* Local one generator theorem.

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

Columbia RTG Seminar, 11/19/2020.

*The author is partially supported by the NSF grant: DMS 1464106.

Abstract: The universal modular ordinary representation $\rho_{\mathbb{T}}$ deforming a p-distinguished modulo p representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ for a finite field $\mathbb{F}$ of characteristic $p \geq 3$ has values in the Hecke algebra $\mathbb{T}$ which is an algebra free of finite rank over $\Lambda = W[[T]]$ for $W = W(\mathbb{F})$ (the ring of Witt vectors with coefficients in $\mathbb{F}$). We want to compute $\rho_{\mathbb{T}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ very explicitly.

§**0. Set-up, assumptions and notations.** Let $\mathbb{T}$ be a local ring free of finite rank over the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[T]]$ and let $\rho = \rho_{\mathbb{T}}$ be an ordinary Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{T})$. Ordinarity means that for the decomposition group $D = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ $\rho_{\mathbb{T}}|_D = \left(\begin{smallmatrix}\boldsymbol{\epsilon} & * \\ 0 & \boldsymbol{\delta}\end{smallmatrix}\right)$ with unramified $\boldsymbol{\delta}$. Let $I \triangleleft D$ be the wild inertia subgroup. By local class field theory $\rho_{\mathbb{T}}|_I$ factors through $\mathrm{Gal}(\mathbb{Q}_p[\mu_{p^\infty}]/\mathbb{Q}_p)$, we assume that $\boldsymbol{\epsilon}([1+p, \mathbb{Q}_p]) = t = 1 + T \in \mathbb{Z}_p[[T]]$ which determines the p-profinite part of $\boldsymbol{\epsilon}|_I$.

Consider the composite $\mathcal{K}_\infty$ of the unramified $\mathbb{Z}_p$-extension k_∞/k and the cyclotomic $\mathbb{Z}_p$-extension K_∞ over a p-adic field k. Let $\Gamma = \mathrm{Gal}(K_\infty/k)$ and $\Upsilon = \mathrm{Gal}(k_\infty/k)$. Taking k to be splitting field of $\overline{\rho} := \rho_{\mathbb{T}} \mod \mathfrak{m}_{\mathbb{T}}$ restricted to D, then for the stabilizer D_k of k, we find that $\rho_{\mathbb{T}}|D_k$ factors through $\mathrm{Gal}(\mathcal{M}/k)$ for the maximal p-abelian p-ramified extension $\mathcal{M}/\mathcal{K}_\infty$. Thus we study the maximal quotient Y of $\mathrm{Gal}(\mathcal{M}/\mathcal{K}_\infty)$ on which Γ and Υ commute. Our goal is to show $Y = W[[\Gamma \times \Upsilon]]\theta$ for a finite extension $W_{/\mathbb{Z}_p}$. Write $d = [k : \mathbb{Q}_p]$.

§**1. A theorem of Iwasawa.** Let $\Gamma = \gamma^{\mathbb{Z}_p}$ and put $K_n := K_\infty^{\Gamma^{p^n}}$ with integer ring $\mathfrak{O}_n$. Let L (resp. L_n) be the maximal abelian p-extension of K_∞ (resp. K_n); so, $L_n \supset K_\infty$.

Theorem 1 (Iwasawa). *Let* $\Lambda := \mathbb{Z}_p[[\Gamma]]$ *and* $X :=$ Gal(L/K_∞). *As* Λ*-modules, we have*

$$X \cong \begin{cases} \Lambda^d & \text{if } |\mu_{p^\infty}(K_\infty)| = 1, \\ \Lambda^d \oplus \mathbb{Z}_p(1) & \text{otherwise.} \end{cases}$$

We split $\mathrm{Gal}(L/k) = \Gamma \ltimes X$. Then the commutator subgroup of $\mathrm{Gal}(L/K_n)$ is given by $(\gamma^{p^n} - 1)X$. Thus

$$X_n = \mathrm{Gal}(L_n/K_\infty) = X/(\gamma^{p^n} - 1)X \quad \text{and} \quad X = \varprojlim_n X_n.$$

For a multiplicative module M, let $\widehat{M} := \varprojlim_m M/M^{p^m}$.

§2. **Proof.** We only prove the case when $\mu_{p^\infty} = \{1\}$. By local class field theory, noting $dp^n = [K_n : \mathbb{Q}_p]$,

$$\mathrm{Gal}(L_n/K_n) \cong \widehat{K}_n^\times \cong \mu_{p^\infty}(K_n) \times \mathbb{Z}_p^{dp^n+1} = \mathbb{Z}_p^{dp^n+1}$$

which implies, from $\mathrm{Gal}(L_n/K_n) \twoheadrightarrow \Gamma_n \cong \mathbb{Z}_p$,

$$X/(\gamma^{p^n} - 1)X = X_n \cong \mathbb{Z}_p^{dp^n}, \tag{1}$$

and by Nakayama's lemma applied to $n = 0$, we have a Λ-linear surjection $\Lambda^d \twoheadrightarrow X$.

Take $n > 0$. Then

$$\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]]^d = \Lambda^d/(\gamma^{p^n} - 1)\Lambda^d \cong X_n \cong \mathbb{Z}_p^{dp^n}.$$

comparing the $\mathbb{Z}_p$-rank of the two sides, we have $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]]^d \cong X_n$, and passing to the limit, we get $\Lambda^d \cong X$. □

For a general $\mathbb{Z}_p$-extension K_∞/k with $|\mu_{p^\infty}(K_\infty)| < \infty$, we have an exact sequence $X \hookrightarrow \Lambda^d \twoheadrightarrow \mu_{p^\infty}(K_\infty)$ of Λ-modules.

§3. **A Corollary.** We now assume that $k/\mathbb{Q}_p$ is a finite abelian extension with $G = \mathrm{Gal}(k/\mathbb{Q}_p)$ and $p \nmid [k : \mathbb{Q}_p]$. Then $L/\mathbb{Q}_p$ is a Galois extension and $\mathrm{Gal}(L/\mathbb{Q}_p) = (\Gamma \times \mathrm{Gal}(k/\mathbb{Q}_p)) \ltimes X$. Thus X is naturally a $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$-module. Note

$$\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] = \Lambda[\mathrm{Gal}(k/\mathbb{Q})].$$

Corollary 1. *Suppose* $p \nmid [k : \mathbb{Q}_p]$. *Then*

$$X \cong \begin{cases} \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] & \text{if } \mu_p(k) = 1, \\ \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] \oplus \mathbb{Z}_p(1) & \text{if } \mu_p(k) \neq 1 \end{cases}$$

as $\Lambda[\mathrm{Gal}(k/\mathbb{Q}_p)]$*-modules. Thus for each character* η *of* $\mathrm{Gal}(k/\mathbb{Q}_p)$ *with values in he ring* $\mathbb{Z}_p[\eta] =: W$ *generated by the values of* η*, we have*

$$X[\eta] = X \otimes_{\mathbb{Z}_p[G]} \eta \cong \begin{cases} W[[\Gamma]] & \text{if } \eta \neq \omega, \\ \mathbb{Z}_p[[\Gamma]] \oplus \mathbb{Z}_p(1) & \text{if } \eta = \omega \end{cases}$$

as $\mathrm{Gal}(K_\infty/\mathbb{Q}_p)$*-modules. Here* ω *is the Teichmüller character and* $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_p)$ *acts on* W *via* η*.*

§4. **A version for a $\mathbb{Z}_p^2$-extension.** Recall $\mathcal{K}_n = K_\infty k_n$ and $\Upsilon := \mathrm{Gal}(k_\infty/k) \cong \mathrm{Gal}(\mathcal{K}_\infty/K_\infty)$. Let $\mathcal{L}$ be the maximal abelian p-extension of $\mathcal{K}_\infty$. Set $\mathcal{Y} := \mathrm{Gal}(\mathcal{L}/\mathcal{K}_\infty)$. Pick a lift $\phi \in \mathrm{Gal}(\mathcal{L}/k)$ (a Frobenius) of a generator of Υ with $\phi|_{\mathcal{K}_\infty}$ generating Υ and a lift $\tilde{\gamma} \in \mathrm{Gal}(\mathcal{L}/k)$ of the generator γ of $\mathrm{Gal}(K_\infty/k) = \Gamma$. The commutator $\tau := [\phi, \tilde{\gamma}]$ acts on $\mathcal{Y}$ by conjugation, and $(\tau - 1)x := [\tau, x] = \tau x \tau^{-1} x^{-1}$ for $x \in \mathcal{Y}$ is determined independent of the choice of γ and ϕ. Define $\mathcal{M} \subset \mathcal{L}$ and $\mathcal{M}_n \subset \mathcal{L}_n$ by the fixed field of $(\tau - 1)\mathcal{Y}$ (i.e., the fixed field of τ), which is independent of the choice of $\tilde{\gamma}$ and ϕ. Let $Y = \mathrm{Gal}(\mathcal{M}/\mathcal{K}_\infty) = \mathcal{Y}/(\tau - 1)\mathcal{Y}$.

Theorem 2. (1) *The restriction map $Y \to X$ induces an isomorphism of $Y/(\phi - 1)Y \cong \mathfrak{a}$ for the augmentation ideal $\mathfrak{a}$ of the factor $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] \subset X$.*

(2) *For the character $\eta : \mathrm{Gal}(k/\mathbb{Q}_p) \to W^\times$ in* Corollary 1, *the factor $Y[\eta] = W[[\Gamma \times \Upsilon]]\theta_\eta$ for $\theta_\eta \in Y[\eta]$.*

What is the exact structure of $W[[\Gamma \times \Upsilon]]$-module $Y[\eta]$?

§**5. Proof.** (1): For simplicity, we suppose $\mu_p(k) = 1$. We have an exact sequence: $Y_\infty/(\phi-1)Y_\infty \hookrightarrow Y_0 \xrightarrow[\text{onto}]{\text{Res}} \mathrm{Gal}(K_\infty/k) = \mathbb{Z}_p$. Since $Y_0 \cong \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q}_p)]]$, the image of $Y_\infty/(\phi-1)Y_\infty$ is $\mathfrak{a}$.

Proof of (2). Note that $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q}_p)]] = \bigoplus_\chi \mathbb{Z}_p[\chi][[\Gamma]]$ for χ running over all characters of $\mathrm{Gal}(k/\mathbb{Q})$ (up to Galois conjugation). Every factor has one generator over the Iwasdawa algebra. Then $\mathfrak{a} = (\gamma-1)\mathbb{Z}_p[[\Gamma]] \oplus \bigoplus_{\chi\neq 1} \mathbb{Z}_p[\chi][[\Gamma]]$. Thus $Y[\eta]/(\phi-1)Y[\eta] \cong W[[\Gamma]]$ or $(\gamma-1)\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[\Gamma]]$ as $\mathbb{Z}_p[\eta][[\Gamma]]$-modules by the assertion (1). □

For the splitting field k of a representation $\overline{\rho}$ of D_p, writing $\rho_{\mathbb{T}}([p,\mathbb{Q}_p]) = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$, we have an exact sequence

$$I \hookrightarrow \mathrm{Gal}(F(\rho_{\mathbb{T}})/k) \twoheadrightarrow \mathrm{Gal}(k_\infty/k).$$

By Theorem 2, for $\theta \in \mathbb{T}$, $\Lambda[a^2]\theta \hookrightarrow \rho_{\mathbb{T}}(I) \twoheadrightarrow \mathrm{Gal}(K_\infty/k)$ is exact. **What is this θ? Any arithmetic meaning of θ?**