<table>
<thead>
<tr>
<th>Title</th>
<th>Integral representations of Galois groups of local fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Yamagata, Shuji</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1996), 971: 145-152</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1996-10</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/60691">http://hdl.handle.net/2433/60691</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
<tr>
<td>Publisher</td>
<td>Kyoto University</td>
</tr>
</tbody>
</table>
§ 0. Notations

Let $K$ be a local field (not necessarily of characteristic 0) with algebraically closed residue field of characteristic $p > 0$. In this paper, a separable extension of $K$ is supposed to be contained in some fixed separable closure $\overline{K}$ of $K$ with the Galois group $G = \text{Gal}(\overline{K}/K)$. Let $K_\infty/K$ be an abelian extension whose Galois group $\Gamma = \text{Gal}(K_\infty/K)$ has a subgroup of finite index $\Gamma_0 \cong \mathbb{Z}_p$. Denote by $K_n$ the subfield of $K_\infty$ fixed by $\Gamma_n = \Gamma_0^{p^n}$. For a finite extension $F/K$, let $\pi_F$ be a prime element of $F$ and $v_F$ the discrete valuation of $F$ normalized by $v_F(\pi_F) = 1$. Especially put $\pi_n = \pi_{K_n}$, $\pi = \pi_K$ and $v = v_K$. Let $C$ be the completion of $\overline{K}$ with respect to the valuation (we also denote it by $v$) which extends $v$ if $K$ is of characteristic 0. Let $\mathcal{O}(F)$ be the ring of integers of an extension $F/K$. Especially put $\mathcal{O}_\infty = \mathcal{O}(K_\infty)$, $\mathcal{O}_n = \mathcal{O}(K_n)$, $\mathcal{O} = \mathcal{O}(K)$ and $\mathcal{O}_C = \mathcal{O}(C)$. For a product $R$ of finite separable extensions of $K$, let $\mathcal{O}(R)$ be the product of the rings of integers of the factors i.e. the unique maximal order of $R$. Put $F_{\otimes m} = F \otimes_K K_m$.

§ 1. Integral representations associated with field extensions

In § 1, we assume that $\Gamma = \Gamma_0 \cong \mathbb{Z}_p$.

Let $F/K$ be a finite Galois $p$-extension with Galois group $H = \text{Gal}(F/K)$. 

- **Galois** groups of local fields
- **Integral representations** of Galois groups of local fields
- Shuji Yamagata

東京電機大学理工学部。山形周二（Shuji Yamagata）
By an $\mathcal{O}(F)$-semi-linear representation $M$ of $H$, we mean a free $\mathcal{O}(F)$-module of finite rank on which $H$ acts semi-linearly. Sen defined invariants for $\mathcal{O}(F)$-semi-linear representations in [5]: For $0 \neq x \in M \otimes_{\mathcal{O}(F)} F$, let
\[ \text{Ord}_M x = \max\{ t \in \mathbb{Z} \mid x \pi_F^{-t} \in M \}. \]

By a reduced basis of $M^H$ we mean an $\mathcal{O}$-basis $\{x_i\}$ of $M^H$ satisfying the condition $\text{Ord}_M(\sum c_i x_i) = \min_i \{\text{Ord}_M c_i x_i\}$ whenever the $c_i$'s belong to $K$. The orders of the members of a reduced basis of $M^H$ are called the orders of $M$. We remark that these numbers, together with their multiplicities, are independent of the choice of the reduced basis.

We attach to any finite extension $E/K$ the $\mathcal{O}_m$-semi-linear representation $\mathcal{O}(E_{\otimes m})$ of $\Gamma/\Gamma_m$ given by its Galois action on the right factor $K_m$. For finite Galois extensions, Sen [5] and Destrempes[1] proved:

**Theorem 1.** Let $E/K$ and $E'/K$ be two finite Galois extensions. Then $E = E'$ if and only if, for some sufficiently large $m$, the $\mathcal{O}_m$-semi-linear representations of $\Gamma/\Gamma_m$ on the additive groups $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ are isomorphic.

In [8](cf. [8], Remark 2), for any separable extensions, we proved:

**Theorem 2.** Let $E/K$ and $E'/K$ be two finite separable extensions. Assume that, for some sufficiently large $m$ (cf. §1, Remark 1), the $\mathcal{O}_m$-semi-linear representations of $\Gamma/\Gamma_m$ on the additive groups $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ are isomorphic. Then the Galois closures of $E/K$ and $E'/K$ coincide and $\deg E/K = \deg E'/K$.

**Corollary.** Let $E/K$ be a finite Galois extension and $E'/K$ a finite separable extension. Then $E = E'$ if and only if, for some sufficiently large $m$, the $\mathcal{O}_m$-semi-linear representations of $\Gamma/\Gamma_m$ on the additive groups $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ are isomorphic.

In the following of §1, we sketch the outline of our proof of Theorem 2.
First we generalize [5], Proposition 7.

**Proposition 1.** Let $M$ be the $\mathcal{O}_m$-semi-linear representation of $\Gamma/\Gamma_m$ given by (a) $M = \mathcal{O}(E_{\otimes m})$ and (b) $M = \mathcal{O}(E_{\otimes m} \otimes_{K_m} E_{\otimes m}^*)$ where $E/K$ is a finite separable extension and $E^*/K$ is a finite Galois extension such that $\deg E/K$ and $\deg E^*/K$ are powers of $p$. Write $E \otimes_K E^* \cong \prod E_i$ as the product of the composite fields. Suppose $p^m \geq \deg E_i/K$. (deg $E_i/K$ does not depend on $i$ and is a power of $p$.) Then the orders of $M$ are:

(a) $\{0, p^{m-n}, 2p^{m-n}, \ldots, (p^n - 1)p^{m-n}\}$ with multiplicity 1, where $p^n = \deg E/K$. 
(b) $\{0, p^{m-h}, 2p^{m-h}, \ldots, (p^h - 1)p^{m-h}\}$ with multiplicity $\frac{(\deg E/K)(\deg E^*/K)}{\deg(E_i/K)}$, where $p^h = \deg E_i/K$.

Destrempes [1] gave the following lemma on tensor products of rings of integers.

**Lemma 1.** Let $E_1$ and $E_2$ be two finite separable extensions of a local field $L$ (with residue field not necessarily algebraically closed). Let $d = \min\{v_L(\delta(E_1/L)), v_L(\delta(E_2/L))\}$, where $\delta(E_i/L)$ denotes the discriminant ideal of the extension $E_i/L$. Then

$$\pi^{[d/2]}\mathcal{O}(E_1 \otimes_L E_2) \subseteq \mathcal{O}(E_1) \otimes_{\mathcal{O}(L)} \mathcal{O}(E_2)$$

where $\{d/2\}$ denotes the least integer greater than or equal to $d/2$.

Using the above lemma and the ramification theory, we have the following generalization of [5], Proposition 6 and [1], Proposition 6.

**Proposition 2.** Let $E/K$ and $E^*/K$ be two finite separable extensions. Then there is an integer $s$, independent of $m$, such that

$$\pi_m^s\mathcal{O}(E_{\otimes m} \otimes_{K_m} E_{\otimes m}^*) \subseteq \mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}(E_{\otimes m}^*).$$

Here $s$ depends only on one of the two extensions $E/K$ and $E^*/K$. 


By the above Propositions 1 and 2, we prove the following proposition by modifying the argument of the proof of [5], Theorem 2.

**Proposition 3.** Let $E/K$ and $E'/K$ be two finite separable extensions. We assume that, for some sufficiently large $m$, the $O_m$-semi-linear representations of $\Gamma/\Gamma_m$ on the additive groups $O(E_{\otimes m})$ and $O(E'_{\otimes m})$ are isomorphic. Then, for any finite Galois extension $E^*/K$, we have $\deg E_i/K = \deg E'_i/K$ where $E \otimes_K E^* \cong \prod E_i$ and $E' \otimes_K E^* \cong \prod E'_i$ are the products of the composite fields.

Take the Galois closure of $E/K$ and that of $E'/K$ for $E^*$ and apply Proposition 3. Thus we have proved Theorem 2.

**Remark 1.** From our proof "sufficiently large $m$" in Theorem 2 admits a bound depending only on $K_{\infty}$ and one of the two fields $E$ and $E'$.

**Remark 2.** The following example shows that the conclusion of Proposition 3 does not imply the isomorphism of $E$ and $E'$.

An example: Suppose that $p > 3$. Let $G$ (resp. $A_3$) be the $p$-group of order $p^4$ (resp. the element "A_3") of Satz 12.6 (13) in Huppert [3] p.346. Put $H_1$ the cyclic subgroup of $G$ of order $p$ generated by $A_2^2A_3$ and $H_2$ the cyclic subgroup of $G$ of order $p$ generated by $A_3$. Then for any normal subgroup $N$ of $G$, $\text{card}(N \cap H_1) = \text{card}(N \cap H_2)$ . However $H_1$ and $H_2$ are not conjugate each other in $G$. Let $K$ be the completion of the maximal unramified extension of $Q_p$. Take a Galois extension $L/K$ with $\text{Gal}(L/K) = G$. Let $E/K$ (resp. $E'/K$) be the subextension of $L/K$ fixed by $H_1$ (resp. $H_2$).

§ 2. Sen's Theory (Generalized Hodge-Tate decompositions)

Let $\chi : G \rightarrow Z_p^*$ be a character of $G$ with infinite image. In § 2 we assume that $K$ is of characteristic 0 and $K_{\infty} = k^{\ker \chi}$.

An element of $H^1(G, GL_d(C))$ (resp. $H^1(\Gamma, GL_d(K_{\infty}))$) may be regarded as an isomorphism class of $C$(resp. $K_{\infty}$)-semi-linear representa-
tions of $\mathcal{G}$ of dim $d$. Sen [4] proved the following:

**Theorem 3.** ([4]) The map $H^1(\Gamma, GL_d(K_{\infty})) \to H^1(\mathcal{G}, GL_d(C))$, which is induced by $\mathcal{G} \to \Gamma$ and the inclusion $GL_d(K_{\infty}) \hookrightarrow GL_d(C)$, is a bijection. The isomorphism class given by a $C$-semi-linear representation $V$ of $\mathcal{G}$ corresponds to the isomorphism class given by the $K_{\infty}$-semi-linear representation $V_\infty$ of $\Gamma$, where $V_\infty = \{x \in V^{\ker \chi} \mid$ the translates of $x$ by $\Gamma$ generate a $K$-space of finite dimension $\}$.

Furthermore, Sen defined the $K_{\infty}$-linear operator $\varphi$ on $V_\infty$ satisfying, for $v \in V_\infty$,

$$\varphi(v) = \lim_{\sigma \rightarrow 1} \frac{\sigma(v) - v}{\log \chi(\sigma)}$$

where $\sigma \in \Gamma$ and $\log$ is the $p$-adic log. We also denote by $\varphi$ the $C$-linear extension of $\varphi$. Sen [4] proved the following:

**Theorem 4.** (i) Let $V_1$ and $V_2$ be two $C$-semi-linear representations of $\mathcal{G}$, and $\varphi_1$ and $\varphi_2$ the corresponding operators. For $V_1$ and $V_2$ to be isomorphic it is necessary and sufficient that $\varphi_1$ and $\varphi_2$ should be similar.

(ii) For a $C$-semi-linear representations $V$ of $\mathcal{G}$, there is a basis of $V_\infty$ with respect to which the matrix of $\varphi$ has coefficients in $K$. Because we assume that the residue field of $K$ is algebraically closed, for every matrix $\Phi$ with coefficients $\in K$ of degree $d$, there is a $C$-semi-linear representation $V$ of $\mathcal{G}$ of dimension $d$ whose operator $\varphi$ is similar to $\Phi$.

When the matrix of $\varphi$ is similar to a diagonal matrix whose coefficients $\in Z$ and $\chi$ is the cyclotomic character, then the decomposition of $V$ into the eigenspaces of $\varphi$ agrees with the Hodge-Tate decomposition into maximal subspaces of constant weight. Therefore Sen [4] regarded the primary decomposition given by $\varphi$ as a generalized Hodge-Tate decomposition.

Sen [6] considered integral semi-linear representations and proved the following integral analogue of the above Theorem 3.

**Theorem 5.** The map $H^1(\Gamma, GL_d(\mathcal{O}_\infty)) \to H^1(\mathcal{G}, GL_d(\mathcal{O}_C))$ induced by $\mathcal{G} \to \Gamma$ and the inclusion $GL_d(\mathcal{O}_\infty) \hookrightarrow GL_d(\mathcal{O}_C)$ is a injection.
Let $M$ be an $\mathcal{O}_C$-semi-linear representation $M$ of $\mathcal{G}$ of rank $d$. Put $V = M \otimes_{\mathcal{O}_C} C$. $V$ is a $C$-semi-linear representation of $\mathcal{G}$ of dimension $d$. We define an $\mathcal{O}_\infty$-module $M_\infty$ by $M_\infty = V_\infty \cap M$. Let $\varphi$ be the $K_\infty$-linear operator on $V_\infty$ as above. Put $\varphi' = p^r \varphi$ where $r$ is the smallest integer such that $M_\infty$ is stable under $\varphi'$. Sen [6] defined invariants $(M_\infty, \varphi')$ of $M$. (Whenever $M_\infty$ is free, Sen defined a further more refined version.) The following theorem in [6] characterizes the image of the map of Theorem 5.

**Theorem 6.** Let $M$ be an $\mathcal{O}_C$-semi-linear representation of $\mathcal{G}$. For $M$ to be induced (up to isomorphism) from an $\mathcal{O}_\infty$-semi-linear representation of $\Gamma$ it is necessary and sufficient that $M_\infty$ is a free $\mathcal{O}_\infty$-module.

Sen [6] asked whether the integral structures as above are linked to the conditions for representations of geometric type and also asked whether $M_\infty$ is a free $\mathcal{O}_\infty$-module for such a representation $M$. We give two examples for the latter question in § 3.

**§ 3. Examples**

Let the notations be the same as in § 2.

(1) ([6], Theorem 6) Let $E/K$ be a finite Galois $p$-extension with $G = \text{Gal}(E/K)$. Let $R = \mathcal{O}[G]$ be a regular representation of $G$ over $\mathcal{O}$. Define an $\mathcal{O}_C$-semi-linear representation $M$ of $\mathcal{G}$ by $M = \mathcal{O}_C \otimes_{\mathcal{O}} R$. Put $E_\infty = E K_\infty$. $M_\infty$ is a product of copies of $\mathcal{O}(E_\infty)$. Then we have:

(i) $\mathcal{O}(E_\infty)$ is an indecomposable $\mathcal{O}_\infty$-module. Hence $M_\infty$ is a free $\mathcal{O}_\infty$-module if and only if $E_\infty = K_\infty$.

(ii) Suppose that the index $(\Gamma : \Gamma_0)$ is prime to $p$. From § 1, Theorem 1, the extension $E/K$ is determined (up to isomorphism) by the isomorphism class of the $\mathcal{O}_\infty$-semi-linear representation $\mathcal{O}_\infty \otimes_{\mathcal{O}_m} \mathcal{O}(E_{\otimes m})$ of $\Gamma$.

(2) Suppose that $K$ is absolutely unramified for simplicity. Let $\chi$ be the cyclotomic character, $E/\mathcal{Q}_p$ a finite (unramified Galois) subextension of $K/\mathcal{Q}_p$ with residue degree $f$. Let $\mathcal{G}$ be the Lubin-Tate formal group.
associated to $E$ and a prime element $\pi_E$ of $E$. The Tate module $T_p(G)$ of $G$ is a free $\mathcal{O}(E)$-module of rank 1. Define an $\mathcal{O}_C$-semi-linear representation $M$ of $G$ by $M = \mathcal{O}_C \otimes_{\mathbb{Z}_p} T_p(G)$. Since $E/\mathbb{Q}_p$ is unramified, $\mathcal{O}_C \otimes_{\mathbb{Z}_p} \mathcal{O}(E) = \prod \mathcal{O}_C$ by applying Lemma 1 for $E$ and the finite extensions of $K$ and by completion. For a $\mathbb{Q}_p$-embedding $\sigma$ of $E$ into $\overline{K}$, put $M_\sigma = \{ \sum x_i \otimes y_i \in M | \sum \sigma(a)x_i \otimes y_i = \sum x_i \otimes ay_i \text{ for all } a \in \mathcal{O}(E) \}$. Then we have $M = M_{id} \oplus \sum_{\sigma \neq id} M_\sigma$ as in Serre [7], III-43. By [7], III-45, $\mathbb{C} \otimes_{\mathcal{O}_C} M_\sigma (\sigma \neq id)$ is of Hodge-Tate type of weight 0 and $\mathbb{C} \otimes_{\mathcal{O}_C} M_{id}$ is such of weight 1. From Fontaine [2], Corollary 1 of Theorem 1, we have

$$M_{id} \simeq i_{K,G}^{-1} \otimes_{\mathcal{O}_C} \hat{i}_K \otimes_{\mathbb{Z}_p} T_p(G_m) \simeq \mathcal{O}_C \otimes_{\mathbb{Z}_p} T_p(G_m),$$

where $i_{K,G}^{-1} = \{ x \in \mathbb{C} | v(x) \geq -\frac{1}{p^{f-1}} \}$, $\hat{i}_K = \{ x \in \mathbb{C} | v(x) \geq -\frac{1}{p-1} \}$ and $v(a) = -\frac{1}{p^{f-1}} - \frac{1}{p-1}$. Therefore $(M_{id})_\infty$ is a free $\mathcal{O}_\infty$-module if and only if $E = \mathbb{Q}_p$. Hence $M_\infty$ is a free $\mathcal{O}_\infty$-module if and only if $E = \mathbb{Q}_p$.

References


New York, Benjamin

[8] S. Yamagata, A remark on integral representations associated with