^s) = \Gamma_s^s$, we may consider the finite cyclic quotient group $C := \frac{\Gamma_s^r}{\Gamma_1(Np^s)}$. By the inflation restriction sequence, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
H^1(C,\mathbf{T}) & \overset{\hookrightarrow}{\longrightarrow} & H^1(Y_s^r,\mathbf{T}) & \longrightarrow & H^1(Y_s,\mathbf{T})^{\gamma^{p^{r-1}}=1} & \longrightarrow & H^2(C,\mathbf{T}) \\
\| \uparrow & & \| \uparrow & & \| \uparrow & & \uparrow \| \\
H^1(C,\mathbf{T}) & \overset{\hookrightarrow}{\longrightarrow} & H^1(\Gamma_s^r,\mathbf{T}) & \longrightarrow & H^1(\Gamma_s^s,\mathbf{T})^{\gamma^{p^{r-1}}=1} & \longrightarrow & H^2(C,\mathbf{T}) \\
\uparrow & & \cup \uparrow & & \uparrow \cup & & \uparrow \\
? & \longrightarrow & J_s^r(\mathbb{C}) & \longrightarrow & J_s(\mathbb{C})[\gamma^{p^{r-1}}-1] & \longrightarrow & ?.
\end{array}$$

§11. Another $U(p)$-isomorphism.

Since C is a finite cyclic group of order p^{s-r} (with generator g) acting trivially on $\mathbf{T}$, we have $H^1(C,\mathbf{T}) = \mathrm{Hom}(C,\mathbf{T}) \cong C$ and

$$H^2(C,\mathbf{T}) = \mathbf{T}/(1+g+\cdots+g^{p^{s-r}-1})\mathbf{T} = \mathbf{T}/p^{s-r}\mathbf{T} = 0.$$

By the same token, for $\mathbb{T}_p := \mathbb{Q}_p/\mathbb{Z}_p$, we get $H^2(C,\mathbb{T}_p) = 0$. By computing explicitly the double coset action of $U(p)$, we confirm that $U(p)$ acts on $H^1(C,\mathbf{T})$ and $H^1(C,\mathbb{T}_p)$ via multiplication by its degree p, and hence $U(p)^{s-r}$ kill $H^1(C,\mathbf{T})$ and $H^1(C,\mathbb{T}_p)$. Hence

$$J_s^r \xrightarrow{\pi^*} J_s[\gamma^{p^{r-1}} - 1] \text{ is a } U(p)\text{-isomorphism over } \mathbb{Q} \qquad \text{(u1)}$$

for $J_s[\gamma^{p^{r-1}} - 1] = \mathrm{Ker}(\gamma^{p^{r-1}} - 1) = J_s(\mathbb{C})^{\Gamma^{p^{r-1}}}$. If we replace $\mathbf{T}$ by $\mathbb{T}_p$, we get an $U(p)$-isomorphism of p-divisible groups also

$$J_s^r[p^\infty] \xrightarrow{\pi^*} J_s[\gamma^{p^{r-1}} - 1][p^\infty] \ (U(p)\text{-isomorphism over } \mathbb{Q}).$$

§12. Ind-Barsotti–Tate groups.

Let

$$J_r[p^\infty] = \{x \in J_r(\mathbb{C}) | p^n x = 0 \exists n > 0\} \hookrightarrow H^1(X_r, \mathbb{T}_p).$$

Define the ordinary projector e in $\mathrm{End}(J_r[p^\infty]) = \mathrm{End}(J_r) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ by $e = \lim_{n\to\infty} U(p)^{n!}$, which is an idempotent (i.e., $e^2 = e$). More generally, for any $\mathbb{Z}_p$-module M on which $U(p)$ and e acts, we put $M^{\mathrm{ord}} = e(M)$; so, M^{ord} is a direct summand of M. If we have an $U(p)$-isomorphism $M \to L$, then $M^{\mathrm{ord}} \cong L^{\mathrm{ord}}$.

Put $\mathcal{G}_r = J_r[p^\infty]^{\mathrm{ord}}$ which is a Barsotti–Tate group over $\mathbb{Q}$ (i.e., a p-divisible group with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). Put $\mathcal{G} = \varinjlim_r \mathcal{G}_r$ over which

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim_m \mathbb{Z}_p[\Gamma/\Gamma^{p^m}] \cong \mathbb{Z}_p[[T]]$$

$(\gamma = 1 + p \mapsto t = 1 + T)$ acts by endomorphsms.

§13. $U(p)$-isomorphisms $J_s^r \to J_r$ and $J_s[\gamma^{p^{r-1}} - 1] \to J_s^r$.

From the two $U(p)$-isomorphisms $J_s^r \to J_r$ and $J_s[\gamma^{p^{r-1}} - 1] \to J_s^r$, we get the controllability

$$\mathcal{G}_s[\gamma^{p^{r-1}} - 1] = J_s[p^\infty][\gamma^{p^{r-1}} - 1]^{\mathrm{ord}} = J_r[p^\infty]^{\mathrm{ord}} = \mathcal{G}_r.$$

For each character $\varepsilon : \Gamma/\Gamma^{p^{r-1}} \to \mu_{p^\infty}$, by the inflation and restriction sequence, we have that

$$\begin{aligned}\mathcal{G}_{\mathbb{Q}}[p^n](\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)] &\cong J_r[p^n](\overline{\mathbb{Q}})^{\mathrm{ord}} \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)] \\ &\cong H^1(X_r^1, \mathbb{T}_p(\varepsilon))^{\mathrm{ord}},\end{aligned}$$

where $\mathbb{T}_p(\varepsilon)$ is a Γ_r^1-module isomorphic to $\mathbb{T}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon]$ on which Γ_r^1 acts by ε. Thus the group $\mathcal{G}_{\mathbb{Q}}(\overline{\mathbb{Q}}) \otimes \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)]$ is a nontrivial p-divisible group.

§14. Co-freeness over Λ

Taking the Pontryagin dual $T := \mathcal{G}(\overline{\mathbb{Q}})^*$, the residue module $T/\mathfrak{m}T$ for the maximal ideal $\mathfrak{m}$ of Λ is the dual of $J_1[p]^{\mathrm{ord}}$.

By Nakayama's lemma, we find a surjection $\pi : \Lambda^{2j} \twoheadrightarrow T$ for $2j = \dim_{\mathbb{F}_p} J_1[p]^{\mathrm{ord}}$. Then for a prime $P = P_\varepsilon := (\gamma - \varepsilon(\gamma)) \cap \Lambda$, T/PT is the dual of $\mathcal{G}_{\mathbb{Q}}[P]$ which is $\mathbb{Z}_p$-free of rank $2j$.

Thus $\mathrm{Ker}(\pi) \subset P_\varepsilon \Lambda^{2j}$. Moving ε around, from $\bigcap_\varepsilon P_\varepsilon \Lambda^{2j} = \{0\}$, we find that $T \cong \Lambda^{2j}$; so, we get a Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_\Lambda(T) \cong GL_{2j}(\Lambda).$$

§15. Hecke algebra

Let

$$\mathbf{h} = \Lambda[T(l), U(p)|l \text{ primes different from } p\}.$$

Then $\mathbf{h}/(\gamma^{p^{r-1}} - 1)\mathbf{h} \hookrightarrow \mathrm{End}(\mathcal{G}_r)$ essentially by $\mathcal{G}_r = \mathcal{G}[\gamma^{p^{r-1}} - 1]$. Thus

$$\mathbf{h}/(\gamma^{p^{r-1}} - 1)\mathbf{h} \cong h_r^{\mathrm{ord}} \text{ and } \mathbf{h} \otimes_{\Lambda, t \mapsto \varepsilon(\gamma)} \mathbb{Z}_p[\varepsilon] \cong h_\varepsilon^{\mathrm{ord}},$$

where $h_\varepsilon = \mathbb{Z}_p[\varepsilon][U(p), T(l)]_l \subset \mathrm{End}_{\mathbb{Z}_p}(H^1(X_r, \mathbb{T}_p))$ and $h_r = \mathbb{Z}_p[T(l), U(p)]_l \subset \mathrm{End}(J_r) \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Thus for any algebra homomorphism $P : \mathbf{h} \to \overline{\mathbb{Q}}_p \in \mathrm{Spec}(\mathbf{h})(\overline{\mathbb{Q}}_p)$ with $P(\gamma^{p^{r-1}} - 1) = 0$, we have a Hecke eigenform $f_P \in S_2(\Gamma_1(Np^r))$ such that $f_P|T(l) = P(T(l))f_P$ for all prime l with

$$f_P = \sum_{n \geq 1} P(T(n))q^n.$$

Such point P is called **arithmetic**.

§16. Analytic families

Each irreducible component $\text{Spec}(\mathbb{I}) \subset \text{Spec}(\mathbf{h})$ gives rise to a family of Hecke eigenform

$$\mathcal{F}_{\mathbb{I}} = \{f_P | P \in \text{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)\}$$

whose q-expansion coefficients are p-adic nalytic on $\text{Spf}(\mathbb{I})$.

Each f_P for arithmetic P has Galois representation

$$\rho_P : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{I}/P)$$

unramified outside Np satisfying

$$\text{Tr}(\rho_P(Frob_l)) = P(T(l)) = a(l, f_P).$$

This is the Galois representation of f_P constructed by Eichler–Shimura if P is arithmetic.

§17. Big representations.

In most cases, $T_{\mathbb{I}} := T \otimes_{\mathbf{h}} \mathbb{I} \cong \mathbb{I}^2$ and by the Galois action on T, we get

$$\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{I})$$

unramified outside Np. By definition,

$$P \circ \rho_{\mathbb{I}} \cong \rho_P.$$

Then $\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = T(l)|_{T_{\mathbb{I}}}$ for all primes l.

Thus we get a family of Galois representations

$$\Phi_{\mathbb{I}} = \{\rho_P | P \in \mathrm{Spec}(\mathbb{I})\}$$

for all point $P \in \mathrm{Spec}(\mathbb{I})$