数理解析研究所講究録
971 巻 1996 年 145-152

局所体の Galois 群の整表現について
(Integral representations of Galois groups of local fields)

東京電機大学理工学部 山形周二 (Shuji Yamagata)

§ 1 で体の拡大に付随する整 Galois 表現について S. Sen 、 F. Destrempes らの結果の拡張、§ 2 で整 Galois 表現の一般化 Hodge-Tate 分解についての S. Sen の結果の紹介、§ 3 で例 を述べる。

§ 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 $\bar{K}$ of K with the Galois group $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$. Let K_∞/K be an abelian extension whose Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ has a subgroup of finite index $\Gamma_0 \cong \mathbf{Z}_p$. Denote by K_n the subfield of K_∞ fixed by $\Gamma_n = \Gamma_0^{p^n}$. For a finite extension F/K, let π_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 $\mathbf{C}$ be the completion of $\bar{K}$ 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 $\mathcal{O}_{\mathbf{C}} = \mathcal{O}(\mathbf{C})$. 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 $\Gamma = \Gamma_0 \cong \mathbf{Z}_p$.

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

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

$$\mathrm{Ord}_M \; x = \max\{t \in \mathbf{Z} \mid x\pi_F^{-t} \in M\}.$$

By a reduced basis of M^H we mean an $\mathcal{O}$-basis $\{ x_i \}$ of M^H satisfying the condition $\mathrm{Ord}_M(\sum_i c_i x_i) = \min_i \{\mathrm{Ord}_M \; c_i x_i\}$ 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 Γ/Γ_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 Γ/Γ_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 Γ/Γ_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 Γ/Γ_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 Γ/Γ_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 arguement 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 $\mathcal{O}_m$-semi-linear representations of Γ/Γ_m on the additive groups $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ are isomorphic. Then, for any finite Galois extension E^*/K, we have $\deg E_i/K = \deg E'_j/K$ where $E \otimes_K E^* \cong \prod E_i$ and $E' \otimes_K E^* \cong \prod E'_j$ 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_∞ 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 isomorphy of E and E'.

An example: Suppose that $p > 3$. Let G (resp. A_i) be the p-group of order p^4 (resp. the element "A_i") of Satz 12.6 (13) in Huppert [3] p.346. Put H_1 the cyclic subgroup of G of order p generated by $A_2^2 A_3$ and H_2 the cyclic subgroup of G of order p generated by A_3. Then for any normal subgroup N of G, $\mathrm{card}(N \cap H_1) = \mathrm{card}(N \cap H_2)$. However H_1 and H_2 are not conjugate each other in G. Let K be the completion of the maximal unramified extension of $\mathbf{Q}_p$. Take a Galois extension L/K with $\mathrm{Gal}(L/K) = G$. 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 $\chi : \mathcal{G} \to \mathbf{Z}_p^*$ be a character of $\mathcal{G}$ with infinite image. In § 2 we assume that K is of characteristic 0 and $K_\infty = \bar{K}^{\ker \chi}$.

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

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

Furthermore, Sen defined the K_∞-linear operator φ on V_∞ satisfying, for $v \in V_\infty$,

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

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

THEOREM 4. (i) Let V_1 and V_2 be two $\mathbf{C}$-semi-linear representations of $\mathcal{G}$, and φ_1 and φ_2 the corresponding operators. For V_1 and V_2 to be isomorphic it is necessary and sufficient that φ_1 and φ_2 should be similar.

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

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

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

THEOREM 5. The map $H^1(\Gamma, GL_d(\mathcal{O}_\infty)) \to H^1(\mathcal{G}, GL_d(\mathcal{O}_\mathbf{C}))$ induced by $\mathcal{G} \to \Gamma$ and the inclusion $GL_d(\mathcal{O}_\infty) \hookrightarrow GL_d(\mathcal{O}_\mathbf{C})$ is a injection.

Let M be an $\mathcal{O}_{\mathbf{C}}$-semi-linear representation M of $\mathcal{G}$ of rank d. Put $V = M \otimes_{\mathcal{O}_{\mathbf{C}}} \mathbf{C}$. V is a $\mathbf{C}$-semi-linear representation of $\mathcal{G}$ of dimension d. We define an $\mathcal{O}_\infty$-module M_∞ by $M_\infty = V_\infty \cap M$. Let φ be the K_∞-linear operator on V_∞ as above. Put $\varphi' = p^r \varphi$ where r is the smallest integer such that M_∞ is stable under φ'. Sen [6] defined invariants (M_∞, φ') of M. (Whenever M_∞ 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 $\mathcal{O}_{\mathbf{C}}$-semi-linear representation of $\mathcal{G}$. For M to be induced (up to isomorphism) from an $\mathcal{O}_\infty$-semi-linear representation of Γ it is necessary and sufficient that M_∞ 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_∞ 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 $G = \mathrm{Gal}(E/K)$. Let $R = \mathcal{O}[G]$ be a regular representation of G over $\mathcal{O}$. Define an $\mathcal{O}_{\mathbf{C}}$-semi-linear representation M of $\mathcal{G}$ by $M = \mathcal{O}_{\mathbf{C}} \otimes_{\mathcal{O}} R$. Put $E_\infty = EK_\infty$. M_∞ 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_∞ 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 Γ.

(2) Suppose that K is absolutely unramified for simplicity. Let χ be the cyclotomic character, $E/\mathbf{Q}_p$ a finite (unramified Galois) subextension of $K/\mathbf{Q}_p$ with residue degree f. Let $\mathbf{G}$ be the Lubin-Tate formal group

associated to E and a prime element π_E of E. The Tate module $T_p(\mathbf{G})$ of $\mathbf{G}$ is a free $\mathcal{O}(E)$-module of rank 1. Define an $\mathcal{O}_{\mathbf{C}}$-semi-linear representation M of $\mathcal{G}$ by $M = \mathcal{O}_{\mathbf{C}} \otimes_{\mathbf{Z}_p} T_p(\mathbf{G})$. Since $E/\mathbf{Q}_p$ is unramified, $\mathcal{O}_{\mathbf{C}} \otimes_{\mathbf{Z}_p} \mathcal{O}(E) = \prod \mathcal{O}_{\mathbf{C}}$ by applying Lemma 1 for E and the finite extensions of K and by completion. For a $\mathbf{Q}_p$-embedding σ of E into $\bar{K}$, put $M_\sigma = \{\sum x_i \otimes y_i \in \mathrm{M} | \sum \sigma(a) x_i \otimes y_i = \sum x_i \otimes a y_i$ 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, $\mathbf{C} \otimes_{\mathcal{O}_{\mathbf{C}}} M_\sigma$ $(\sigma \neq id)$ is of Hodge-Tate type of weight 0 and $\mathbf{C} \otimes_{\mathcal{O}_{\mathbf{C}}} M_{id}$ is such of weight 1. From Fontaine [2], Corollary 1 of Theorem 1, we have

$$M_{id} \simeq \hat{I}_{K,\mathbf{G}}^{-1} \otimes_{\mathcal{O}_{\mathbf{C}}} \hat{I}_K \otimes_{\mathbf{Z}_p} T_p(\mathbf{G_m}) \simeq a\mathcal{O}_{\mathbf{C}} \otimes_{\mathbf{Z}_p} T_p(\mathbf{G_m}),$$

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

References

[1] F. Destrempes, Generalization of a result of Shankar Sen:Integral representations associated with local field extentions, Acta Arith., LXIII.(3) (1993), 267-286.

[2] J-M. Fontaine, Formes differentielles et modules de Tate des varietes abeliennes sur les corps locaux, Invent. Math., **65** (1982), 379-409.

[3] B. Huppert, Endlich Gruppen I, (1967) Berlin-Heidelberg-New York, Springer-Verlag.

[4] S. Sen, Continuous cohomology and p-adic Galois representations, Invent. Math., **62** (1980), 89-116.

[5] S. Sen, Integral representations associated with p-adic field extensions, Invent. Math., **94** (1988), 1-12.

[6] S. Sen, Galois cohomohogy and Galois representations, Invent. Math., **112** (1993), 639-656

[7] S-P, Serre, Abelian l-adic representations and elliptic curves, (1968) New york, Benjamin

[8] S. Yamagata, A remark on integral representations associated with p-adic field extensions, Proc. of the Japan Acad., **71** (1995),215-217.