A Remark on Integral Representations Associated with p-adic Field Extensions

By Shuji YAMAGATA

Department of Mathematical Sciences, Tokyo Denki University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 13, 1995)

Let K be a local field of characteristic 0 with algebraically closed residue field of characteristic $p > 0$. In this paper, an extension of K means an extension of K contained in some fixed algebraic closure $\bar{K}$ of K. Let K_∞/K be a $\boldsymbol{Z}_p$-extension with Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ $(\cong \boldsymbol{Z}_p)$. Let $\Gamma_n = \Gamma^{p^n}$ and K_n the subfield of K_∞ fixed by Γ_n. Denote by $\mathcal{O}(F)$ the ring of integers of an extension F/K. Especially put $\mathcal{O}_n = \mathcal{O}(K_n)$ and $\mathcal{O} = \mathcal{O}(K)$. For a product R of extensions of K, $\mathcal{O}(R)$ denotes the product of the rings of integers of the factors i.e. the unique maximal order of R. For two finite extensions F/K and F'/K, let F_i, $i = 1,2,\dots,f$ be all the composite fields of the images of K-embeddings of F into $\bar{K}$ (up to equivalence of proper embeddings of F above F' in the sense of [4])) with F'. Then we have $F \otimes_K F' \cong \Pi F_i$. Put $F_{\otimes m} = F \otimes_K K_m$.

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 K_m. In [3] S. Sen proved (probably in collaboration with J-M. Fontaine): Let E/K and E'/K be two finite Galois p-extensions.E/K and E'/K are isomorphic 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 [1], F. Destrempes generalized this theorem for two finite Galois extensions.

The purpose of this paper is to prove the following theorem:

Theorem (cf. Theorem 2 of [3] and Theorem 1 of [1]). Let E/K and E'/K be two finite extensions. Assume that, for some sufficiently large m (cf. Remark 1 of §2), 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 $\deg E/K = \deg E'/K$.

The author would like to express his hearty thanks to Professor Keiichi Komatsu for his advice and encouragements.

§1. Preliminaries. For a finite extension F/K, let π_F be a prime element of F and v_F the valuation of F normalized by $v_F(\pi_F) = 1$. Especially put $\pi_n = \pi_{K_n}$ and $v_n = v_{K_n}$.

The following proposition is a generalization of Proposition 6 of [3] and Proposition 6 of [1].

Proposition 1. Let E/K and E^*/K be two finite extensions. Then there is an integer s, independent of m, such that

$$\mathcal{O}(E_{\otimes m} \otimes_{K_m} E^*_{\otimes m})/(\mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}(E^*_{\otimes m}))$$

is killed by π_m^s. Here s depends only on one of the two extensions E/K and E^*/K.

Proof. Let F/K be a finite extension. We claim that, for sufficiently large m, $v_m(\delta(FK_m/K_m))$ has an upper bound which depends only on F/K, not on m. Here $\delta(FK_m/K_m)$ is the discriminant ideal of the extension FK_m/K_m. If F/K is a finite Galois p-extension, the assertion was proved in Lemma 1 of [1]. General case follows from it by considering the Galois closure and using transitivity of discriminant. Hence we have proved the proposition by Lemma 4 of [1].

The next elementary lemma is used in the following.

Lemma. Let E/K be a finite extension and F/K a finite Galois extension. Write $E \otimes_K F \cong \Pi E_i$ as the product of the composite fields. Then $\deg E_i/K$ does not depend on i. Furthermore, if $\deg E/K$ and $\deg F/K$ are powers of p, so is $\deg E_i/K$.

Proof. Write $E \cong K[x]/(f)$ with an irreducible monic polynomial $f \in K[x]$. We have $E \otimes_K F \cong F[x]/(f) \cong \Pi F[x]/(f_i)$ if we decompose f into the product Πf_i of irreducible monic polynomials in $F[x]$ (cf. for example, Lemma 6, Chap. 2, §5.2 of [2]). As F/K is a Galois extension, f_i's are conjugate under $\mathrm{Gal}(F/K)$-action on the coefficients. Thus $\deg E_i/K = \deg f_i$ does not depend on i.

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. We recall Sen's theory on semi-linear representations in [3]: 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 $\mathrm{Ord}_M(\sum_i c_i x_i) = \mathrm{Min}_i\{\mathrm{Ord}_M c_i x_i\}$ 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.

The following proposition is a generalization of Proposition 7 of [3].

Proposition 2. 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 extension and E^*/K is a finite Galois extension such that $\deg E/K$ and $\deg E^*/K$ are powers of p. Write $E \otimes_K E^* \cong \Pi E_i$ as the product of the composite fields. Suppose $p^m \geq \deg E_i/K$. (By Lemma $\deg E_i/K$ 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 $\dfrac{(\deg E/K)(\deg E^*/K)}{\deg E_i/K}$, where $p^h = \deg E_i/K$.

Proof. (a) Let $E_{\otimes m} \cong \Pi F_i$ where F_i is the composite field $\lambda_i(E)K_m$ of K_m with the image of a K-embedding λ_i of E into $\bar{K}$.

For $x \in E = (M \otimes_{\mathcal{O}_m} K_m)^{\Gamma/\Gamma_m}$, we have

$$\pi_m^{-t} x \in M \Leftrightarrow \pi_m^{-t}\lambda_i(x) \in \mathcal{O}(F_i) \text{ for all } i$$
$$\Leftrightarrow v_{F_i}(\lambda_i(x)) \geq t v_{F_i}(\pi_m) \text{ for all } i$$
$$\Leftrightarrow t \leq \frac{v_{F_i}(\lambda_i(x))}{v_{F_i}(\pi_m)} = v_E(x)\,\frac{\deg F_i/E}{\deg F_i/K_m} = v_E(x)\,\frac{p^m}{\deg E/K} \text{ for all } i.$$

Then for $x \in E$, $\mathrm{Ord}_M x = p^{m-n} v_E(x)$.

Thus we get the orders of M applying the argument in the proof of Proposition 7 of [3].

(b) Since $E_{\otimes m} \otimes_{K_m} E^*_{\otimes m} \cong \Pi(E_i)_{\otimes m}$ and $\deg E_i/K$ is a power of p independ of i, applying case (a) to E_i yields the orders in this case.

§2. Proof of Theorem.

We prove the following proposition by modifying the argument in Theorem 2 of [3].

Proposition 3. Let E/K and E'/K be two finite 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 $E \otimes_K E^* \cong \Pi E_i$ and $E' \otimes_K E^* \cong \Pi E'_j$ are the products of the composite fields.

Proof. Assume that $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ are isomorphic representations while, for some finite Galois extension E^*/K, we have $\deg E_i/K \neq \deg E'_j/K$, where $E \otimes_K E^* \cong \Pi E_i$ and $E' \otimes_K E^* \cong \Pi E'_j$. From the isomorphy of representations, we have $\deg E/K = \deg E'/K$. By Lemma 3 of [1] the maximal tamely ramified subextensions of E/K and E'/K coincide and put it $\tilde{L}$. Let L^*/K be the maximal tamely ramified subextension of E^*/K and put $L = \tilde{L}L^*$. Since E_i is the composite field $\lambda_i(E)E^*$ of E^* with the image of a K-embedding λ_i of E into $\bar{K}$ and $\tilde{L}/K$ is a Galois extension, we have $E_i \supset L$ and $E_i = \lambda_i(E)(E^*L)$. That is, E_i is the composite field of E^*L with the image of the K-embedding of E into $\bar{K}$. Thus E_i is a factor of $E \otimes_K E^*L$. Also E'_j is a factor of $E' \otimes_K E^*L$. Hence we may take E^*L for E^* and may assume that $L^* \supset \tilde{L}$ i.e. $L = L^*$. We remark that $\deg E_i/L$ (resp. $\deg E'_j/L$) is a power of p independ of i (resp. j).

Put $p^\lambda = \deg E_i/L$, $p^\mu = \deg E'_j/L$, $p^n = \deg E/\tilde{L} = \deg E'/\tilde{L}$, $p^t = \deg E^*/L$ and $L_m = LK_m (\cong L_{\otimes m})$. In the following of this proof we may suppose $\lambda < \mu$ without loss of generality. We define the following $\mathcal{O}(L_m)$-semi-linear representations $M \supset N$ of $\mathrm{Gal}(L_m/L) \cong \Gamma/\Gamma_m$:

$$M = \mathcal{O}(((E \otimes_K L) \otimes_L L_m) \otimes_{L_m} (E^* \otimes_L L_m))$$
$$(\cong \mathcal{O}(E_{\otimes m} \otimes_{K_m} E^*_{\otimes m}) \text{ as } \mathcal{O}\text{-algebras}),$$
$$N = (\mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}(L_m)) \otimes_{\mathcal{O}(L_m)} \mathcal{O}(E^* \otimes_L L_m)$$
$$(\cong \mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}(E^*_{\otimes m}) \text{ as } \mathcal{O}\text{-algebras}).$$

Similarly we define $M' \supset N'$ by using E' instead of E.

Let s_0 be the larger of the two numbers "s" of Proposition 1 for the pairs E/K, E^*/K and E'/K, E^*/K. Put $s = s_0 \deg L/K$. Then $\pi_{L_m}^s$ kills M/N and M'/N'.

Write $E \otimes_K L \cong \Pi \tilde{E}_\alpha$ as the product of the composite fields. Because $\Pi(\tilde{E}_\alpha \otimes_L E^*) \cong (E$

$\otimes_K L) \otimes_L E^* \cong E \otimes_K E^* \cong \Pi E_i$, the degree of any factor of $\tilde{E}_\alpha \otimes_L E^*$ over L is equal to p^λ, especially independent of α. Therefore the orders of M (without taking into account their multiplicities) are $0, p^{m-\lambda}, 2p^{m-\lambda}, \ldots, (p^\lambda - 1)p^{m-\lambda}$ by Proposition 2 after taking LK_∞/L for K_∞/K. Also those of M' are $0, p^{m-\mu}, 2p^{m-\mu}, \ldots, (p^\mu - 1)p^{m-\mu}$.

Choose m so large that $2sp^{n+t} \deg \tilde{L}/K < p^m$. Applying the argument in the proof of Theorem 2 of [3] to the $\mathcal{O}(L_m)$-semi-linear representations M, N, M', N', the assumption $\lambda < \mu$ gives a contradiction.

Proof of Theorem. Let $\hat{E}$ (resp. $\hat{E}'$) be the Galois closure of E/K (resp. E'/K). Write $E \otimes_K \hat{E} \cong \Pi F_i$ and $E' \otimes_K \hat{E} \cong \Pi F_j'$, where F_i is a copy of $\hat{E}$ and F_j' is the composite field of $\hat{E}$ with the image of a K-embedding of E' into $\bar{K}$. By applying Proposition 3 for $E, E', \hat{E}$, we have $\deg \hat{E}/K = \deg F_i/K = \deg F_j'/K$. Thus $\hat{E} = F_j' \supset E'$ and $\hat{E} \supset \hat{E}'$. We also have $\hat{E}' \supset \hat{E}$. Hence $\hat{E} = \hat{E}'$.

Remark 1. From our proof "sufficiently large m" in Proposition 3 admits a bound depending only on K_∞, E^* and $\deg E/K = \deg E'/K$ and also one depending only on K_∞, E, E' and $\deg E^*/K$. Hence "sufficiently large m" in Theorem admits a bound depending only on K_∞ and one of the two fields E and E'.

Corollary. Let E/K be a finite Galois extension and E'/K a finite 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.

Remark 2. Our arguments and results hold just as well in the case where K is a local field of characteristic $p > 0$ with algebraically closed residue field if we consider only separable extensions of K (cf. p. 268 of [1]).

Remark 3. If the residue field of K is perfect but not necessarily algebraically closed, we still have the following result as Theorem 1D of [1] by Corollary above: Let K_∞/K be a totally ramified $\mathbf{Z}_p$-extension, E/K a finite totally ramified Galois extension and E'/K a finite totally ramified extension. Then $EK_u = E'K_u$ for some finite unramified extension K_u/K if and only if the $\mathcal{O}_m$-semi-linear representations $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ of Γ/Γ_m are isomorphic for some sufficiently large m.

References

[1] F. Destrempes: Generalization of a result of Shankar Sen: Integral representations associated with local field extensions. Acta Arith., **63(3)**, 267–286 (1993).

[2] S. Iyanaga *et al.*: The Theory of Numbers. North-Holland Publishing Company. Amsterdam, New York, Oxford (1975).

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

[4] A. Weil: Basic Number Theory. Springer-Verlag, Berlin, Heidelberg, New York (1967).