RAMIFICATION INDEX AND MULTIPLICITY

BY

M. AUSLANDER AND D. S. RIM[1]

Introduction

Consider the family consisting of all pairs of valuation rings $R \subset S$ such that S dominates R and the field of quotients of S is a finite algebraic extension of the field of quotients of R. Then for each such pair $R \subset S$, the ramification index $r(S/R)$ is by definition $e(S/R)[\bar{S}:\bar{R}]_i$, where $[\bar{S}:\bar{R}]_i$ is the degree of inseparability of the residue class field extension $\bar{S} \supset \bar{R}$ and $e(S/R)$ is the reduced ramification index which is the index of the value group of R in that of S (see [8, pp. 50–82]). This integer-valued function on this family has the following basic properties:

(1) $r(S/R) = 1$ if and only if S is unramified over R.
(2) $r(T/R) = r(T/S) \cdot r(S/R)$.
(3) $r(S/R) = [S:R]$ (the degree of the field extension of the field of quotients of R) if S is a finitely generated R-module and the residue class field extension $\bar{R} \subset \bar{S}$ is purely inseparable.

Our main purpose in this paper is to show that there exists one and only one integer-valued function $r(S/R)$ having the above properties, where R and S are local, integrally closed noetherian domains instead of valuation rings. Before we can give a more detailed account of the main results, we need some definitions which will hold throughout the rest of the paper.

By a ring we mean a commutative, noetherian ring with a unit element 1 different from zero. If R is a ring, a ring S together with a ring homomorphism $f : R \to S$ such that $f(1) = 1$ will be called an *R-algebra*. An R-algebra S will be called a *local R-algebra* if R and S are local rings and if there is an R-algebra A which is finitely generated as an R-module such that S is isomorphic, as an R-algebra, to $A_{\mathfrak{M}}$ for some maximal ideal $\mathfrak{M}$ in A. Thus if S is a local R-algebra, then the residue class field extension $\bar{R} \subset \bar{S}$ is of finite degree, and $\mathfrak{m}S$ is an ideal of definition of S where $\mathfrak{m}$ is the maximal ideal of R (i.e., $\mathfrak{m}S$ contains some power of the maximal ideal of S). Since $\mathfrak{m}S$ and $\mathfrak{m}$ are ideals of definition in S and R, we can talk about $e_S(\mathfrak{m}S)$, the multiplicity in the sense of Samuel (see [7] or [8, VIII, Section 10]) of $\mathfrak{m}S$ in S, and $e_R(\mathfrak{m})$, the multiplicity of $\mathfrak{m}$ in R. The rational number $e_S(\mathfrak{m}S)/e_R(\mathfrak{m})$ will be called the multiplicity or reduced ramification index of the local R-algebra S and will be denoted by $e(S/R)$. In analogy with the valuation ring situation, we define the ramification index $r(S/R)$ of the local R-algebra S to be $e(S/R)[\bar{S}:\bar{R}]_i$.

Received April 13, 1962; received in revised form October 23, 1962.

[1] This work was partly supported by the National Science Foundation.

Now let $\mathfrak{A}_0$ be the family of pairs $R \subset S$ of local, integrally closed domains such that S is an R-algebra. We show in Section 1 that $r(S/R)$ on $\mathfrak{A}_0$ is an integral-valued function having the properties given above. In Section 2 we show that $r(S/R)$ is the only integral-valued function having these properties, and we also give another way of computing $r(S/R)$ for $R \subset S$ in $\mathfrak{A}_0$ using the notion of a fibre algebra. The paper then concludes with a discussion of tame ramification in terms of the reduced ramification index given above.

1. Ramification index and reduced ramification index

In the following lemma we give some elementary facts from multiplicity theory which are essentially well known. While we sketch a proof, the reader is referred to [8, VIII, Section 10] and [7] for definitions and more complete accounts of this theory.

LEMMA 1.1. (a) *Let S be a local R-algebra such that* $\dim R = \dim S$, $\mathfrak{q}$ *an ideal of definition of R, and E a finitely generated R-module. Then*

$$e_{S\otimes_R E}(\mathfrak{q}S) \leqq L_S(\bar{R} \otimes_R S)e_E(\mathfrak{q}),$$

and equality holds if S is flat as R-module (i.e., tensoring with S over R preserves exact sequences of R-modules) where $\bar{R}$ is the residue field of R, and $L_S(*)$ denotes the length of the S-module $*$.

(b) *Let R be a local domain, S a finite integral extension of R (and hence semilocal) such that* $\dim S_{\mathfrak{M}} = \dim R$ *for all maximal ideals $\mathfrak{M}$ in S. If E is a finitely generated S-module, we have that*[2]

$$e_R(\mathfrak{q})[E:R] = \textstyle\sum_i e_{E_{\mathfrak{M}(i)}}(\mathfrak{q}S_{\mathfrak{M}_i})[\bar{S}_{\mathfrak{M}_i}:\bar{R}]$$

where $[E:R]$ denotes the rank of E over R, and $\mathfrak{M}_i$ runs through all maximal ideals of S.

Proof. (a) It is clear that

$$L_S(S/\mathfrak{q}^\nu S \otimes_R E) = L_S(S \otimes_R E/\mathfrak{q}^\nu E) \leqq L_S(S \otimes_R R)L_R(E/\mathfrak{q}^\nu E)$$

for all positive integers ν. Therefore we get $e_{S\otimes_R E}(\mathfrak{q}S) \leqq L_S(S \otimes_R \bar{R})e_E(\mathfrak{q})$ if $\dim R = \dim S$. Now assume that S is R-flat. Then if $E \supset E_1 \supset \cdots \supset E_t = \mathfrak{q}^\nu E$ is a composition series of R-module E with successive factors isomorphic to $\bar{R}$, then

$$S \otimes_R E \supset S \otimes_R E_1 \supset \cdots \supset S \otimes_R E_t = \mathfrak{q}^\nu S \otimes_R E$$

is a composition series of S-module $S \otimes_R E$ with successive factors isomorphic to $S \otimes_R \bar{R}$. Then we have that $L_S(S/\mathfrak{q}^\nu S \otimes_R E) = L_S(S \otimes_R \bar{R})L_R(E/\mathfrak{q}^\nu E)$ for all ν, which implies that $e_{S\otimes_R E}(\mathfrak{q}S) = L_S(S/\mathfrak{m}S)e_E(\mathfrak{q})$.

(b) Let $0 \to F \to E \to E/F \to 0$ be an exact sequence of R-modules with F a free R-module such that $[F:R] = [E:R]$. Then E/F is a torsion R-module,

[2] When $\mathfrak{M}(i)$ is a second-order subscript, it is to be read as $\mathfrak{M}_i$.

and hence $e_{E/F}(\mathfrak{q}) = 0$. But $e_E(\mathfrak{q}) = e_F(\mathfrak{q}) + e_{E/F}(\mathfrak{q})$. Since $e_F(\mathfrak{q}) = [F:R]e_R(\mathfrak{q}) = [E:R]e_R(\mathfrak{q})$ we have that $e_E(\mathfrak{q}) = [E:R]e_R(\mathfrak{q})$. On the other hand, we know that[2]

$$L_R(E/\mathfrak{q}^\nu E) = \sum_i L_R(E_{\mathfrak{M}_i}/\mathfrak{q}^\nu E_{\mathfrak{M}_i}) = \sum L_{S_{\mathfrak{M}(i)}}(E_{\mathfrak{M}_i}/\mathfrak{q}^\nu E_{\mathfrak{M}_i})[\bar{S}_{\mathfrak{M}_i}:\bar{R}]$$

for all ν where $\mathfrak{M}_i$ runs through all the maximal ideals in S. Therefore we get $e_E(\mathfrak{q}) = \sum_i e_{E_{\mathfrak{M}(i)}}(\mathfrak{q}S_{\mathfrak{M}_i})[\bar{S}_{\mathfrak{M}_i}:\bar{R}] = [E:R]e_R(\mathfrak{q})$ since $\dim S_{\mathfrak{M}_i} = \dim R$ for all $\mathfrak{M}_i$ by the hypothesis.

Now let $\mathfrak{A}$ be the family of pairs $R \subset S$ of local domains in which R is integrally closed and S is a local R-algebra. Clearly $\mathfrak{A}$ contains the family $\mathfrak{A}_0$ of pairs $R \subset S$ of local domains in which both R and S are integrally closed and S is a local R-algebra which was mentioned in the introduction. We observe here that if $R \subset S$ and $S \subset T$ are in $\mathfrak{A}$, then so is $R \subset T$. Indeed, let $R \subset A$ and $S \subset B = S[\alpha_1, \cdots, \alpha_t]$ be finite integral extensions such that $S = A_\mathfrak{m}$ and $T = B_\mathfrak{M}$ where $\mathfrak{m}$, $\mathfrak{M}$ are maximal ideals in A, B respectively. Since α_i is integral over $S = A_\mathfrak{m}$, we can find u in $A - \mathfrak{m}$ such that $u\alpha_i$ is integral over A. It follows that, for some u in $A - \mathfrak{m}$, $B' = A[u\alpha_1, \cdots, u\alpha_t]$ is integral over A and hence is integral over R. If we set $\mathfrak{M}' = \mathfrak{M} \cap B'$, then u becomes a unit in $B'_{\mathfrak{M}'}$ and hence $B'_{\mathfrak{M}'}$ contains $\alpha_1, \cdots, \alpha_t$ and consequently $B'_{\mathfrak{M}'} = B_\mathfrak{M} = T$. Therefore $R \subset T$ is also in $\mathfrak{A}$. It is then clear that if $R \subset S$ and $S \subset T$ are in $\mathfrak{A}_0$, then so is $R \subset T$. We also observe that if $R \subset S$ is in $\mathfrak{A}$, then $\dim R = \dim S$ by the Cohen-Seidenberg "going-down theorem" since R is integrally closed [8, p. 299].

In this section we show that the ramification index, the definition of which was given in the introduction, enjoys the necessary basic properties in $\mathfrak{A}$. The following proposition gives us a useful way of computing the reduced ramification index $e(S/R)$ for $R \subset S$ in $\mathfrak{A}$.

PROPOSITION 1.2. *Let $R \subset S$ be in $\mathfrak{A}$. Then given an element α in $\bar{S}$, we can find an $R \subset A$ in $\mathfrak{A}$ with $R \subset A \subset S$ such that*

(a) $\bar{A} = \bar{R}(\bar{\alpha})$.

(b) *A is a flat R-module.*

(c) *S is a finitely generated A-module.*

Further, if $\mathfrak{q}$ is any ideal of definition of R, then

$$e_S(\mathfrak{q}S)/e_R(\mathfrak{q}) = L_A(A/\mathfrak{m}A)([S:A]/[\bar{S}:\bar{A}])$$

where $\mathfrak{m}$ is the maximal ideal in R.

Proof. Since S is a local R-algebra which is a domain, we can find an R-algebra B which is a domain and a finitely generated R-module such that $S = B_\mathfrak{M}$ for some maximal ideal $\mathfrak{M}$ in B. Let $\mathfrak{M}_1, \cdots, \mathfrak{M}_t$ be the maximal ideals in B with $\mathfrak{M} = \mathfrak{M}_1$. By the Chinese remainder theorem, we can choose an element u in $\bigcap_{i=2}^t \mathfrak{M}_i$ but not in $\mathfrak{M}$ such that the canonical image of u in $B/\mathfrak{M} = \bar{S}$ is α. Set $V = R[u]$ and $A = V_T$ where $T = V - (\mathfrak{M} \cap V)$.

Since R is integrally closed and B is a domain which is integrally dependent in R, we know that $R[u]$ is a free R-module. Since A is $R[u]$-flat, we know that A is R-flat. Further it is clear that A is a local R-algebra and that $\bar{A} = \bar{R}(\alpha)$. Thus A satisfies conditions (a) and (b) of the proposition.

Since u is in T and u is in $\bigcap_{i=2}^{t} \mathfrak{M}_i$ but not in $\mathfrak{M}_1$, we know that B_T is a local ring with maximal ideal $\mathfrak{M}_1 B_T$. Thus $B_T = B_{\mathfrak{M}_1} = S$. But B is a finite $V = R[u]$-module and T is a multiplicative set contained in V. Therefore B_T is a finite $V_T = A$-module, which shows that S is a finite A-module.

Suppose now that $\mathfrak{q}$ is an ideal of definition in R. Since A is R-flat, we know by Lemma 1.1(a) that $e_A(\mathfrak{q}A) = L_A(A/\mathfrak{m}A)e_R(\mathfrak{q})$. On the other hand, since S is a finitely generated A-module, we have by Lemma 1.1(b) that $e_S(\mathfrak{q}S)[S:A] = e_A(\mathfrak{q}A)[S:A]$. Consequently we have that

$$e_S(\mathfrak{q}S)/e_R(\mathfrak{q}) = e_S(\mathfrak{q}S)/e_A(\mathfrak{q}A)\cdot e_A(\mathfrak{q}A)/e_R(\mathfrak{q}) = L_A(A/\mathfrak{m}A)([S:A]/[\bar{S}:\bar{A}]).$$

COROLLARY 1.3. *For each $R \subset S$ in $\mathfrak{A}$ we have*

(a) $e(S/R) = e_S(\mathfrak{q}S)/e_R(\mathfrak{q})$ *where $\mathfrak{q}$ is any ideal of definition of R.*

(b) $r(S/R) = e(S/R)[\bar{S}:\bar{R}]_i$ *is a positive integer.*

(c) *If $\bar{R} \subset \bar{S}$ is a simple extension, then $e(S/R)$ is a positive integer.*

(d) *If $S \subset T$ is also in $\mathfrak{A}$, then $R \subset T$ is in $\mathfrak{A}$, and $e(T/R) = e(T/S)\cdot e(S/R)$.*

(e) *If $R \subset S$ is unramified, S is R-flat and integrally closed.*

Proof. (a) and (*b*). Let α in $\bar{S}$ be such that $\bar{R}(\alpha)$ is the separable closure of $\bar{R}$ in $\bar{S}$. Let $R \subset A$ be an R-algebra in $\mathfrak{A}$ such that $\bar{A} = \bar{R}(\alpha)$ and satisfies the other conditions of Proposition 1.2. Then we know that $[\bar{S}:\bar{A}] = [\bar{S}:\bar{R}]_i$, and thus for any ideal of definition we have that

$$e_S(\mathfrak{q}S)/e_R(\mathfrak{q}) = L_A(A/\mathfrak{m}A)([\bar{S}:\bar{R}]_i),$$

an expression which does not depend on the choice of $\mathfrak{q}$. Thus we have proved (a). Since $e(S/R)[\bar{S}:\bar{R}]_i = L_A(A/\mathfrak{m}A)[S:A]$, we have also proved (b).

(c) If $\bar{R}(\alpha) = \bar{S}$, we know there exists an $R \subset A$ in $\mathfrak{A}$ such that $\bar{A} = \bar{S}$ and such that $e(S/R) = L_A(A/\mathfrak{m}A)([S:A]/[\bar{S}:\bar{A}])$. Therefore

$$e(S/R) = L_A(A/\mathfrak{m}A)[S:A]$$

which is a positive integer.

(d) We already know that if $R \subset S$ and $S \subset T$ are in $\mathfrak{A}$, then $R \subset T$ is in $\mathfrak{A}$. Let $\mathfrak{q}$ be an ideal of definition in R. Then $\mathfrak{q}S$ is an ideal of definition in S, and we have that

$$e(T/R) = e_T(\mathfrak{q}T)/e_R(\mathfrak{q}) = e_T(\mathfrak{q}T)/e_S(\mathfrak{q}S)\cdot e_S(\mathfrak{q}S)/e_R(\mathfrak{q}) = e(T/S)\cdot e(S/R)$$

since by (a) any ideal of definition can be used to compute the multiplicity $e(S/R)$ for $R \subset S$ in $\mathfrak{A}$.

(e) Let $R \subset S$ be unramified. Then $\bar{R} \subset \bar{S}$ is separably algebraic, and hence we can find $R \subset A$ ($\subset S$) in $\mathfrak{A}$ such that $\bar{A} = \bar{S}$ and S is finitely generated as A-module. We claim that $S = A$. Indeed, S is unramified over A since S is unramified over R, and thus $S/\mathfrak{M}S = A/\mathfrak{M}$ where $\mathfrak{M}$ is the maximal ideal of A. Therefore S is generated by one element as A-module by Nakayama's lemma, and hence $S = A$. Therefore S itself is a localization of $V = R[\alpha]$ where α is integral over R. Let $f(x)$ be a minimal polynomial of α over R. Then the different[3] of V over R is the ideal $f'(\alpha)V$, and it is contained in the conductor of V in its integral closure [8, vol. 1, pp. 303–305]. Since S which is a localization of V is unramified over R, we must have that $f'(\alpha)S = S$, and in particular the conductor of S is the whole ring. Therefore S is integrally closed.

Remark. The reduced ramification index $e(S/R)$ is not in general an integer [6].

THEOREM 1.4. *The ramification index has the following properties:*

(a) *For $R \subset S$ in $\mathfrak{A}$, S is an unramified R-algebra if and only if $r(S/R) = 1$. Moreover if S is unramified, then S is R-flat.*

(b) *$r(T/R) = r(T/S)r(S/R)$ if $R \subset S$ and $S \subset T$ are both in $\mathfrak{A}$.*

(c) *Suppose S is an R-algebra which is a finite R-module and S and R are both domains with R a local ring. Then*

$$[S:R] = \textstyle\sum_i r(S_{\mathfrak{M}_i}/R)[\bar{S}_{\mathfrak{M}_i}:\bar{R}]_s$$

where $\mathfrak{M}_i$ runs through all the maximal ideals in S and $[\bar{S}_{\mathfrak{M}_i}:\bar{R}]_s$ is the degree of separability of the extension $\bar{S}_{\mathfrak{M}_i}$ of $\bar{R}$. Thus S is an unramified R-algebra if and only if $[S:R] = \sum_i [\bar{S}_{\mathfrak{M}_i}:\bar{R}]_s$.

Proof. (a) By Proposition 1.2, we know that there exists an $R \subset A$ in $\mathfrak{A}$ such that $R \subset A \subset S$, $\bar{A}$ is the separable closure of $\bar{R}$ in $\bar{S}$, $e(S/R) = L_A(A/\mathfrak{m}A)([S:A]/[\bar{S}:\bar{A}])$, and A is R-flat. Thus $r(S/R) = e(S/R)[\bar{S}:\bar{R}]_i = L_A(A/\mathfrak{m}A)[S:A]$. Therefore if $r(S/R) = 1$, then $L_A(A/\mathfrak{m}A) = 1$ and $[S:A] = 1$. Therefore A is unramified over R and hence is integrally closed, and thus we must have $A = S$ since S is integral over A and $[S:A] = 1$. Consequently S is unramified. Conversely, if S is unramified over R, then S is R-flat, and hence, by Lemma 1.1(a), $e(S/R) = L_S(\bar{R} \otimes_R S) = 1$. Therefore $r(S/R) = e(S/R)[\bar{S}:\bar{R}]_i = 1$.

(b) follows immediately from the definition $r(S/R) = e(S/R)[\bar{S}:\bar{R}]_i$ and the fact that $e(S/R)$ is multiplicative (see Corollary 1.3) and the fact that the degree of inseparability is multiplicative.

(c) By Lemma 1.1(b) we have that[2]

$$e_R(\mathfrak{q})[S:R] = \sum e_{S_{\mathfrak{M}(i)}}(\mathfrak{q}S_{\mathfrak{M}_i})[\bar{S}_{\mathfrak{M}_i}:\bar{R}],$$

and thus $[S:R] = \sum e(S_{\mathfrak{M}_i}/R)[\bar{S}_{\mathfrak{M}_i}:\bar{R}]$. Since

$$r(S_{\mathfrak{M}_i}/R) = e(S_{\mathfrak{M}_i}/R)[\bar{S}_{\mathfrak{M}_i}:\bar{R}]_i,$$

it follows that $[S:R] = \sum r(S_{\mathfrak{M}_i}/R)[\bar{S}_{\mathfrak{M}_i}:\bar{R}]_s$. Now S is an unramified R-algebra if and only if $S_{\mathfrak{M}_i}$ is an unramified R-algebra for all i, or in view

[3] For a simple extension over an integrally closed domain, the various notions of different coincide [5].

of (a), if and only if $r(S_{\mathfrak{M}_i}/R) = 1$ for all i. Since the $r(S_{\mathfrak{M}_i}/R)$ are all positive integers, we have that $[S:R] = \sum_i [\bar{S}_{\mathfrak{M}_i}:\bar{R}]_s$ if and only if $r(S_{\mathfrak{M}_i}/R) = 1$ for all i, which finishes the proof of the theorem.

PROPOSITION 1.5. (a) *Let $R \subset S$ be in $\mathfrak{A}$. If the completion $\hat{R}$ is an integral domain, then $r(S/R) = [\hat{S}:\hat{R}]/[\bar{S}:\bar{R}]_s$ where the circumflex denotes the completion.*[4]

(b) *Let $R \subset S$ be in $\mathfrak{A}_0$ and let the quotient-field extension $k \subset K$ be Galois. Then $r(S/R)$ = the order of the inertia group*[5] *of S over R.*

Proof. (a) $r(S/R) = e(S/R)[\bar{S}:\bar{R}]_i = e(\hat{S}/\hat{R})[\bar{S}:\bar{R}]_i$. Since $\hat{R}$ is complete and $\hat{S} \otimes_R \bar{R}$ is finitely generated, $\hat{S}$ is a finitely generated $\hat{R}$-module, i.e., $\hat{S}$ is integral over $\hat{R}$. Therefore by Lemma 1.1(b) we get

$$e(\hat{S}/\hat{R}) = [\hat{S}:\hat{R}]/[\bar{S}:\bar{R}],$$

and consequently $r(S/R) = [\hat{S}:\hat{R}][\bar{S}:\bar{R}]_i/[\bar{S}:\bar{R}] = [\hat{S}:\hat{R}]/[\bar{S}:\bar{R}]_s$.

(b) Let G_I be the inertia group of S over R, and let U be the subring of S which is left fixed by G_I. Then we know that $R \subset U$ is unramified, S is finitely generated as U-module, and $\bar{U} \subset \bar{S}$ is purely inseparable [1, pp. 35–40]. Therefore $r(S/R) = r(S/U)r(U/R) = r(S/U) = e(S/U)[\bar{S}:\bar{U}]$. But S is finitely generated as U-module, and thus by Lemma 1.1(b) we get $e(S/U) = [S:U]/[\bar{S}:\bar{U}]$. Therefore $r(S/R) = [S:U]$ = the order of the inertia group G_I.

2. Axioms for ramification index

We now consider the ramification index as a function in $\mathfrak{A}_0$, the family of pairs $R \subset S$ of integrally closed local domains such that S is a local R-algebra. We know that if $R \subset S$ and $S \subset T$ are in $\mathfrak{A}_0$, then $R \subset T$ is also in $\mathfrak{A}_0$. Since $\mathfrak{A}_0$ is contained in $\mathfrak{A}$, we know by Theorem 1.4 that the ramification index restricted to $\mathfrak{A}_0$ has the following properties:

(A1) If $R \subset S$ in $\mathfrak{A}_0$ is unramified, then $r(S/R) = 1$.
(A2) If $R \subset S$ and $S \subset T$ are in $\mathfrak{A}_0$ and either $R \subset S$ or $S \subset T$ is unramified, then $r(T/R) = r(T/S)$ or $r(S/R)$ respectively.
(A3) If $R \subset S$ in $\mathfrak{A}_0$ is such that $\bar{S}$ is a purely inseparable extension of $\bar{R}$ and S is a finite R-module, then $r(S/R) = [S:R]$.

THEOREM 2.1. *Properties* (A1) *through* (A3) *completely characterize the ramification index restricted to $\mathfrak{A}_0$.*

This theorem follows easily from the following result.

PROPOSITION 2.2. *Given $R \subset S$ in $\mathfrak{A}_0$, there exists an unramified extension $S \subset V$ in $\mathfrak{A}_0$ with the property that there exists an unramified extension U of*

[4] This shows that our definition of the ramification index coincides with that of Abhyankar in the geometric case (see [1]).

[5] The inertia group G_I of S over R is the subgroup of G, the Galois group of K over k, consisting of all σ in G such that $\sigma(S) \subset S$ (see [1, pp. 35–40]).

R in $\mathfrak{A}_0$ such that V contains U and is a finitely generated U-module, and such that $\bar{V}$ is a purely inseparable extension of $\bar{U}$.

Proof. Let $k \subset K$ be the fields of quotients of R and S respectively, let K' be the separable closure of k in K, and let $S' = K \cap S$. Then it is easily seen that $R \subset S'$ and $S' \subset S$ are in $\mathfrak{A}_0$ and also that S is a finitely generated S'-module since $K' \subset K$ is a purely inseparable extension and hence every integral extension of S' in K is a local ring. Let L be the normal closure of K over k, and L' the separable closure of k in L. Then $k \subset L'$ is a finite Galois extension, and the integral closure A of R in L' is a finitely generated R-module. Let $\mathfrak{M}$ be a maximal ideal in A such that $A_{\mathfrak{M}}$ dominates S', and let U be the inertial ring of $A_{\mathfrak{M}}$ over R, i.e., U is the intersection of $A_{\mathfrak{M}}$ with the fixed field of the subgroup of the Galois group of $k \subset L'$ which sends $\mathfrak{M}$ into itself. It follows from Krull's ramification theory in Galois extensions (see [1, I, Section 7]) that $R \subset U$ is the maximal unramified extension of R in $A_{\mathfrak{M}}$, that $A_{\mathfrak{M}}$ is a finitely generated U-module, and that $\bar{U}$ is the separable closure of $\bar{R}$ in $\bar{A}_{\mathfrak{M}}$. Letting $S'U$ be the composite of S' and U in $A_{\mathfrak{M}}$, we see that $U \subset S'U \subset A_{\mathfrak{M}}$ and thus $S'U$ is a local ring which is a finitely generated U-module, and also that $\overline{S'U}$ is a purely inseparable extension of $\bar{U}$. Since S is finitely generated as an S'-module, it follows that SU is finitely generated as an $S'U$-module. Also SU is local since the field of quotients of $S'U$ is purely inseparable over SU. For the same reason $\overline{S'U}$ is purely inseparable over $\overline{SU}$. Finally, since U is unramified over R, SU is unramified over S and thus integrally closed, by Corollary 1.3(e), since S is integrally closed. Therefore SU is our desired V, and the proposition is complete.

We now return to the proof of Theorem 2.1. Let f be a function from $\mathfrak{A}_0$ to the rationals which satisfies properties (A1) through (A3). Let $R \subset S$ be in $\mathfrak{A}_0$, and $S \subset V$ and $R \subset U$ elements in $\mathfrak{A}_0$ which satisfy the hypothesis of Proposition 2.2. Then $f(V/R) = f(V/U)f(U/R) = f(V/U) = [V:U]$. But we also have that $f(V/R) = f(V/S)f(S/R) = f(S/R)$. Thus $f(S/R) = [V:U]$ which is independent of the choice of f. Thus if f satisfies (A1) through (A3), f equals the ramification index on $\mathfrak{A}_0$.

As an application of Theorem 2.1, we conclude this section of the paper by giving another method of computing the ramification index of $R \subset S$ in $\mathfrak{A}_0$ in terms of the fibre algebra of S over R.

Given a local R-algebra S over a local ring R we have an exact sequence

$$0 \to \mathfrak{J} \to S \otimes_R S \xrightarrow{\varphi} S \to 0$$

where $\varphi(x \otimes y) = xy$ and $\mathfrak{J}$ is the kernel of φ. Let $\mathfrak{N} = \varphi^{-1}(\mathfrak{M})$ where $\mathfrak{M}$ is the maximal ideal of S. We define $S_R^f = (S \otimes_R S)_{\mathfrak{N}}$ and call it the fibre algebra of a local R-algebra S. As usual we use the notation S^e for $S \otimes_R S$. The map $S \to S \otimes_R S$ given by $s \to s \otimes 1$ induces a ring homomorphism

$S \to S^f$, and through this map S^f becomes a local S-algebra. Now S, being a local R-algebra, is equal to A_Δ for some finite integral extension A of R and for some multiplicative set Δ in A. Therefore $S^e = S \otimes_R S = (A \otimes_R A)_{\Delta'}$ where $\Delta' = \{u \otimes v \mid u, v \in \Delta\}$ is a multiplicative subset of $A \otimes_R A$. Consequently S^e is a noetherian ring. Thus we know that S is unramified over R if and only if S is S^e-projective [2, §7] i.e., $S_{\mathfrak{P}}$ is $(S^e)_{\mathfrak{P}}$-free for all maximal ideals $\mathfrak{P}$ in S^e. But if $\mathfrak{P} \neq \mathfrak{M}$, then $S_{\mathfrak{P}} = 0$, and hence S is S^e-projective if and only if $S_{\mathfrak{M}} = S$ is $(S^e)_{\mathfrak{M}} = S^f$-free. However

$$S^f \xrightarrow{\varphi} S \to 0$$

is exact, and thus S is S^f-free if and only if φ is an isomorphism. Since the composite map $S \to S^f \to S$ is identity, we see that S is unramified over R if and only if $S^f = S$ as a local S-algebra. Thus the deviation of S^f from being identical to S measures a degree of the ramification, and thus we are led to consider $e(S^f/S)$. The rest of this section is devoted to showing that $r(S/R) = e(S^f/S)$ if $R \subset S$ is in $\mathfrak{A}_0$. We begin with the following lemma.

LEMMA 2.3. *Let S be a local R-algebra, and T a local S-algebra. If S is an unramified R-algebra, then the homomorphism $T^f_R \to T^f_S$ induced from the natural map $T \otimes_R T \to T \otimes_S T$ is an isomorphism.*

Proof. Since S is an unramified R-algebra, the exact sequence

$$0 \to \mathfrak{J} \to S \otimes_R S \to S \to 0$$

splits as S^e-modules. Therefore $0 \to T^e_R \otimes_{S^e} \mathfrak{J} \to T^e_R \to T^e_R \otimes_{S^e} S \to 0$ is exact and splits as T^e_R-modules. By one of the standard associativity laws we have that $T^e_R \otimes_{S^e} S = (T \otimes_R T) \otimes_{S \otimes S} S = T \otimes_S T = T^e_S$. Thus we find that the natural epimorphism $T^e_R \to T^e_S$ splits as T^e_R-modules. Let $\mathfrak{N}$ be the maximal ideal of T, and $\mathfrak{n}$ the preimage of $\mathfrak{N}$ under the map $T \otimes_R T \to T$. Localizing by $\mathfrak{n}$, we see that $T^f_R \to T^f_S$ splits as T^f_R-module since $(T^e_R)_\mathfrak{n} = T^f_R$ and $(T^e_S)_\mathfrak{n} = T^f_S$. Consequently $T^f_R = T^f_S$ since T^f_R is a local ring.

PROPOSITION 2.4. *Let S be a local R-algebra, and T a local S-algebra. Then we have the following*:

(a) *If S is an unramified R-algebra, then $e(T^f_R/T) = e(T^f_S/T)$.*

(b) *If T is an unramified and flat S-algebra, then $e(T^f_R/T) = e(S^f_R/S)$.*

Proof. (a) If S is an unramified R-algebra, we have that $T^f_R \approx T^f_S$ by Lemma 2.3, and hence $e(T^f_R/T) = e(T^f_S/T)$.

(b) The fact that T is a flat and unramified S-algebra entails that T^e_R is a flat and unramified S^e_R-algebra [4, Proposition 1.5], and hence $T^e_R \otimes_{S^e} S^f$ is a flat and unramified S^f-algebra [4, Corollary 1.6]. However T^f_R is a localization of $T^e_R \otimes_{S^e} S^f$ by a maximal ideal, and consequently T^f_R is a flat and unramified S^f-algebra. Now applying Lemma 1.1(a), we have that

$e_{S^f}(\mathfrak{M}S^f) = e_{T^f_R}(\mathfrak{M}T^f_R)$ and $e_S(\mathfrak{M}) = e_T(\mathfrak{M}T)$ where $\mathfrak{M}$ is the maximal ideal of S. Since $\mathfrak{M}T$ is the maximal ideal of T and $\mathfrak{M}T^f_R = (\mathfrak{M}T)T^f_R$, we have that $e(T^f_R/T) = e(S^f_R/S)$.

THEOREM 2.5. *For a local algebra $R \subset S$ in $\mathfrak{A}_0$, we have that $r(S/R) = e(S^f/S)$.*

Proof. Since $S^f = S$ if S is an unramified R-algebra, we know that $e(S^f/S) = 1$ if $S \supset R$ is unramified. Thus $e(S^f/S)$ satisfies condition (A1). The fact that $e(S^f/S)$ satisfies condition (A2) follows immediately from Proposition 2.4 and the fact that if $R \subset S$ is in $\mathfrak{A}_0$ and S is an unramified R-algebra, then S is R-flat (see Theorem 1.4). Thus if we show that $e(S^f/S)$ satisfies (A3), we will be done.

Suppose S is a finite R-module, and that $\bar{S}$ is purely inseparable over $\bar{R}$. Then $S \otimes_R S$ is a local ring, and consequently $S^f_R = S \otimes_R S$ is a finite local S-algebra with $[S \otimes_R S:S] = [S:R]$. However by Lemma 1.1(b) we have that $e(S^f_R/S) = [S \otimes_R S:S]/[\overline{S \otimes_R S}:S] = [S:R]$ since $\bar{S}$ is purely inseparable over $\bar{R}$ and thus $\bar{S} = \overline{S \otimes_R S}$. Therefore $e(S^f/S)$ satisfies (A1) through (A3), and thus $e(S^f/S) = r(S/R)$.

3. Tame ramification

Let $R \subset S$ of local domains be in $\mathfrak{A}$, i.e., R is integrally closed and S is a local R-algebra. Then the ramification index $r(S/R)$ is an integer, and thus the notion of tame ramification is well defined. Namely $R \subset S$ in $\mathfrak{A}$ is called tamely ramified if $\bar{S}$ is separably algebraic over $\bar{R}$ and $r(S/R)$ is not divisible by the field characteristic of $\bar{R}$. More generally, let R be an integrally closed local domain, and let $R \subset S$ be an integral extension with a separable quotient-field extension of finite degree. Then, for each maximal ideal $\mathfrak{p}$ in S, $R \subset S_\mathfrak{p}$ is in $\mathfrak{A}$. We shall simply say that $R \subset S$ is tamely ramified if there exists at least one maximal ideal $\mathfrak{p}$ in S such that $R \subset S_\mathfrak{p}$ is tamely ramified. We observe that in the case when S is the integral closure of R in a Galois extension of finite degree, then all maximal ideals are conjugate, and consequently if $R \subset S$ is tamely ramified in our sense, then every maximal ideal is tamely ramified.

The main purpose of this section is to prove Theorem 3.2. If R is an integrally closed domain, and if $R \subset S$ is an integral extension with the quotient-field extension $k \subset K$ of finite degree, then $t(x; K \mid k)$ is in R for all $x \in S$, where $t(x; K \mid k) =$ the trace of $x \in \mathrm{Hom}_k(K, K)$ given by $x(y) = xy$. If R is a local ring, $\overline{t(x; K \mid k)}$ will denote the image of $t(x; K \mid k)$ under the canonical map $R \to \bar{R}$. For each maximal ideal $\mathfrak{M}_i$ in S we set $S_i = S_{\mathfrak{M}_i}$ and denote by h_i the canonical map $S \to \bar{S}_i$.

PROPOSITION 3.1. *Let R be an integrally closed local domain, and let $R \subset S$ be an integral extension with the quotient-field extension $k \subset K$ being separably* *algebraic of finite degree. Then for each $x \in S$ we have*

$$\overline{t(x;\, K \mid k)} = \textstyle\sum_{\mathfrak{M}_i} r(S_i/R)t(h_i\, x;\, \bar{S}_i \mid \bar{R})$$

where $\mathfrak{M}_i$ ranges through all maximal ideals of S.

Proof. (i) Assume that S is R-free. Then $\overline{t(x;\, K \mid k)} = t(x;\, \bar{S} \mid \bar{R})$ where $\bar{S} = S/\mathfrak{m}S$ and $\mathfrak{m}$ is the maximal ideal of R. However, if

$$\begin{array}{ccccccccc} 0 & \rightarrow & V' & \rightarrow & V & \rightarrow & V'' & \rightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \rightarrow & V' & \rightarrow & V & \rightarrow & V'' & \rightarrow & 0 \end{array}$$

is an exact commutative diagram of vector spaces over a field, then $\mathrm{Tr}(f) = \mathrm{Tr}(f') + \mathrm{Tr}(f'')$ where $Tr(*)$ = trace of the linear transformation $*$. It folows from this fact and Lemma 1.1(a) that

$$\overline{t(x;\, K \mid k)} = t(x;\, \bar{S} \mid \bar{R}) = \textstyle\sum_i L_{S_i}(S_i/\mathfrak{m}S_i)t(h_i\, x;\, \bar{S}_i \mid \bar{R})$$
$$= \textstyle\sum_i e(S_i/R)t(h_i\, x;\, \bar{S}_i \mid \bar{R})$$

Since $t(h_i\, x;\, \bar{S}_i \mid \bar{R}) = 0$ for all i for which $\bar{S}_i$ is not separably algebraic over $\bar{R}$, and $e(S_i/R) = r(S_i/R)$ if $\bar{R} \subset \bar{S}_i$ is separably algebraic, we see that our proposition is valid for a free extension.

(ii) *General case.* Among the maximal ideals $\mathfrak{M}_1, \mathfrak{M}_2, \cdots, \mathfrak{M}_l$ of S, let $\mathfrak{M}_1, \cdots, \mathfrak{M}_t$ be such that $\bar{S}_i$ is separably algebraic over $\bar{R}$. Thus $\bar{S}_j$ is not separably algebraic over $\bar{R}$ for $t < j \leqq l$. Our proof proceeds in two steps: (a) Assume that $x \in S$ has the property that $\bar{R}(h_i\, x)$ is not separable over $\bar{R}$ for all $t < i \leqq l$. Set $T = R[x]$, and let L be the field of quotients of T. Then the hypothesis on x implies that if $S_i \supset T_j$ and $\bar{T}_j$ is separably algebraic over $\bar{R}$, then $1 \leqq i \leqq t$. Now $T = R[x]$ is R-free since R is integrally closed. Therefore

$$\overline{t(x;\, L \mid k)} = \textstyle\sum_j e(T_j/R)t(h_j\, x;\, \bar{T}_j \mid \bar{R})$$

by (i) where j ranges through only those subscripts for which $\bar{T}_j$ is separably algebraic over $\bar{R}$. On the other hand we have

$$(**) \qquad e_{T_j}(\mathfrak{m}T_j)[K:L] = \textstyle\sum_k e_{S_{jk}}(\mathfrak{m}S_{jk})[\bar{S}_{jk}:\bar{T}_j]$$

by Lemma 1.1. If $\bar{T}_j$ is separably algebraic over $\bar{R}$, then $\bar{S}_{jk}$ is also separably algebraic over $\bar{R}$ by the hypothesis on x. It follows from Corollary 1.3 that $e(S_{jk}/R)$ are all integers. In other words, all $e_{S_{jk}}(\mathfrak{m}S_{jk})$ (and of course $e_{T_j}(\mathfrak{m}T_j)$) are divisible by $e_R(\mathfrak{m})$. Therefore from $(**)$ we get

$$e(T_j/R)[K:L] = \textstyle\sum_k e(S_{jk}/R)[\bar{S}_{jk}:\bar{T}_j].$$

Consequently we have

$$\begin{aligned}\overline{t(x;K\mid k)} &= [K:L]\overline{t(x;L\mid k)} = \textstyle\sum_j [K:L]e(T_j/R)t(h_j x;\ \bar{T}_j \mid \bar{R})\\ &= \textstyle\sum_{j,k} e(S_{jk}/R)[\bar{S}_{jk}:\bar{T}_j]t(h_j x;\ \bar{T}_j\mid \bar{R}) = \sum_{j,k} e(S_{jk}/R)t(h_{jk}x;\ \bar{S}_{jk}\mid\bar{R})\\ &= \textstyle\sum_{1\leqq i\leqq t} e(S_i/R)t(h_i x;\ \bar{S}_i\mid\bar{R}) = \sum_{\mathfrak{M}_i} r(S_i/R)t(h_i x;\ \bar{S}_i\mid\bar{R})\end{aligned}$$

since $t(h_j x;\ \bar{S}_j \mid \bar{R}) = 0$ for $j > t$ and $e(S_i/R) = r(S_i/R)$ for $1 \leqq i \leqq t$.

(b) Let $x \in S$ be arbitrary. Let

$$\Delta = \{j \mid t < j \leqq l \text{ and } h_j x \text{ is separable over } \bar{R}\}.$$

Since $\bar{S}_j$ is not separable over $\bar{R}$ for each $j \in \Delta$, we can find $a_j \in \bar{S}_j$ such that $h_j x - a_j$ is not separable over $\bar{R}$. Then a_j is also not separable over $\bar{R}$ since $h_j x$ is separable over $\bar{R}$. By the Chinese remainder theorem we can find $y \in S$ such that

$$\begin{aligned} h_j y &= 0 \quad \text{if} \quad j \notin \Delta,\\ &= a_j \quad \text{if} \quad j \in \Delta.\end{aligned}$$

Then $z = x - y$ and y both have the property that $h_j z$ and $h_j y$ are not separable for all $t < j \leqq l$. Therefore we are brought to the above case (a), and we get

$$\begin{aligned}\overline{t(x;K\mid k)} &= t(y+z;K\mid k) = \overline{t(y;K\mid k)} + \overline{t(z;K\mid k)}\\ &= \textstyle\sum_{\mathfrak{M}_i} r(S_i/R)t(h_i y;\ \bar{S}_i\mid\bar{R}) + \sum_{\mathfrak{M}_i} r(S_i/R)t(h_i z;\ \bar{S}_i\mid\bar{R})\\ &= \textstyle\sum_{\mathfrak{M}_i} r(S_i/R)t(h_i x;\ \bar{S}_i\mid\bar{R}).\end{aligned}$$

This completes the proof.

THEOREM 3.2. *Let R be an integrally closed local domain, and $R \subset S$ an integral extension with the quotient-field extension $k \subset K$ being separably algebraic of finite degree. Then S is tamely ramified over R if and only if $t(S; K \mid k) = R$.*

Proof. We have from Proposition 3.1 that

$$\overline{t(x;K\mid k)} = \textstyle\sum_i r(S_i/R)t(h_i x;\ \bar{S}_i\mid\bar{R})$$

for all $x \in S$. Assume that $t(S; K \mid k) = R$. Then there exists x in S such that $t(x; K \mid k) = 1$ and consequently $r(S_i/R)t(h_i x;\ \bar{S}_i \mid \bar{R}) \neq 0$ for some i. Therefore $t(h_i x;\ \bar{S}_i \mid \bar{R}) \neq 0$ and $r(S_i/R) \neq 0$ in $\bar{R}$, i.e., $\bar{S}_i$ is separably algebraic over $\bar{R}$, and $r(S_i/R)$ is not divisible by the field characteristic. Conversely, assume that S is tamely ramified over R, i.e., for some i, $\bar{S}_i$ is separably algebraic over $\bar{R}$ and $r(S_i/R)$ is not divisible by the field characteristic of $\bar{R}$. Then from the above formula and the Chinese remainder theorem we can find x in S such that $\overline{t(x;K\mid k)} \neq 0$. Thus $t(S;K\mid k) \not\subset \mathfrak{m}$, and consequently $t(S;\ K \mid k) = R$ where $\mathfrak{m}$ is the maximal ideal of R.

COROLLARY 3.3. *Let R be an integrally closed domain (which need not be local), and let $S \supset R$ be an integral extension with the quotient-field extension*

$k \subset K$ being separably algebraic of finite degree. Then the set of prime ideals $\mathfrak{p}$ in R such that $S_{\mathfrak{p}}$ is not tamely ramified over $R_{\mathfrak{p}}$ form a closed set $\{\mathfrak{p} \mid \mathfrak{p} \supset t(S; K \mid k)\}$.

For the Galois extensions we find an interesting connection between tamely ramified extensions and the twisted group ring. Given a representation of a finite group G by ring automorphisms of S, the twisted group ring $S(G)$ is defined as follows: $S(G)$ is free (left) S-module with free basis $\{\sigma \mid \sigma \in G\}$ and multiplication $(a\sigma)(b\tau) = a\sigma(b)\sigma\tau$. This is nothing but the trivial factor set in $H^2(G, U(S))$ where $U(S)$ = the group of units in S.

LEMMA 3.4. *For any $S(G)$-module A and S-module C we have*

$$\mathrm{Ext}_S(A, C) \approx \mathrm{Ext}_{S(G)}(A, S(G) \otimes_S C).$$

Consequently, $\mathrm{hd}_S A \leqq \mathrm{hd}_{S(G)} A$, *and the equality holds if* $\mathrm{hd}_{S(G)} A < \infty$.

Proof. For $S(G)$-module A and S-module C, define

$$p : \mathrm{Hom}_S(A, C) \to \mathrm{Hom}_{S(G)}(A, S(G) \otimes_S C)$$

by $pf(a) = \sum_{g\in G} g \otimes f(g^{-1}a)$ as in the ordinary group algebra. This is well defined since for any $x \in S$ and $h \in G$ we have

$$\begin{aligned} pf(sha) &= \textstyle\sum_{g\in G} g \otimes f(g^{-1}sha) = \sum_{g\in G} g \otimes g^{-1}(s)f(g^{-1}ha) \\ &= \textstyle\sum_{g\in G} sg \otimes f(g^{-1}ha) = \sum_{g\in G} shg^{-1} \otimes f(ga) = sh(pf(a)). \end{aligned}$$

Consider $\phi \in \mathrm{Hom}_S(S(G) \otimes_S C, C)$ given by $\phi(\sum_{g\in G} g \otimes c_g) = c_1$. Then it is clear that $x = \sum_{g\in G} g \otimes \phi(g^{-1}x)$ for all $x \in S(G) \otimes_S C$. Thus given $f \in \mathrm{Hom}_{S(G)}(A, S(G) \otimes_S C)$ we have

$$[p(\phi f)](a) = \textstyle\sum_{g\in G} g \otimes \phi f(g^{-1}a) = \sum_{g\in G} g \otimes \phi(g^{-1}f(a)) = f(a),$$

i.e., p is an epimorphism. However p is clearly a monomorphism, and thus p establishes the isomorphism $\mathrm{Hom}_S(A, C) \approx \mathrm{Hom}_{S(G)}(A, S(G) \otimes_S C)$. Consequently $\mathrm{Ext}_S(A, C) \approx \mathrm{Ext}_{S(G)}(A, S(G) \otimes_S C)$, and hence $\mathrm{hd}_S A \leqq \mathrm{hd}_{S(G)} A$. If $\mathrm{hd}_{S(G)} A = d < \infty$, then $\mathrm{Ext}^d_{S(G)}(A, S(G)) \neq 0$, and hence $\mathrm{Ext}^d_S(A, S(G)) \neq 0$, and consequently $\mathrm{hd}_S A = \mathrm{hd}_{S(G)} A$.

PROPOSITION 3.5. *Let a finite group G be represented as ring automorphisms of S. Then the following statements are equivalent:*

(1) $\mathrm{hd}_{S(G)} S < \infty$.

(2) $\mathrm{hd}_{S(G)} S = 0$.

(3) *There exists an element $x \in S$ such that* $\sum_{g\in G} g(x) = 1$.

(4) $\mathrm{hd}_{S(G)} A = \mathrm{hd}_S A$ *for all $S(G)$-modules A.*

Proof. (1) $\Rightarrow$ (2) follows immediately from the above lemma. (2) $\Rightarrow$ (3): Consider the $S(G)$-epimorphism

$$S(G) \xrightarrow{\varphi} S \to 0$$

given by $\varphi(\sum_{g\in G} s_g\, g) = \sum_{g\in G} s_g$. S being $S(G)$-projective, the epimorphism $\varphi : S(G) \to S$ admits a cross-section $\psi : S \to S(G)$. Let $\psi(1) = \sum_{g\in G} s_g\, g$. Then

$$\psi(1) = \psi(h(1)) = h(\textstyle\sum_{g\in G} s_g\, g) = \sum_{g\in G} h(s_g)hg = \sum_{g\in G} h(s_{h^{-1}g})g$$

for all $h \in G$ entails that $s_g = g(s_1)$ for all $g \in G$, i.e., $\psi(1) = \sum_{g\in G} g(s)g$ for some $s \in S$. Then $1 = \varphi\psi(1) = \sum_{g\in G} g(s)$. (3) $\Rightarrow$ (4): For $S(G)$-modules A, B, it is clear that

$$\mathrm{Hom}_{S(G)}(A, B) = \mathrm{Hom}_{S(G)}(S, \mathrm{Hom}_S(A, B)).$$

Since $\psi : S \to S(G)$ given by $\psi(s) = \sum_{g\in G} sg(x)g$ provides a cross-section for the map $\varphi : S(G) \to S$, S is $S(G)$-projective. Therefore we have

$$\mathrm{Ext}_{S(G)}(A, B) = \mathrm{Hom}_{S(G)}(S, \mathrm{Ext}_S(A, B)),$$

and consequently $h_{S(G)}A \leqq \mathrm{hd}_S\, A$. However we have $\mathrm{hd}_{S(G)}\, A \geqq \mathrm{hd}_S\, A$ by Lemma 3.4, and hence $\mathrm{hd}_{S(G)}\, A = \mathrm{hd}_S\, A$. (4) $\Rightarrow$ (1) is obvious.

COROLLARY 3.6. *Let R be an integrally closed domain with field of quotients k, and let S be the integral closure of R in a Galois extension of k with Galois group G. Then S is tamely ramified over R if and only if* $\mathrm{hd}_{S(G)}\, A = \mathrm{hd}_S\, A$ *for all $S(G)$-modules A.*

Let $R \subset S$ be as in the above corollary with Galois group G, and assume that R is a Dedekind domain. Then it follows from the above corollary that $S(G)$ is an hereditary order if and only if S is a tamely ramified extension of R. On the other hand, we have $S(G) \subset \mathrm{Hom}_R(S, S)$, and then $S(G)$ is a maximal order if and only if $S(G) = \mathrm{Hom}_R(S, S)$, i.e., if and only if S is unramified over R (see [4, p. 398, A5, A6]). Thus if S is tamely ramified over R with the ramification index > 1, then $S(G)$ is an hereditary order without being maximal. An example of nonmaximal hereditary order given in [3] is actually of this kind. We studied above only the trivial factor set in $H^2(G, U(S))$. S. Williamson has recently shown (unpublished) that if $S \supset R$ is tamely ramified, every order corresponding to any factor set in $H^2(G, U(S))$ is hereditary.

4. Trace map

We conclude this paper with a proof of the fact that if R is an integrally closed, noetherian domain and S is an integral extension of R in a finite, separable field extension of the field of quotients of R, then $t(S)S$ contains $\mathfrak{H}(S/R)$ where t is the trace map of S into R, and $\mathfrak{H}(S/R)$ is the homological different of the R-algebra S as defined in [2]. This result will follow quickly from the following general remarks concerning the trace.

Suppose S is an arbitrary commutative R-algebra where R is also an arbitrary commutative ring. Then we have an exact sequence

$$0 \to \mathcal{J} \to S \otimes_R S \xrightarrow{\phi} S \to 0$$

of S^e-modules where $\phi(x \otimes y) = xy$. Then if we let $\mathfrak{A}$ be the annihilator of $\mathcal{J}$ in S^e, the homological different of the R-algebra S is defined to be the ideal $\phi(\mathfrak{A})$ contained in S. The R-algebra S is said to be separable (or unramified) if there is an element a in $\mathfrak{A}$ such that $\phi(a) = 1$, or what amounts to the same thing, if S is S^e-projective. The reader is referred to [2] for the basic properties of $\mathfrak{H}(S/R)$ and its connections with ramification theory.

Now suppose $f \in \mathrm{Hom}_R(S, R)$. Then we define $\alpha(f) : S^e \to S$ by $\alpha(f)(x \otimes y) = f(x)y$. It is clear that $\alpha(f)$ is an S-homomorphism if $S \otimes S$ is considered an S-module by means of the operation $s(x \otimes y) = x \otimes sy$ but not in general an S^e-homomorphism. However a simple calculation shows that $\alpha(f) \mid \mathfrak{A}$ is an S^e-homomorphism. For an element $\sum x_i \otimes y_i$ is in $\mathfrak{A}$ if and only if $(x \otimes 1)(\sum x_i \otimes y_i) = (1 \otimes x)(\sum x_i \otimes y_i)$ for all x in S. Therefore if $\sum x_i \otimes y_i \in \mathfrak{A}$, then we have that

$$\begin{aligned}(x \otimes y)(\textstyle\sum x_i \otimes y_i) &= (1 \otimes y)((x \otimes 1)(\textstyle\sum x_i \otimes y_i)) \\ &= (1 \otimes y)((1 \otimes x)\textstyle\sum x_i \otimes y_i) = \textstyle\sum x_i \otimes y_i xy.\end{aligned}$$

Therefore

$$\begin{aligned}\alpha(f)((x \otimes y)(\textstyle\sum x_i \otimes y_i)) &= \alpha(f)(\textstyle\sum x_i \otimes y_i xy) = xy \textstyle\sum f(x_i) y_i \\ &= (x \otimes y)(\alpha(f)(\textstyle\sum x_i \otimes y_i)).\end{aligned}$$

Thus we have a homomorphism $\alpha : \mathrm{Hom}_R(S, R) \to \mathrm{Hom}_{S^e}(\mathfrak{A}, S)$. Now if we consider $\mathrm{Hom}_R(S, R)$ an S-module by $(xf)(y) = f(xy)$ for all s, y in S and all f in $\mathrm{Hom}_R(S, R)$, and consider $\mathrm{Hom}_{S^e}(\mathfrak{A}, S)$ an S-module by $(xg)(a) = x(g(a))$ for all x in S, g in $\mathrm{Hom}_{S^e}(\mathfrak{A}, S)$, and a in $\mathfrak{A}$, then α is an S-homomorphism. For if $\sum x_i \otimes y_i$ is in $\mathfrak{A}$, then

$$\begin{aligned}\alpha(xf)\textstyle\sum x_i \otimes y_i &= \textstyle\sum f(xx_i)y_i = \alpha(f)((x \otimes 1)(\textstyle\sum x_i \otimes y_i)) \\ &= \alpha(f)(\textstyle\sum x_i \otimes y_i x) = \textstyle\sum f(x_i) y_i x = (x(\alpha f))(\textstyle\sum x_i \otimes y_i).\end{aligned}$$

Viewing S as an R-module, then it is well known that S is a finitely generated projective R-module if and only if there exists a finite number of elements $b_1, \cdots, b_n$ in S and $g_1, \cdots, g_n$ in $\mathrm{Hom}_R(S, R)$ such that $x = \sum g_i(x) b_i$ for all x in S. Such a system of elements will be called a projective coordinate system. Assuming that S is a finitely generated, projective R-module, we define t in $\mathrm{Hom}_R(S, R)$ by $t = \sum b_i g_i$ (i.e., $t(x) = \sum g_i(xb_i)$). Then it is well known that it is independent of the particular coordinate system used, and in case S is a free finitely generated R-module, t is the ordinary trace map [3, p. 21]. We will call this t the trace map in the case S is a finitely generated, projective R-module.

PROPOSITION 4.1. *Let S be an R-algebra.*

(a) *If S is a finitely generated, projective R-module, then $\alpha(t) = \phi \mid \mathfrak{A}$.*

(b) *If S is a separable R-algebra, then S is a finitely generated, projective R-module if and only if there is an f in* $\mathrm{Hom}_R(S, R)$ *such that* $\alpha(f) = \phi \mid \mathfrak{A}$.

(c) *If S is a separable R-algebra which is a finitely generated, projective R-module, then f in* $\mathrm{Hom}_R(S, R)$ *is t if and only if* $\alpha(f) = \phi \mid \mathfrak{A}$.

Proof. (a) Suppose $b_1, \cdots, b_n$ in S and $g_1, \cdots, g_n$ in $\mathrm{Hom}_R(S, R)$ are a projective coordinate system for S and $\sum x_j \otimes y_j$ is in $\mathfrak{A}$. Then

$$\alpha(t)(\sum x_i \otimes y_i) = \alpha(\sum_i b_i g_i)(\sum_j x_j \otimes y_j) = \sum_i b_i(\alpha(g_i)(\sum_j x_j \otimes y_j))$$
$$= \sum_{i,j} b_i g_i(x_j) y_j = \sum_j (\sum_i g_i(x_j) b_i) y_j = \sum_j x_j y_j = \phi(\sum x_j \otimes y_j).$$

(b) and (c). If S is a finitely generated projective R-module, then we know by (a) that $\alpha(t) = \phi \mid \mathfrak{A}$. So suppose S is separable, and there is an f in $\mathrm{Hom}_R(S, R)$ such that $\alpha(f) = \phi \mid \mathfrak{A}$. Since S is separable, there is an element $\sum_{i=1}^n x_i \otimes y_i$ in $\mathfrak{A}$ such that $\phi(\sum x_i \otimes y_i) = 1$. Now

$$\alpha(f)((x \otimes 1)(\sum x_i \otimes y_i)) = \alpha(f)(\sum x x_i \otimes y_i) = \sum f(x x_i) y_i .$$

However, by hypothesis $\alpha(f) = \phi \mid \mathfrak{A}$. Therefore

$$\alpha(f)((x \otimes 1)(\sum x_i \otimes y_i))$$

also equals $x \sum x_i y_i = x$. Thus we have that $x = \sum f(x x_i) y_i$. Therefore $y_1, \cdots, y_n$ and $x_1 f, \cdots, x_n f$ is a projective coordinate system for S over R, and thus S is a finitely generated projective R-module. Also by the definition of t we have

$$t(x) = \sum y_i(x_i f)(x) = \sum f(x x_i y_i) = f(\sum x x_i y_i) = f(x)$$

for all x in S. Therefore we have that $t = f$, which also proves (c).

Remark. It should be observed that Proposition 4.1 essentially gives an intrinsic characterization of the trace for separable R-algebras S which are finitely generated projective R-modules. It is therefore tempting to say that an element f in $\mathrm{Hom}_R(S, R)$ for an arbitrary R-algebra S is a trace if and only if $\alpha(f) = \phi \mid \mathfrak{A}$. Since there are separable R-algebras which are not projective, not every R-algebra has a trace in this sense. It would be interesting to know if a trace map is unique if it does exist. While what follows sheds a little light on the question, it does not settle it.

THEOREM 4.2. *Let R be a noetherian integrally closed domain with field of quotients K. Let L be a finite, separable algebraic extension of K, and S an integral extension of R in L such that $S \otimes_R K = L$. Then the trace map t of L with respect to K maps S into R and is the only element of* $\mathrm{Hom}_R(S, R)$ *such that $\alpha(t) = \phi \mid \mathfrak{A}$. From this it follows that $t(S)S$ contains $\mathfrak{H}(S/R)$.*

Proof. Since R is integrally closed, the trace maps S into R. Tensoring the exact sequence $0 \to \mathfrak{J} \to S \otimes_R S \to S \to 0$ with K (over R) we deduce the exact sequence $0 \to \mathfrak{J} \otimes_R K \to L \otimes_K L \to L \to 0$. Since S is a finitely generated R-module (because L is a finite, separable extension of K), we have that $S \otimes_R S$ is noetherian, and therefore $\mathfrak{A}$ is a finitely generated $S \otimes_R S$-module. Consequently, it follows that $\mathfrak{A} \otimes_R K$ is the annihilator of $\mathfrak{J} \otimes_R K$ in $L \otimes_K L = S \otimes_R S \otimes_R K$. Also we know that every f in $\mathrm{Hom}_R(S, R)$ has a unique extension $f_K : L \to K$. From the facts that $S \subset L$ and that the diagram

$$\begin{array}{ccc} S \otimes S & \rightarrow & L \otimes L \\ \downarrow \phi & & \downarrow \phi_K \\ S & \longrightarrow & L \end{array}$$

commutes, it follows that $\alpha(f) = \phi \mid \mathfrak{A}$ if and only if $\alpha(f_K) = \phi_K \mid \mathfrak{A} \otimes_R K$. Since the trace $t : L \to K$ is the only element of $\mathrm{Hom}_K(L, K)$ with the property that $\alpha(t) = \phi_K \mid \mathfrak{A} \otimes_R K$ (see Proposition 4.1) and $t(S) \subset R$ (because R is integrally closed), it follows that t is the only element in $\mathrm{Hom}_R(S, R)$ such that $\alpha(t) = \phi \mid \mathfrak{A}$. It is clear that the image of $\alpha(t) : S \otimes S \to S$ defined by $t(x \otimes y) = t(x)y$ is $t(S)S$. Now by definition $\mathfrak{H}(S/R)$ is $\phi(\mathfrak{A})$; therefore since $\alpha(t) | \mathfrak{A} = \phi \mid \mathfrak{A}$, we have that $t(S)S$ contains $\mathfrak{H}(S/R)$.

Bibliography

1. S. Abhyankar, *Ramification theoretic methods in algebraic geometry*, Annals of Mathematics Studies, no. 43, Princeton, Princeton University Press, 1959.
2. M. Auslander and D. A. Buchsbaum, *On ramification theory in noetherian rings*, Amer. J. Math., vol. 81 (1959), pp. 749–765.
3. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc., vol. 97 (1960), pp. 1–24.
4. ———, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc., vol. 97 (1960), pp. 367–409.
5. R. Berger, *Über verschiedene Differentenbegriffe*, S.-B. Heidelberger Akad. Wiss. Math.-Nat. Kl., 1960/61, pp. 1–44.
6. M. Nagata, *An example to a problem of Abhyankar*, Amer. J. Math., vol. 81 (1959), pp. 501–502.
7. J-P. Serre, *Algèbre locale-multiplicités*, mimeographed lecture notes by P. Gabriel, Collège de France, 1958.
8. O. Zariski and P. Samuel, *Commutative algebra*, vols. I and II, Princeton, Van Nostrand, 1958, 1960.

Brandeis University
Waltham, Massachusetts