ACTA ARITHMETICA
LXIII.3 (1993)

Generalization of a result of Shankar Sen: Integral representations associated with local field extensions

by

François Destrempes (Ottawa, Ont.)

1. Statement of the main results. Let K be a local field (i.e., a field which is complete with respect to a discrete valuation) with perfect residue field of characteristic $p > 0$. Let K_∞/K be a totally ramified $\mathbb{Z}_p$-extension and denote by

(1.1a) $$K_m$$

the fixed field of K_∞ under $p^m\mathbb{Z}_p$. So

(1.1b) $$\Gamma_m = \mathrm{Gal}(K_m/K)$$

is a cyclic group of order p^m. Let

(1.1c) $$\mathcal{O}_m \quad \text{(respectively } \mathcal{O}\text{)}$$

be the integer ring of K_m (respectively K).

Following Sen [5], given a finite Galois extension E/K, we consider the semi-linear K_m-representation of Γ_m

(1.2a) $$E_{\otimes m} = E \otimes_K K_m$$

where Γ_m and K_m act on the right factor; see Section 2 for a discussion of semi-linear representations. This yields a semi-linear $\mathcal{O}_m$-representation of Γ_m

(1.2b) $$\mathcal{O}(E_{\otimes m})$$

by taking the unique maximal $\mathcal{O}_m$-order in the commutative separable f.d. K_m-algebra $E_{\otimes m}$ (see [2, Proposition 26.10, p. 563]).

This work was completed (except for the final modifications) as the author was a Postdoctoral Fellow of the CRM (Centre de recherches mathématiques, Université de Montréal), and was supported in part by the Natural Sciences and Engineering Research Council of Canada and by le fonds FCAR du Québec.

The main purpose of this paper is to prove the following generalization of a theorem of Sen ([5, Theorem 2]).

Theorem 1. *Assume that K has algebraically closed residue field. Two finite Galois extensions E/K and E'/K are isomorphic if and only if for some m large enough* (*depending only on the ramification of one of the extensions*, *say E/K*, *if K has characteristic $p > 0$*, *and only on K and the degrees of the extensions if K has characteristic* 0) *the semi-linear $\mathcal{O}_m$-representations $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ of Γ_m are isomorphic.*

In [5], this is proved in the case of finite Galois p-extensions of p-adic fields (i.e., in the unequal characteristic case). In this paper, we follow the basic strategy used in [5], and, in particular, we make use of various crucial results developed there, except for the ones in [5, Section 1]. Instead, we use our Lemma 4 in Section 5, a result which does not depend on the characteristic of K.

As in [5, Theorem 2′], Theorem 1 can be interpreted as follows (see Proposition 1 and Remark 2 in Section 2).

Theorem 1A. *Assume that K has algebraically closed residue field. A finite Galois extension E/K is determined by the invariant*

$$\alpha_m(E/K) \in H^1(\Gamma_m, Gl(d, \mathcal{O}_m))$$

for m large enough (*as in Theorem* 1), *where $d = (E:K)$.*

In Proposition 3 we present another interpretation of the cohomology set $H^1(\Gamma_m, Gl(d, \mathcal{O}_m))$ in terms of certain double cosets of $Gl(d, K_m)$. So we have the following equivalent version of Theorems 1 and 1A (see Remark 2).

Theorem 1B. *Assume that K has algebraically closed residue field. A finite Galois extension E/K is determined by the invariant*

$$\beta_m(E/K) \in Gl(d, K)\backslash Gl(d, K_m)/Gl(d, \mathcal{O}_m)$$

for m large enough (*as in Theorem* 1), *where $d = (E:K)$.*

Also, we scrutinize [5] in order to give an explicit lower bound for m "large enough" in Theorems 1, 1A, and 1B.

Definitions 1. For the statement of the following results it will be convenient to make the following conventions. Given a finite *totally and wildly ramified* Galois extension of local fields E/L, denote by $i(E/L)$ the smallest integer $i \geq 0$ for which the ramification group $\mathrm{Gal}(E/L)_{i+1}$ is trivial. We have $E = L$ if and only if $i(E/L) = 0$.

If E/K is a finite totally ramified Galois extension, and K_∞/K is a *fixed* totally ramified $\mathbb{Z}_p$-extension, let L be the maximal tamely ramified subextension of E/K, and set $L_\infty = LK_\infty$. So E/L is totally and wildly ramified. Denote the compositum of E and K_m by E_m. We define

$$
\begin{aligned}
i_* &= i_*(E/K) = i(E/E\cap L_\infty)\,,\\
i^* &= i^*(E/K) = i(E/L)\,,\\
p^{n_*} &= (E\cap L_\infty : L)\,,\\
n^* &= \text{smallest } m \ge n_* \text{ such that } E_{m+1}/E_m \text{ ramifies.}
\end{aligned}
\tag{1.3}
$$

Note 1. We have: $i_* \le i^*$ (see [6, Proposition 2, p. 62]); $i_* = 0$ iff $E \subseteq L_\infty$; and $i^* = 0$ iff $E = L$. Moreover, one can easily check that $n_* \le n^* \le n$, where $p^n = (E : L)$. If K has algebraically closed residue field, any algebraic extension over K is totally ramified. Hence, in that case, $n^* = n_*$.

Note 2. Note that i_*, i^*, n_*, n^* admit upper bounds which depend only on the ramification of the extension E/K (and its degree). *In characteristic* 0, one has (cf. [6, Exercise 3(c), p. 72])

$$
i^* \le p^n l e_K/(p-1) \tag{1.4}
$$

where $p^n = (E : L)$, $l = (L : K)$, and e_K is the absolute ramification index of K. So, in that case, i_*, i^*, n_*, n^* are bounded by quantities depending only on K (its absolute ramification index) and the degree of the extension E/K.

THEOREM 1C. *Assume that K has algebraically closed residue field. Let E/K and E'/K be two finite Galois extensions of the same degree $d = p^n l$, with $(p, l) = 1$. Then any integer m satisfying the inequality*

$$
\begin{aligned}
&m > \left(\frac{\log p}{\log\left\{1-\left(1-\dfrac{1}{p}\right)\dfrac{1}{i^*}\right\}^{-1}} + 1\right)\log_p i^* + 4n + \log_p(2l(l+1)) && \textit{if } n > 0\,,\\
&m \ge 0 && \textit{if } n = 0\,,
\end{aligned}
$$

is "large enough", in the sense of Theorems 1, 1A, *and* 1B, *where $i^* = i^*(E/K) = i(E/L)$ is as in* (1.3).

Note 3. In Theorem 1C, E/K and E'/K are assumed to have the same degree, since this is the case whenever $\mathcal{O}(E_{\otimes m}) \approx \mathcal{O}(E'_{\otimes m})$ (see Remark 2 in Section 2). Moreover, the maximal tamely ramified subextension L/K of E/K is determined by l (see Lemmas 2 and 3 in Section 5). Thus, if $n = 0$ (equivalently, if $i^* = 0$, from Note 1) m can be taken to be 0, as is asserted in Theorem 1C.

Note 4. The bound on m given in Theorem 1C is $O(i^* \log i^* + \log d)$, where $d = (E : K)$ and $i^* = i(E/K)$ (as in (1.3)). This follows from Remark 3 in Section 3. If K has characteristic 0, this is $O(d \log d)$ (from (1.4)).

If the residue field of K is *not* algebraically closed, we still have the following result (see also [5, Remark 1]), which shows in particular that the hypothesis of Theorem 1C cannot be removed.

THEOREM 1D. *Let E/K and E'/K be two finite Galois totally ramified extensions of K. Then $EF = E'F$ for some finite unramified extension F/K if and only if the semi-linear $\mathcal{O}_m$-representations $\mathcal{O}(E_{\otimes m})$ and $\mathcal{O}(E'_{\otimes m})$ of Γ_m are isomorphic for some m large enough* (*as in Theorem* 1C).

In order to prove Theorem 1C, we need the following explicit version of [4, Lemma 1, p. 40]. Here, L is *not* assumed to have an algebraically closed residue field.

We observe that the proof given in [4] holds just as well in characteristic $p > 0$. However, a uniform bound (in terms of the ground field and the degree of the extension) can be given only in characteristic 0.

LEMMA 1 (cf. [4, Lemma 1]). *Let L_∞/L be a totally ramified $\mathbb{Z}_p$-extension of local fields, and let E/L be a totally ramified finite Galois p-extension. Set $E_m = EL_m$, where L_m is the layer of the $\mathbb{Z}_p$-extension of degree p^m. Then the ramification filtration of the extension E_m/L_m stabilizes for m large enough*; *i.e.*, *whenever m satisfies the condition*

$$m > n^* + \frac{\log(p^{n^*-n_*} i_*)}{\log\left\{1 - \left(1 - \frac{1}{p}\right)\frac{1}{p^{n^*-n_*} i_*}\right\}^{-1}} \qquad \text{for } i_* \geq 1 \ (\text{i.e., } E \not\subseteq L_\infty),$$

$$m \geq n_* = n \qquad \text{for } i_* = 0 \ (\text{i.e., } E \subseteq L_\infty),$$

where $i_* = i(E/E \cap L_\infty)$, n_*, and n^* are defined in (1.3).

Note 5. Note that, in the case where the residue field of K is *algebraically closed*, the factor $p^{n^*-n_*}$ is just 1 (see Note 1).

Note 6. From Remark 3 in Section 3, we see that the right-hand side in the inequality of Lemma 1 is $O((di_*)\log(di_*))$, where $d = (E : L)$ and $i_* = i_*(E/L)$ is as in (1.3). In the case where K has algebraically closed residue field, we have $n^* = n_*$ (see Note 1), so that, in Lemma 1, one can take

$$m > n^* + \frac{\log i_*}{\log\left\{1 - \left(1 - \frac{1}{p}\right)\frac{1}{i_*}\right\}^{-1}}\,.$$

Assuming moreover that L has characteristic 0, we see, using (1.4), that

$$m > n + \frac{\log(p^n e_L/(p-1))}{\log\left\{1 - \frac{(p-1)^2}{p^{n+1}e_L}\right\}^{-1}}$$

is large enough in Lemma 1, where e_L is the absolute ramification index of L. The right-hand side is $O(d\log d)$. At the present stage, we do not know how much the bounds given in Theorem 1C and Lemma 1 can be improved.

2. Semi-linear representations

Semi-linear representations over commutative rings. Let R be a commutative ring, Γ a finite group, and $\phi : \Gamma \to \mathrm{Aut}(R)$ a group homomorphism. If $\sigma \in \Gamma$ and $\lambda \in R$, we write ${}^{\sigma}\lambda$ for $\phi(\sigma)(\lambda)$.

DEFINITION 2. A *semi-linear R-representation* of Γ (with given homomorphism $\phi : \Gamma \to \mathrm{Aut}(R)$) is a free R-module M of finite rank on which Γ acts and which satisfies $\sigma(\lambda x + y) = {}^{\sigma}\lambda\sigma(x) + \sigma(y)$, for any $\lambda \in R$, $x, y \in M$, and $\sigma \in \Gamma$.

Note that in the case of a trivial group homomorphism $\phi : \Gamma \to \mathrm{Aut}(R)$ we recover the notion of linear representation.

Recall (cf. [2, (28.1) and (28.2), p. 589]) that the *twisted algebra* $R\#\Gamma$ is defined by

$$(x\#\sigma)(y\#\tau) = x\,{}^{\sigma}y\#\sigma\tau \tag{2.1}$$

with $x, y \in R$ and $\sigma, \tau \in \Gamma$. So, a semi-linear R-representation of Γ is the same thing as an $R\#\Gamma$-module which is a free R-module of finite rank.

If M is a semi-linear R-representation of Γ, with given R-basis $\{x_i\}_{i=1}^{d}$, we define, for each $\sigma \in \Gamma$, a matrix $A(\sigma) = (a_{ij})$ by the equations

$$\sigma(x_j) = \sum_{i=1}^{d} a_{ij} x_i \tag{2.2}$$

for $1 \le j \le d$. The semi-linearity condition implies that the function $A : \Gamma \to Gl(d, R)$, $\sigma \mapsto A(\sigma)$, is a 1-cocycle; i.e., $A(\sigma\tau) = A(\sigma)\,{}^{\sigma}A(\tau)$, for any $\sigma, \tau \in \Gamma$ (see [6, p. 123]). Moreover, if $\{x'_i\}_{i=1}^{d}$ is any other R-basis of M, an elementary computation shows that the corresponding 1-cocycle A' is cohomologous to A; namely, we have

$$A'(\sigma) = S^{-1}A(\sigma)\,{}^{\sigma}S$$

where $S \in Gl(d, R)$ is defined by $x'_j = \sum_{i=1}^{d} s_{ij} x_i$, for $1 \le j \le d$.

We obtain in this manner a well-defined map from the set of isomorphism classes of semi-linear R-representations of Γ of rank d, into the cohomology set of Γ with values in $Gl(d, R)$. This map is clearly surjective. Namely, a 1-cocycle $A : \Gamma \to Gl(d, R)$ defines a representation via the equations (2.2). Moreover, the map is injective. In fact, if two representations M, M' have cohomologous corresponding 1-cocycles A and A', say $A'(\sigma) = S^{-1}A(\sigma)\,{}^{\sigma}S$

($\sigma \in \Gamma$), then the R-module homomorphism $\theta : M' \to M$ defined by

$$\theta(x'_j) = \sum_{i=1}^{d} s_{ij} x_i,$$

for $1 \le j \le d$, is an isomorphism of semi-linear representations.

So we have proved the following description of semi-linear representations. (The only reference I have for this result, as well as for Proposition 3 below, is a set of notes from a talk given by Sen at Cornell University.)

PROPOSITION 1. *Equations* (2.2) *above yield a* 1-1 *correspondence between the isomorphism classes of semi-linear R-representations of Γ of rank d, and the cohomology set $H^1(\Gamma, Gl(d,R))$.*

Hilbert's 90

PROPOSITION 2 (cf. [5, Proposition 1(a)]). *Let F/K be a finite Galois extension of fields, with Galois group Γ. Any semi-linear K-representation V of Γ* (*with the obvious homomorphism $\Gamma \hookrightarrow \mathrm{Aut}(F)$*) *is isomorphic to the representation $V^\Gamma \otimes_K F$* (*with F and Γ acting on the right factor*).

Proof. See [5]. This follows from Proposition 1 and Hilbert's 90 ([6, Proposition 3, p. 151]). ■

Remark 1. One can actually give a proof of Hilbert's 90 as follows. As noted in (2.1), a semi-linear F-representation V of Γ is the same thing as a finitely generated $F\#\Gamma$-module. But we have an isomorphism of K-algebras

$$F\#\Gamma \xrightarrow{\approx} \mathrm{End}_K(F)$$

which maps $x\#\sigma$ to the endomorphism of F (as a f.d. vector space over K) $\phi(y) = x\sigma(y)$ (see [3, Proposition 1.2(3,ii), pp. 80–81]). Since $\mathrm{End}_K(F)$ is a simple K-algebra, we see that the $F\#\Gamma$-module V is determined by its dimension d over F. From Proposition 1, we conclude that $H^1(\Gamma, Gl(d,F))=1$.

Next, consider F/K and Γ as in Proposition 2, and suppose that $\mathcal{O}_F$ is an integral domain for which F is the field of fractions. Hilbert's 90 implies that any 1-cocycle $A : \Gamma \to Gl(d, \mathcal{O}_F)$ can be realized as a trivial 1-cocycle in $H^1(\Gamma, Gl(d, F))$; i.e., for some $T \in Gl(d, F)$

$$A(\sigma) = T^{-1}\,{}^{\sigma}T \tag{2.3}$$

for any $\sigma \in \Gamma$. One easily checks that two matrices $T, T' \in Gl(d, F)$ define the same 1-cocycle via (2.3) if and only if $T' \in Gl(d, K)T$. Also, if A and A' are cohomologous 1-cocycles in the set $H^1(\Gamma, Gl(d, \mathcal{O}_F))$, say $A'(\sigma) = S^{-1}A(\sigma)\,{}^{\sigma}S$ ($\sigma \in \Gamma$), with $S \in Gl(d, \mathcal{O}_F)$, then $A'(\sigma) = (TS)^{-1}\,{}^{\sigma}(TS)$ ($\sigma \in \Gamma$).

So equation (2.3) yields a well-defined map

$$H^1(\Gamma, Gl(d, \mathcal{O}_F)) \to Gl(d,K)\backslash Gl(d,F)/Gl(d,\mathcal{O}_F)\,.$$

It is straightforward to check that this map is 1-1 and onto the set of those double cosets of matrices $T \in Gl(d,F)$ for which $T^{-1}{}^{\sigma}T \in Gl(d,\mathcal{O}_F)$ for any $\sigma \in \Gamma$. That is, we have the following description of semi-linear $\mathcal{O}_F$-representations of Γ of rank d.

PROPOSITION 3. *Let F/K, $\mathcal{O}_F$ be as above. Equations* (2.2) *and* (2.3) *yield a* 1-1 *correspondence between the isomorphism classes of semi-linear $\mathcal{O}_F$-representations of Γ of rank d, and the double cosets in*

$$Gl(d,K)\backslash Gl(d,F)^*/Gl(d,\mathcal{O}_F)$$

where $Gl(d,F)^* = \{T \in Gl(d,F) : T^{-1}\,{}^{\sigma}T \in Gl(d,\mathcal{O}_F)$ *for any* $\sigma \in \Gamma\}$.

Remark 2. Let K_m/K, Γ_m, $\mathcal{O}_m$ be as at the beginning of Section 1. Given a finite Galois extension E/K, its invariant $\mathcal{O}(E_{\otimes m})$ has $\mathcal{O}_m$-rank equal to the degree $d = (E : K)$ of the extension. In fact, it is a full $\mathcal{O}_m$-lattice in $E \otimes_K K_m$.

Applying equations (2.2) (with $R = \mathcal{O}_m$, $\Gamma = \Gamma_m$), and equation (2.3) (with $F/K = K_m/K$, $\Gamma = \Gamma_m$, $\mathcal{O}_F = \mathcal{O}_m$), to the representation $\mathcal{O}(E_{\otimes m})$, we obtain invariants $\alpha_m(E/K)$ in $H^1(\Gamma, Gl(d,\mathcal{O}_m))$, and $\beta_m(E/K)$ in $Gl(d,K)\backslash Gl(d,K_m)/Gl(d,\mathcal{O}_m)$ attached to the extension E/K.

It is clear that Theorems 1A and 1B follow at once from Theorem 1, and Propositions 1 and 3.

Orders of semi-linear representations. We now consider a finite Galois p-extension of local fields

$$L_m/L$$

which is *totally ramified*. We set $\Gamma_m = \mathrm{Gal}(L_m/L)$, and we denote the integer ring of L_m (L) by $\mathcal{O}_{L_m}$ (respectively $\mathcal{O}_L$). We recall the following results from Sen's theory [5] (L_m/L and Γ_m play the role of F/K and H in [5, Section 2]). We stress the fact that [5, Section 2] holds just as well in characteristic $p > 0$. However, we present here a mildly simplified version of it (this turns out to be enough for this paper).

If M is a semi-linear $\mathcal{O}_{L_m}$-representation of Γ_m of rank d, let V denote the induced semi-linear L_m-representation of Γ_m, $L_m \otimes_{\mathcal{O}_{L_m}} M$. An ultrametric is defined on V as follows:

$$\mathrm{Ord}_M(x) = \max\{t \in \mathbb{Z} : \pi_{L_m}^{-t} x \in M\} \tag{2.4}$$

where π_{L_m} is a prime element of L_m.

DEFINITION 3. We define the *set of orders* of M as follows:

$$\mathrm{Ord}(M) = \{\mathrm{Ord}_M(x) \bmod p^m : x \in M^{\Gamma_m}\}\,.$$

So, $\mathrm{Ord}(M)$ is a subset of $\mathbb{Z}/p^m\mathbb{Z}$.

Note 7. This corresponds to Sen's notion of orders in [5, Section 2], except that we do not take into account their multiplicities.

We recall here the following proposition of Sen (omitting multiplicities).

PROPOSITION 4 ([5, Proposition 7]). *Notation as above. Let E/L and E'/L be totally ramified finite p-extensions of local fields, and consider the semi-linear $\mathcal{O}_{L_m}$-representation M defined by* (a) $M = \mathcal{O}(E_{\otimes L} L_m)$ *and* (b) $M = \mathcal{O}(E_{\otimes L} L_m \otimes_{L_m} E'_{\otimes L} L_m)$ (*where $\mathcal{O}(A)$ denotes the maximal order of the commutative f.d. algebra A*). *Suppose that $(EE' : L) < p^m$. Assume that L has algebraically closed residue field. Then the set of orders of M is given by*:

(a) $\{0, p^{m-n}, 2p^{m-n}, \ldots, (p^n - 1)p^{m-n}\}$, *where* $p^n = (E : L)$.
(b) $\{0, p^{m-k}, 2p^{m-k}, \ldots, (p^k - 1)p^{m-k}\}$, *where* $p^k = (EE' : L)$.

Proof. The proof given in [5] holds also in characteristic $p > 0$. ■

The following result of Sen says that the invariants "orders" behave well under "approximation" of semi-linear $\mathcal{O}_{L_m}$-representations of Γ_m.

PROPOSITION 5 (cf. [5, Proposition 4]). *Let $M \subseteq M'$ be two semi-linear $\mathcal{O}_{L_m}$-representations of Γ_m, of the same rank d. Suppose that $\pi_{L_m}^s M' \subseteq M$, where π_{L_m} is a prime element of $\mathcal{O}_{L_m}$. Let $\{\delta\}$* (*respectively $\{\delta'\}$*) *be the set of orders of M* (*respectively M'*). *Then, for each δ, there exists a δ' such that*

$$|\delta - \delta' + cp^m| \leq s$$

where c is some integer; *and, for each δ', there exists a δ such that*

$$|\delta' - \delta + cp^m| \leq s$$

for some integer c.

Proof. Note first, as in [5], that, for any $x \in M$, we have

$$|\mathrm{Ord}_M(x) - \mathrm{Ord}_{M'}(x)| \leq s\,.$$

Since $M^{\Gamma_m} \subseteq (M')^{\Gamma_m}$, the first statement of the proposition is clear. For the other statement, let π_L be a prime element of L. Note that if $x \in (M')^{\Gamma_m}$, then $\mathrm{Ord}_{M'}(x) = \mathrm{Ord}_{M'}(\pi_L^s x) \bmod p^m$. But $\pi_L^s x$ is an element of M^{Γ_m}. This proves the proposition. ■

3. Proof of Lemma 1. In this section, we consider a *totally ramified* $\mathbb{Z}_p$-extension L_∞/L of a local field L with residue field *not* necessarily algebraically closed. L_m will denote the (cyclic) layer of degree p^m of L_∞/L.

Let E/L be a finite Galois p-extension which is totally ramified. Denote by E_m the composite field EL_m, and set $G_m = \mathrm{Gal}(E_m/L_m)$. We will scrutinize the proof of [4, Lemma 1], in order to find a number m^* such that the filtration G_m stabilizes for $m \geq m^*$ (this will be valid also in characteristic $p > 0$). We need to recall most of the proof of Sen's Lemma. Note that the roles of E and L in [4] are interchanged here!

For the moment, let $m \geq n_*$, where $L_{n_*} = E \cap L_\infty$ (i.e., n_* is as in (1.3)); then there are canonical isomorphisms $G_{n_*} = \mathrm{Gal}(E/E \cap L_\infty) \approx G_m \approx G_{m+1}$. If $E \subseteq L_\infty$ (equivalently, if $i_* = 0$) then $G_m = 1$ for all $m \geq n_*$, and so, we may assume that $E \not\subseteq L_\infty$. Consider elements $\tau_m \neq 1$ and τ_{m+1} which correspond to each other under this canonical identification. Also, pick a generator σ_m of the cyclic group (of order p) $\mathrm{Gal}(E_{m+1}/E_m)$. As in [4], define

$$\begin{aligned} i(\sigma_m) &= \text{the greatest } i \text{ such that } \sigma_m \in (\langle\sigma_m\rangle)_i\,, \\ i(\tau_m) &= \text{the greatest } i \text{ such that } \tau_m \in (G_m)_i\,. \end{aligned} \tag{3.1}$$

Note that the $i(\sigma)$ in [6] is equal to 1 plus the $i(\sigma)$ in [4].

Now, let $m \geq n^* \geq n_*$ (as in (1.3)); i.e., E_{m+1}/E_m is (*totally*) *ramified.* In particular,

$$i(\sigma_m) \geq 1. \tag{3.2}$$

In [4], it is proved that

$$\begin{aligned} i(\sigma_{m+1}) &\geq p\, i(\sigma_m) \qquad \text{for } m \geq n^*\,, \\ i(\tau_{m+1}) &\leq p\, i(\tau_m) \qquad \text{for } m \geq n_*\,. \end{aligned} \tag{3.3}$$

For the first inequality one can use [4, Corollary (a)], since E_{m+2}/E_m is wildly ramified for $m \geq n^*$; the second inequality follows from [6, Proposition 3, p. 63]. Also, we have in [4] the inequalities

$$\begin{aligned} (p-(p-1)\alpha_m)i(\tau_m) &\geq i(\tau_{m+1}) \qquad \text{if } i(\sigma_m) \leq i(\tau_m)\,, \\ i(\tau_m) &= i(\tau_{m+1}) \qquad \text{if } i(\sigma_m) > i(\tau_m)\,, \end{aligned} \tag{3.4}$$

for any $m \geq n^*$, where $\alpha_m = i(\sigma_m)/i(\tau_m)$ (this follows from [6, Proposition 3, p. 63]). For the first inequality, note that (3.2) implies that $i(\tau_m) \geq i(\sigma_m) \geq 1$, so that α_m makes sense.

Let $m \geq n^*$ be an integer for which $i(\sigma_m) \leq i(\tau_m)$. From (3.3), we see that $i(\sigma_{m'}) \leq i(\tau_{m'})$ for any $n^* \leq m' \leq m$. So $i(\tau_{m'}) \geq 1$ (from (3.2)). Hence, dividing by $i(\tau_{m'})$, we obtain, from (3.3) again, as well as (3.4), the inequalities

$$\begin{aligned} i(\sigma_{m'})/i(\tau_{m'}) &\geq \alpha_{n^*}\,, \\ (p-(p-1)\alpha_{n^*})i(\tau_{m'}) &\geq i(\tau_{m'+1})\,, \end{aligned} \tag{3.5a}$$

for any $n^* \leq m' < m$ (where $0 < \alpha_{n^*} = i(\sigma_{n^*})/i(\tau_{n^*}) \leq 1$). Hence, we have

$$\begin{aligned} (p-(p-1)\alpha_{n^*})^{m-n^*} i(\tau_{n^*}) &\geq i(\tau_m)\,, \\ i(\sigma_m) &\geq p^{m-n^*} i(\sigma_{n^*})\,. \end{aligned} \tag{3.5b}$$

Thus, if $i(\sigma_m) \le i(\tau_m)$, then m must satisfy the condition

$$\alpha_{n^*} \le \left(1 - \left(1 - \frac{1}{p}\right)\alpha_{n^*}\right)^{m-n^*}. \tag{3.5c}$$

Now, let $i_* = i(E/E \cap L_\infty)$ be as in (1.3). Since we are in the case where $E \not\subseteq L_\infty$, we have $i_* \ge 1$ (see (1.3)). So, since $L_{n_*} = E \cap L_\infty$,

$$i_* = \max\{i(\tau_{n_*}) : \tau_{n_*} \ne 1 \in \mathrm{Gal}(E/E \cap L_\infty)\}. \tag{3.6a}$$

From (3.2) and the second inequality in (3.3), we conclude that, for any $\tau_{n^*} \ne 1$,

$$\alpha_{n^*} \ge \alpha \tag{3.6b}$$

where α is defined (for convenience within the proof) by

$$\alpha = (p^{n^*-n_*} i_*)^{-1}. \tag{3.6c}$$

Combining (3.5c) and (3.6b), we see that the inequality

$$\alpha > \left(1 - \left(1 - \frac{1}{p}\right)\alpha\right)^{m-n^*} \tag{3.7a}$$

implies that $i(\tau_m) < i(\sigma_m)$ (for any $\tau_m \ne 1$), which in turn implies that $i(\tau_m) = i(\tau_{m+1})$ (from (3.4)); i.e., the ramification filtration has stabilized.

Thus, making use of (3.7a), we conclude that any m satisfying

$$m > n^* + \frac{\log(p^{n^*-n_*} i_*)}{\log\left\{1 - \left(1 - \frac{1}{p}\right)\frac{1}{p^{n^*-n_*} i_*}\right\}^{-1}} \tag{3.7b}$$

is large enough in [4, Lemma 1] (for $i_* \ge 1$). ∎

Remark 3. Since

$$f(t) = \frac{-\log(1-\lambda t)}{\lambda t} = 1 + \sum_{\nu \ge 2} \frac{1}{\nu}(\lambda t)^{\nu-1}, \quad \text{where } \lambda = 1 - \frac{1}{p},$$

we see that $f(t)$ is $O(1)$ for $t \in (0,1]$. More precisely,

$$1 \le \frac{\log\{1-\lambda t\}^{-1}}{\lambda t} \le \frac{\log\{1-\lambda\}^{-1}}{\lambda}$$

for $t \in (0,1]$. This can be used to give simpler bounds in Theorem 1C and Lemma 1.

4. Some explicit bound. In this section, we consider a local field L with *algebraically closed* residue field, and a $\mathbb{Z}_p$-extension L_∞/L. The fixed field of L_∞ under $p^m\mathbb{Z}_p$ is denoted by L_m.

Let E/L be a finite Galois p-extension of degree p^n. Denote the compositum of E and L_m by E_m.

Set

$$s_m = \mathrm{val}_{L_m}\mathfrak{d}(E_m/L_m) \tag{4.1}$$

where $\mathfrak{d}(E_m/L_m)$ denotes the discriminant ideal of E_m/L_m. Since the extension E_m/L_m is totally ramified, we have

$$s_m = \mathrm{val}_{E_m}\mathfrak{D}(E_m/L_m) = \sum_{\tau_m \neq 1 \in G_m} (i(\tau_m) + 1)$$

where $\mathfrak{D}(E_m/L_m)$ denotes the different ideal of the extension E_m/L_m, using [6, Proposition 4, p. 64].

We obtain from Lemma 1 (see Note 6) that $s_m = s_{m_*}$ for any $m \geq m_*$, where

$$\begin{aligned} &m_* = n + 1 + \frac{\log\, i_*}{\log\left\{1 - \left(1 - \frac{1}{p}\right)\frac{1}{i_*}\right\}^{-1}} && \text{if } i_* \geq 1\,, \\ &m_* = n && \text{if } i_* = 0\,. \end{aligned} \tag{4.2}$$

Recall that $i_* = 0$ iff $E \subseteq L_\infty$; in that case, $s_m = 0$ for any $m \geq m_* = n$, as stated in equation (4.3) below.

So consider the case where $i_* \geq 1$. We have $i(\tau_{m_*}) \leq p^{m_* - n_*} i(\tau_{n_*})$ (using the second inequality in (3.3)), and $i(\tau_{n_*}) \leq i_*$ (from (3.6a)). Hence,

$$\begin{aligned} s_m = s_{m_*} &\leq p^{m_* - n_*} \sum_{\tau_{n_*} \neq 1 \in G_{n_*}} i(\tau_{n_*}) + (p^{n-n_*} - 1) \\ &\leq p^{m_* - n_*}(p^{n-n_*} - 1) i_* + (p^{n-n_*} - 1) \\ &\leq p^{m_*}(p^n - 1) i_* + p^{m_*} i_* = p^{m_* + n} i_*\,. \end{aligned}$$

We have shown that, for any $m \geq m_*$ as in (4.2), we have

$$s_m \leq s_* \tag{4.3}$$

where $s_* = p^{m_*+n} i_*$.

5. Proof of Theorem 1. Throughout this section, K is assumed to have *algebraically closed* residue field. In particular, any finite extension E/K is totally ramified. We start with the following observation.

LEMMA 2. *Let L/K be a tamely ramified extension of local fields. Let $l = (L : K)$ (so $(p, l) = 1$), and π be any prime element of K. Then $L = K(\pi^{1/l})$.*

Proof. Let π_L be a prime of L. We have $\pi = u\pi_L^l$ for some unit $u \in \mathcal{O}_L^*$. Since L has algebraically closed residue field and $(p, l) = 1$, Hensel's Lemma implies that there is an element $v \in \mathcal{O}_L^*$ such that $v^l = u$. Hence, $(v\pi_L)^l = \pi$. Thus, $\pi^{1/l} = v\pi_L$ is a prime of L. But the extension L/K is totally ramified, and is therefore generated by any prime of L. Hence, L is the Kummer extension $K(\pi^{1/l})$. ■

Remark 4. The proof of Lemma 2 shows that, if K is a local field with algebraically closed residue field of *characteristic* 0, then *any* finite extension E/K is determined by its degree d; namely, E is the Kummer extension $K(\pi^{1/d})$, where π is an arbitrary fixed prime element of K.

LEMMA 3. *Let E/K and E'/K be extensions of local fields, with maximal tamely ramified subextensions L and L', respectively. If $\mathcal{O}(E_{\otimes m}) \approx \mathcal{O}(E'_{\otimes m})$, then $L \approx L'$.*

Proof. The hypothesis implies that $(E:K) = (E':K)$. If $l = (L:K)$ and $l' = (L':K)$, we have $(E:K) = lp^n$ and $(E':K) = l'p^{n'}$, where $(p,l) = (p,l') = 1$. Hence, $l = l'$, and by Lemma 2, $L \approx L'$. ■

We now consider two finite Galois extensions E/K and E'/K, contained in some fixed algebraic closure of K. We assume that the two extensions have the *same degree*.

From Lemma 3, we have a tamely ramified extension $L \subseteq E, E'$, with E/L and E'/L p-extensions of the same degree.

We set $l = (L:K)$, $p^n = (E:L) = (E':L)$, $L_m = LK_m$, and $\mathcal{O}_{L_m} = \mathcal{O}(L_m)$.

We define the following $\mathcal{O}_{L_m}$-representations of $\Gamma_m \approx \mathrm{Gal}(L_m/L)$:

$$
\begin{aligned}
&M_m = \mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m} \otimes_{\mathcal{O}_{L_m}} \mathcal{O}(E'_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m}\,,\\
(5.1)\qquad &M^*_m = \mathcal{O}(E_{\otimes m} \otimes_{K_m} L_m) \otimes_{\mathcal{O}_{L_m}} \mathcal{O}(E'_{\otimes m} \otimes_{K_m} L_m)\,,\\
&M'_m = \mathcal{O}(E_{\otimes m} \otimes_{K_m} L_m \otimes_{L_m} E'_{\otimes m} \otimes_{K_m} L_m)\,.
\end{aligned}
$$

Of course, we have the inclusions $M_m \subseteq M^*_m \subseteq M'_m$, and we wish to find an integer t for which $\pi^t_{L_m} M'_m \subseteq M_m$, where π_{L_m} is a prime of L_m.

The following lemma is a consequence of the product discriminant formula. I wish to thank here S. U. Chase for suggesting to me the particularly simple proof of equation (5.2) below presented here. (See also [1, Theorem 2.4, p. 220].)

Notation. If x is any real number, $\{x\}$ denotes the *least* integer greater than or equal to x.

LEMMA 4. *Let E_1, E_2 be two finite separable extensions of a local field K (with residue field not necessarily algebraically closed). Denote by $\mathcal{O}(E_1)$, $\mathcal{O}(E_2)$, and $\mathcal{O}$, their respective ring of integers. Let $d = \min\{\mathrm{val}_K\, \mathfrak{d}(E_i/K)\}$, where $\mathfrak{d}(E_i/K)$ denotes the discriminant ideal of the extension E_i/K. Then*

$$\pi^{\{d/2\}}\, \mathcal{O}(E_1 \otimes_K E_2) \subseteq \mathcal{O}(E_1) \otimes_{\mathcal{O}} \mathcal{O}(E_2)$$

where π is a prime element of K.

P r o o f. Let E/K be a finite Galois extension containing E_1E_2. Consider the isomorphism of E-algebras

$$\psi:\ E\otimes_K E_2\approx\prod_\sigma E$$

where σ ranges over the set of K-imbeddings of E_2 into E, and which sends $x\otimes y$ (with $x\in E$ and $y\in E_2$) to the element $\{x\sigma(y)\}$.

This yields an imbedding of $\mathcal{O}(E)$-algebras

$$\mathcal{O}(E)\otimes_{\mathcal{O}}\mathcal{O}(E_2)\xrightarrow{\psi}\prod_\sigma\mathcal{O}(E)$$

with the right side isomorphic to $\mathcal{O}(E\otimes_K E_2)$.

Now, let $\{x_i\}$ be an $\mathcal{O}$-basis of $\mathcal{O}(E_2)$. So $\{1\otimes x_i\}$ is an $\mathcal{O}(E)$-basis of $\mathcal{O}(E)\otimes_{\mathcal{O}}\mathcal{O}(E_2)$. Then the matrix of the $\mathcal{O}(E)$-homomorphism ψ with respect to that basis and the canonical basis of $\prod_\sigma\mathcal{O}(E)$ is given by $(\sigma(x_i))$. Hence, if $\det(\sigma(x_i))=\widetilde{\pi}^t$ (with $\widetilde{\pi}$ a prime of E), we have

$$\widetilde{\pi}^t\,\mathcal{O}(E\otimes_K E_2)\subseteq\mathcal{O}(E)\otimes_{\mathcal{O}}\mathcal{O}(E_2)\,.$$

From the product discriminant formula, we also have $\widetilde{\pi}^{2t}=\widetilde{\pi}^{ed_2}$, where $d_2=\mathrm{val}_K\mathfrak{d}(E_2/K)$, and e is the ramification index of E/K. Thus,

$$\pi^{\{d_2/2\}}\,\mathcal{O}(E\otimes_K E_2)\subseteq\mathcal{O}(E)\otimes_{\mathcal{O}}\mathcal{O}(E_2)\,. \tag{5.2}$$

But under the natural imbedding of K-algebras $E_1\otimes_K E_2\to E\otimes_K E_2$, we have $\mathcal{O}(E_1\otimes_K E_2)\subseteq\mathcal{O}(E\otimes_K E_2)$, and $\mathcal{O}(E_1)\otimes_{\mathcal{O}}\mathcal{O}(E_2)=\mathcal{O}(E)\otimes_{\mathcal{O}}\mathcal{O}(E_2)$ $\cap\, E_1\otimes_K E_2$. Hence,

$$\pi^{\{d_2/2\}}\,\mathcal{O}(E_1\otimes_K E_2)\subseteq\mathcal{O}(E_1)\otimes_{\mathcal{O}}\mathcal{O}(E_2)\,.$$

Reversing the roles of E_1 and E_2, we obtain a similar inclusion with d_1 replacing d_2, and this proves the lemma. ∎

Lemma 5. *Notation as in* (5.1).

(a) $$\pi_{L_m}^{l\{(l-1)/2\}}\mathcal{O}(E_{\otimes m}\otimes_{K_m}L_m)\subseteq\mathcal{O}(E_{\otimes m})\otimes_{\mathcal{O}_m}\mathcal{O}_{L_m}\,;$$

(b) $$\pi_{L_m}^{2l\{(l-1)/2\}}M_m^*\subseteq M_m\,.$$

P r o o f. The second inclusion follows easily from the first one. For the first inclusion, consider the isomorphism of L_m-algebras

$$E_{\otimes m}\otimes_{K_m}L_m\approx\prod_{\{\widetilde{\xi}\}}E_m\otimes_{K_m}L_m$$

which sends $x\otimes y\otimes z$ to $\{(\widetilde{\xi}(x)y)\otimes z\}$, with $x\in E$, $y\in K_m$, $z\in L_m$, and where $\{\widetilde{\xi}\}$ is a set of representatives of $\mathrm{Gal}(E\cap K_m/K)$ in $\mathrm{Gal}(E/K)$.

Under this isomorphism, we have the identifications

$$\mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m} \approx \prod_{\{\widetilde{\xi}\}} \mathcal{O}(E_m) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m}\,,$$

$$\mathcal{O}(E_{\otimes m} \otimes_{K_m} L_m) \approx \prod_{\{\widetilde{\xi}\}} \mathcal{O}(E_m \otimes_{K_m} L_m)\,.$$

But the extension L_m/K_m is totally and tamely ramified of degree $l = (E:K)$. Hence, $\mathfrak{d}(E_m/K_m) = (\pi_m^{l-1})$ (with π_m a prime of K_m). From Lemma 4, we see that $\pi_m^{\{(l-1)/2\}}\mathcal{O}(E_m \otimes_{K_m} L_m)$ is contained in $\mathcal{O}(E_m) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m}$.

The inclusion now follows from the equality $(\pi_m) = (\pi_{L_m}^l)$. ■

The following proposition is the analogue of [5, Propositions 6 and 7].

Proposition 6. *Let E/K, E'/K, L, and l be as above.*

(a) *Let m_* and $s_* = p^{m_*+n} i_*$ be as in* (4.2) *and* (4.3) (*with i_* corresponding to the extension E/K*; *i.e., $i_* = i(E/E \cap L_\infty)$ as in* (1.3)). *Then*

$$\pi_{L_m}^{\{s_*/2\}+2l\{(l-1)/2\}} M'_m \subseteq M_m$$

where π_{L_m} is a prime of L_m, for any $m \geq m_*$.

(b) *The orders of M'_m are*

$$\{0, p^{m-k}, 2p^{m-k}, \ldots, (p^k-1)p^{m-k}\}$$

where $p^k = (EE' : L)$.

Proof. (a) From Lemma 5, it remains to show that $\pi_{L_m}^{\{s_*/2\}} M'_m \subseteq M_m^*$. Now, consider the isomorphism of L_m-algebras

$$E_{\otimes m} \otimes_{K_m} L_m \approx \prod_{\widetilde{\xi}} E_m \tag{5.3}$$

where $\{\widetilde{\xi}\}$ is a set of representatives of $\mathrm{Gal}(E \cap L_\infty/K)$ in $\mathrm{Gal}(E/K)$, which maps $x \otimes y \otimes z$ to $\{\widetilde{\xi}(x)yz\}$. Under this isomorphism, we have the identification

$$\mathcal{O}(E_{\otimes m} \otimes_{K_m} L_m) \approx \prod_{\{\widetilde{\xi}\}} \mathcal{O}(E_m)\,. \tag{5.4}$$

Using (5.3) and (5.4) for E and E', we obtain an isomorphism of L_m-algebras

$$E_{\otimes m} \otimes_{K_m} L_m \otimes_{L_m} E'_{\otimes m} \otimes_{K_m} L_m \approx \prod_{\{\widetilde{\xi}\}} \prod_{\{\widetilde{\xi}'\}} E_m \otimes_{L_m} E'_m$$

under which we get the identifications

$$M_m^* \approx \prod_{\{\widetilde{\xi}\}} \prod_{\{\widetilde{\xi}'\}} \mathcal{O}(E_m) \otimes_{\mathcal{O}_{L_m}} \mathcal{O}(E'_m)$$

and

$$M'_m \approx \prod_{\{\widetilde{\xi}\}} \prod_{\{\widetilde{\xi}'\}} \mathcal{O}(E_m \otimes_{L_m} E'_m) \,.$$

Now use Lemma 4 (with $E_1 = E_m$, $E_2 = E'_m$, and $K = L_m$), as well as (4.3).

(b) Consider the isomorphism of L_m-algebras

$$E_{\otimes m} \otimes_{K_m} L_m \approx \prod_{\{\widetilde{\xi}\}} E \otimes_L L_m$$

where now $\{\widetilde{\xi}\}$ is a set of representatives of $\mathrm{Gal}(L/K)$ in $\mathrm{Gal}(E/K)$, which maps $x \otimes y \otimes z$ to $\{\widetilde{\xi}(x) \otimes (yz)\}$. We then get an isomorphism of $\mathcal{O}_{L_m}$-algebras

$$M'_m \approx \prod_{\{\widetilde{\xi}\}} \prod_{\{\widetilde{\xi}'\}} \mathcal{O}(E \otimes_L L_m \otimes_{L_m} E' \otimes_L L_m)$$

which preserves the action of Γ_m. Now use Proposition 4 (i.e., [5, Proposition 7]). ■

R e m a r k 5. If K has characteristic 0, we see from Note 2 that m_* and s_* can be replaced by

$$m^* = n + 1 + \frac{\log(p^n l e_K/(p-1))}{\log\left\{1 - \dfrac{(p-1)^2}{p^{n+1} l e_K}\right\}^{-1}} \,,$$

$$s^* = p^{m^*+2n} l e_K/(p-1)$$

in Proposition 6(a) (with $l = (L : K)$, and e_K the absolute ramification index of K).

We can finally derive Theorem 1 following the method in [5].

End of the proof of Theorems 1, 1A, 1B, 1C. We consider extensions E/K and E'/K such that

$$\mathcal{O}(E_{\otimes m}) \approx \mathcal{O}(E'_{\otimes m}) \,. \tag{5.5}$$

So Lemma 3 applies.

We consider the semi-linear $\mathcal{O}_{L_m}$-representations of $\Gamma_m \approx \mathrm{Gal}(L_m/L)$: M_m, M'_m (N_m, N'_m), as in (5.1), corresponding to the pair of extensions E, E' (respectively E, E).

Now, (5.5) yields an isomorphism

$$\mathcal{O}(E_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m} \approx \mathcal{O}(E'_{\otimes m}) \otimes_{\mathcal{O}_m} \mathcal{O}_{L_m} \tag{5.6}$$

of semi-linear $\mathcal{O}_{L_m}$-representations of Γ_m. Hence, M_m and N_m are isomorphic.

Let $\{\delta\}$, $\{\delta'\}$, $\{\varepsilon\}$, $\{\varepsilon'\}$ be the orders of M_m, M'_m, N_m, N'_m, respectively. Assume that

$$p^m > 2(\{s_*/2\} + 2l\{(l-1)/2\})p^{2n} \tag{5.7}$$

with s_* as in (4.3).

If $i_* = 0$, then $m_* = n$ (see (4.2)); so (5.7) implies that $m \geq m_*$. If $i_* \geq 1$, then $s_* \geq p^{m_*}$; but (5.7) implies that $p^m > s_*$, so that again $m \geq m_*$. Thus, Proposition 5 applies to the conclusion of Proposition 6(a), and we deduce that, for any δ', there is a δ and an integer c_m such that

$$|\delta' - \delta + c_m p^m| \leq \{s_*/2\} + 2l\{(l-1)/2\}\,.$$

Then, for that δ which is equal to some ε (from (5.6)), there is an ε' and an integer d_m such that

$$|\varepsilon' - \varepsilon + d_m p^m| \leq \{s_*/2\} + 2l\{(l-1)/2\}\,.$$

We conclude that for each δ' there is an ε' and an integer a_m such that

$$|\delta' - \varepsilon + a_m p^m| \leq 2(\{s_*/2\} + 2l\{(l-1)/2\}). \tag{5.8}$$

Now, in view of Proposition 6(b), take $\delta' = p^{m-k}$, and note that ε' is of the form bp^{m-n}. Suppose, by way of contradiction, that $E \neq E'$; i.e., $k > n$. Then p^{m-k} is the highest power of p dividing $\delta' - \varepsilon + a_m p^m$.

Henceforth, making use of (5.8), we obtain

$$p^{m-k} \leq 2(\{s_*/2\} + 2l\{(l-1)/2\})\,.$$

So we have

$$p^m \leq 2(\{s_*/2\} + 2l\{(l-1)/2\})p^{2n}\,,$$

a contradiction with (5.7).

Hence $E = E'$. This completes the proof of Theorem 1 (and, hence, of Theorems 1A and 1B).

For Theorem 1C, note that $s_* \leq p^{m_*+n} i^*$ (cf. (4.3) and (1.3)); moreover, as observed after the statement of Theorem 1C, we may assume that $E \neq L$ (i.e., $i^* \geq 1$). One can then check that $\{s_*/2\} + 2l\{(l-1)/2\} < p^{m_*+n} i^* l(l+1)$. So, in order to have (5.7), it is enough to take

$$p^m \geq 2p^{m_*+3n} i^* l(l+1);$$

i.e.,

$$m \geq m_* + 3n + \log_p i^* + \log_p(2l(l+1))\,. \tag{5.9}$$

From (4.2) and (4.3), and since $i_* \le i^*$, we see that it is enough to take

$$m > \left(\frac{\log p}{\log \left\{ 1 - \left(1 - \frac{1}{p}\right) \frac{1}{i^*} \right\}^{-1}} + 1 \right) \log_p i^* + 4n + \log_p (2l(l+1))$$

as is asserted in Theorem 1 (in the case where $i^* \ge 1$). ■

6. Proof of Theorem 1D. In this section we consider a *totally ramified* $\mathbb{Z}_p$-extension of local fields K_∞/K, without the assumption that K has algebraically closed residue field. We use the notation $\mathcal{O}$, K_m, $\mathcal{O}_m$, etc., as in Section 1.

The completion $\widehat{K}$ of the maximal *unramified* extension K^{nr} over K is a local field with algebraically closed residue field (in fact, equal to the algebraic closure of the residue field of K). The integer ring of $\widehat{K}$ will be denoted by $\widehat{\mathcal{O}}$.

Given any (finite) *totally* ramified extension E/K, the extension $E^{nr} = EK^{nr}/K^{nr}$ is totally ramified (of the same degree). Moreover, since $E \cap K^{nr} = K$, there is a natural isomorphism

$$E^{nr} \approx E \otimes_K K^{nr}\,. \tag{6.1a}$$

Hence, its completion $\widehat{E}$ is naturally isomorphic to $E^{nr} \otimes_{K^{nr}} \widehat{K}$ (see [6, Theorem 1, p. 30]), and therefore we have

$$\widehat{E} \approx E \otimes_K \widehat{K}\,. \tag{6.1b}$$

Applying the previous remarks to $E = K_m \subseteq K_\infty$, we see that the compositum field $\widehat{K}_\infty = \widehat{K} K_\infty$ is a $\mathbb{Z}_p$-extension over $\widehat{K}$ (which is, in any case, necessarily totally ramified since $\widehat{K}$ has algebraically closed residue field). Its mth layer is given by

$$\widehat{K}_m \approx K_m \otimes_K \widehat{K}\,. \tag{6.2}$$

Now, for the remainder of this section, let E/K be a *finite Galois* extension (of local fields) which is *totally* ramified. Then, with the notation as above, we have a natural isomorphism of $\widehat{K}_m$-algebras

$$(E \otimes_K K_m) \otimes_{K_m} \widehat{K}_m \approx \widehat{E} \otimes_{\widehat{K}} \widehat{K}_m \tag{6.3}$$

(making use of (6.1a) and (6.2)). Namely, $(x \otimes y) \otimes z$ is mapped to $x \otimes (yz)$, for any $x \in E$, $y \in K_m$, and $z \in \widehat{K}_m$. Moreover, upon identifying $\Gamma_m = \mathrm{Gal}(K_m/K)$ and $\mathrm{Gal}(\widehat{K}_m/\widehat{K})$, (6.3) is actually an isomorphism of $\widehat{K}_m$-semilinear representations of Γ_m, where $\widehat{K}_m$ and Γ_m act as in (1.1).

The following observation allows us to compare $\mathcal{O}(E \otimes_K K_m)$ with $\mathcal{O}(\widehat{E} \otimes_{\widehat{K}} \widehat{K}_m)$.

LEMMA 6. *Notation as above. The isomorphism of* (6.3) *restricts to an isomorphism*

$$\mathcal{O}(E \otimes_K K_m) \otimes_{\mathcal{O}_m} \widehat{\mathcal{O}}_m \approx \mathcal{O}(\widehat{E} \otimes_{\widehat{K}} \widehat{K}_m)$$

of $\widehat{\mathcal{O}}_m$*-semi-linear representations of* Γ_m.

Proof. We have a decomposition of K_m-algebras

$$E \otimes_K K_m \approx \prod E_m \,.$$

To this decomposition corresponds the isomorphism of $\mathcal{O}_m$-algebras

$$\mathcal{O}(E \otimes_K K_m) \approx \prod \mathcal{O}(E_m) \tag{6.4}$$

(by taking maximal orders).

Now, for any finite *unramified* extension F_m/K_m, Lemma 4 (with $E_1 = E_m$, $E_2 = F_m$, $K = K_m$) implies that

$$\mathcal{O}(E_m) \otimes_{\mathcal{O}_m} \mathcal{O}(F_m) = \mathcal{O}(E_m \otimes_{K_m} F_m) \,.$$

We obtain

$$\mathcal{O}(E_m) \otimes_{\mathcal{O}_m} \mathcal{O}_m^{nr} = \mathcal{O}(E_m \otimes_{K_m} K_m^{nr})$$

and, hence, using (6.4), we have

$$\mathcal{O}(E \otimes_K K_m) \otimes_{\mathcal{O}_m} \widehat{\mathcal{O}}_m = \mathcal{O}((E \otimes_K K_m) \otimes_{K_m} K_m^{nr}) \otimes_{\mathcal{O}_m^{nr}} \widehat{\mathcal{O}}_m \tag{6.5}$$

after tensoring with $\widehat{\mathcal{O}}_m$ over $\mathcal{O}_m^{nr}$.

Next, $(E \otimes_K K_m) \otimes_{K_m} K_m^{nr}$ decomposes into a product $\prod_j E_j$ where the E_j's are finite extensions of K_m^{nr}. Since taking maximal orders and taking completions are two operations which commute, using [6, Proposition 4, p. 32], we see that

$$\mathcal{O}((E \otimes_K K_m) \otimes_{K_m} K_m^{nr}) \otimes_{\mathcal{O}_m^{nr}} \widehat{\mathcal{O}}_m = \mathcal{O}((E \otimes_K K_m) \otimes_{K_m} \widehat{K}_m) \,. \tag{6.6}$$

So, combining (6.5) and (6.6), we obtain

$$\mathcal{O}(E \otimes_K K_m) \otimes_{\mathcal{O}_m} \widehat{\mathcal{O}}_m = \mathcal{O}((E \otimes_K K_m) \otimes_{K_m} \widehat{K}_m) \,. \tag{6.7}$$

Lemma 6 now follows from (6.3) and (6.7). ∎

Now let E/K and E'/K be two *finite* Galois extensions which are *totally ramified*. Assume that the semi-linear $\mathcal{O}_m$-representations $\mathcal{O}(E \otimes_K K_m)$ and $\mathcal{O}(E' \otimes_K K_m)$ of Γ_m are isomorphic for *some* m large enough (in the sense of Theorem 1C; note that $i^*(E/K) = i^*(\widehat{E}/\widehat{K})$, see (1.3) and [6, Exercise, p. 65]).

Then $\mathcal{O}(E \otimes_K K_m) \otimes_{\mathcal{O}_m} \widehat{\mathcal{O}}_m$ and $\mathcal{O}(E' \otimes_K K_m) \otimes_{\mathcal{O}_m} \widehat{\mathcal{O}}_m$ are isomorphic semi-linear $\widehat{\mathcal{O}}_m$-representations of Γ_m. With $\widehat{E}$ and $\widehat{E}'$ as above, we see from Lemma 6 that $\mathcal{O}(\widehat{E} \otimes_{\widehat{K}} \widehat{K}_m)$ and $\mathcal{O}(\widehat{E}' \otimes_{\widehat{K}} \widehat{K}_m)$ are isomorphic. From Theorem 1C, it follows that $\widehat{E} = \widehat{E}'$. Hence (as is easily seen from [6, Exercises 1 and 2, p. 30]) $EF = E'F$ for some *finite unramified* extension F/K. This proves one implication of Theorem 1D.

In the other direction, suppose that $EF = E'F$ for some finite unramified extension F/K. Consider the totally ramified $\mathbb{Z}_p$-extension $F_\infty = FK_\infty/F$. Then, of course, the semi-linear $\mathcal{O}(F_m)$-representations of $\Gamma_m = \mathrm{Gal}(K_m/K) \approx \mathrm{Gal}(F_m/F)$ $\mathcal{O}(EF \otimes_F F_m)$ and $\mathcal{O}(E'F \otimes_F F_m)$ are isomorphic (for any m).

Now we have a natural isomorphism of F_m-algebras

$$(E \otimes_K K_m) \otimes_{K_m} F_m \approx EF \otimes_F F_m$$

which maps $x \otimes y \otimes z$ to $x \otimes (yz)$, for $x \in E$, $y \in K_m$, $z \in F_m$. Here we use the fact that $E \otimes_K F \approx EF$, since $E \cap F = K$. Taking maximal orders, we obtain an isomorphism of semi-linear $\mathcal{O}(F_m)$-representations of Γ_m

$$\mathcal{O}((E \otimes_K K_m) \otimes_{K_m} F_m) \approx \mathcal{O}(E'F \otimes_F F_m)\,. \tag{6.8}$$

Since F/K is unramified, Lemma 4 implies the equality

$$\mathcal{O}(E \otimes_K K_m) \otimes_{\mathcal{O}_m} \mathcal{O}(F_m) = \mathcal{O}((E \otimes_K K_m) \otimes_{K_m} F_m)\,. \tag{6.9}$$

Thus, combining (6.8) and (6.9), and using the fact that $\mathcal{O}(F_m)$ is a *free* $\mathcal{O}_m$-module of rank $(F : K)$, we obtain an isomorphism

$$\mathcal{O}(EF \otimes_F F_m) \approx \coprod_{(F:K)} \mathcal{O}(E \otimes_K K_m)$$

of semi-linear $\mathcal{O}_m$-representations of Γ_m.

Henceforth $EF = E'F$ implies that

$$\coprod_{(F:K)} \mathcal{O}(E \otimes_K K_m) \approx \coprod_{(F:K)} \mathcal{O}(E' \otimes_K K_m)\,. \tag{6.10}$$

In order to finish the proof of Theorem 1D, recall from (2.1) that a semi-linear $\mathcal{O}_m$-representation of Γ_m is the same thing as an $\mathcal{O}_m\#\Gamma_m$-module which is a free $\mathcal{O}_m$-module of finite rank. But the ring $\mathcal{O}_m\#\Gamma_m$ is finitely generated as an $\mathcal{O}_m$-module, and $\mathcal{O}_m$ is a discrete valuation ring. Thus the Krull–Schmidt–Azumaya Theorem applies (cf. [2, (6.12), p. 128]), and we conclude from (6.10) that $\mathcal{O}(E \otimes_K K_m)$ and $\mathcal{O}(E' \otimes_K K_m)$ are isomorphic semi-linear representations. ∎

Acknowledgements. I wish to thank the referee for pointing out minor corrections.

References

[1] S. U. Chase, *Ramification invariants and torsion Galois module structure in number fields*, J. Algebra 91 (1) (1984), 207–257.

[2] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. 1, Wiley Interscience Pure Appl. Math. Text, 1981.
[3] F. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, Lecture Notes in Math. 181, Springer, 1971.
[4] S. Sen, *On automorphisms of local fields*, Ann. of Math. 90 (1969), 33–46.
[5] —, *Integral representations associated with p-adic field extensions*, Invent. Math. 94 (1988), 1–12.
[6] J.-P. Serre, *Local Fields*, Graduate Texts in Math. 67, Springer, 1979.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ D'OTTAWA
OTTAWA, ONTARIO
CANADA K1N 6N5

Received on 21.11.1991
and in revised form on 3.8.1992 (2194)