INERTIAL SUBALGEBRAS OF ALGEBRAS OVER COMMUTATIVE RINGS[1]

BY
EDWARD C. INGRAHAM

Introduction. The classical Wedderburn Principal Theorem states that if a finite-dimensional algebra A over a field has the property that A modulo its Jacobson radical N is separable, then A contains a subalgebra S with $S+N=A$ and $S\cap N=(0)$. In [2], M. Auslander and O. Goldman developed the theory of separable algebras over an arbitrary commutative ring. This concept of separability prompts one to ask to what degree the Wedderburn Principal Theorem can be generalized to algebras over a commutative ring. This paper is concerned with the following questions which bear directly on this problem.

(1) Let A be a finitely generated R-algebra, where R is a commutative ring. Under what circumstances does A contain an R-separable subalgebra S such that $S+N=A$? We call such a subalgebra an *inertial subalgebra* of A.

(2) Which commutative rings R have the property that every finitely generated R-algebra A such that $A/\mathrm{rad}(A)$ is separable over R contains an inertial subalgebra? We call such a commutative ring an *inertial coefficient ring.*

We say that the uniqueness statement holds for an inertial coefficient ring R if, whenever S and S' are inertial subalgebras of a finitely generated R-algebra A, there exists an element n in the radical of A such that $(1-n)S(1-n)^{-1}=S'$. In this setting the Wedderburn Principal Theorem along with Malcev's uniqueness assertion state that every field is an inertial coefficient ring for which the uniqueness statement holds.

§1 contains preliminaries. In §2, we first investigate some properties of inertial subalgebras. Then necessary and sufficient conditions are obtained for the existence of an inertial subalgebra in a finitely generated, faithful, commutative R-algebra A having a finite group G of automorphisms such that $A^G=\{a\in A\mid \sigma(a)=a,\forall\sigma\in G\}=R$, where R is a commutative ring containing no idempotents but 0 and 1. §3 is devoted to the second of the above questions, beginning with a discussion of some formal properties of inertial coefficient rings. Azumaya has proved in [3] that every Hensel ring is an inertial coefficient ring for which the uniqueness statement holds. We give the following partial

Presented to the Society, June 19, 1965 under the title *On the existence of inertial subalgebras*; received by the editors June 29, 1965.

[1] This paper consists of my doctoral thesis written at the University of Oregon. I am deeply indepted to Professors Charles W. Curtis and David K. Harrison for their guidance in its preparation. Thanks are also due the referee for a number of helpful suggestions.

converse: Let R be a noetherian, semilocal ring such that either (i) all residue class fields of R are perfect, or (ii) R is an integrally closed integral domain. Then, if R is an inertial coefficient ring, R is a finite direct sum of Hensel rings. Finally, it is proved that a Dedekind domain R is an inertial coefficient ring for which the uniqueness statement holds if and only if either R has zero radical or R is a Hensel ring.

1. **Preliminaries.** All rings, unless specifically stated, are assumed to have an identity and subrings are assumed to contain this identity. Also, all ring homomorphisms carry the identity onto the identity. Throughout this paper R denotes a commutative ring and A denotes an R-algebra; that is, A is a ring along with a ring homomorphism θ of R into the center of A. The image of R under θ is denoted by $R \cdot 1$ (or simply by R when θ is a monomorphism). N always denotes the Jacobson radical of A. By a *finitely generated* or *projective* R-algebra, we mean an algebra which is finitely generated or projective as an R-module. Finally, a *connected ring* is a commutative ring containing no idempotents other than 0 and 1.

An enormously useful result which we will employ repeatedly is the so-called Generalized Nakayama Lemma [13, Lemma 2, p. 215]:

($*$) If R is a commutative ring and U is a finitely generated R-module, an ideal $\mathfrak{a}$ of R has the property that $\mathfrak{a} \cdot U = U$ if and only if $\mathrm{annih}_R(U) + \mathfrak{a} = R$, where $\mathrm{annih}_R(U) = \{r \in R \mid r \cdot U = (0)\}$.

An R-algebra A is called *separable* over R (or R-separable) [2, p. 369] if A is projective over its enveloping algebra $A \otimes_R A^0$. When R is a field, this definition is equivalent to finite dimensionality and separability in the classical sense. If $\mathfrak{a}$ is an ideal of R such that $\mathfrak{a} \subseteq \operatorname{kernel} \theta$, that is, $\mathfrak{a} \cdot 1 = (0)$, then A is naturally an $R/\mathfrak{a}$-algebra and the definition of the tensor product implies that A is separable as an R-algebra if and only if A is separable as an $R/\mathfrak{a}$-algebra. We shall make this shift of coefficient rings frequently without further comment.

The following lemma relates the radical of an R-algebra to the radical and maximal ideals of R.

LEMMA 1.1. *Let A be a finitely generated R-algebra and let $\bigcap(\mathfrak{m}A)$ denote the intersection of the $\mathfrak{m}A$ as $\mathfrak{m}$ runs over all maximal ideals of R.*

(a) $\mathrm{rad}(R) \cdot A \subseteq N$.

(b) *There exists a positive integer n such that $N^n \subseteq \bigcap(\mathfrak{m}A)$.*

(c) *If A is projective,* $\mathrm{rad}(R) \cdot A = \bigcap(\mathfrak{m}A)$.

(d) *If A is separable,* $N = \bigcap(\mathfrak{m}A)$.

Proof. (a) Obviously $\mathrm{rad}(R) \cdot A \subseteq \bigcap(\mathfrak{m}A)$. Suppose $\bigcap(\mathfrak{m}A) \nsubseteq N$. Then there exists a maximal left ideal M of A with $\mathfrak{m}A + M = A$, or, equivalently, $\mathfrak{m}(A/M) = A/M$, for every maximal ideal $\mathfrak{m}$ of R. It follows from ($*$) that $M = A$, a contradiction.

(b) Suppose A is generated as an R-module by $\leqq n$ elements. Then, for any maximal ideal $\mathfrak{m}$ of R, $A/\mathfrak{m}A$ is an algebra of dimension $\leqq n$ over the field $R/\mathfrak{m}$. Hence $[\operatorname{rad}(A/\mathfrak{m}A)]^n = (0)$. Because $(N + \mathfrak{m}A)/\mathfrak{m}A \subseteq \operatorname{rad}(A/\mathfrak{m}A)$, it follows that $N^n \subseteq \mathfrak{m}A$. Since n is independent of $\mathfrak{m}$, we conclude that $N^n \subseteq \bigcap(\mathfrak{m}A)$.

(c) If A is R-free, it is clear that $\operatorname{rad}(R)\cdot A = \bigcap(\mathfrak{m}A)$. The assertion now follows for projective modules from the fact that every projective is a direct summand of a free.

(d) Every ring homomorphic image of a separable algebra is separable [2, Proposition 1.4, p. 370]. Hence $A/\mathfrak{m}A$ is $R/\mathfrak{m}$-separable for every maximal ideal $\mathfrak{m}$ of R. Since separability over a field implies Jacobson semisimplicity, we have $N \subseteq \mathfrak{m}A$ for every maximal ideal, whence $N \subseteq \bigcap(\mathfrak{m}A)$. The opposite inclusion was established in the proof of (a).

We conclude this section with the following well-known property of separable algebras.

Lemma 1.2. *If A is a separable R-algebra, every A-module which is R-projective is A-projective.*

Proof. A separable over R implies that the map from $A \otimes_R A^0$ to A defined by $a \otimes a' \to aa'$ splits over $A \otimes_R A^0$. Hence there exists $\sum x_i \otimes y_i \in A \otimes_R A^0$ with $\sum x_i y_i = 1$ and $\sum ax_i \otimes y_i = \sum x_i \otimes y_i a$, for every $a \in A$. For any (left) A-modules P and M, $\operatorname{Hom}_R(P,M)$ can be considered an $A \otimes_R A^0$-module by $[(a \otimes a')\cdot f](p) = a \cdot f(a' \cdot p)$, where $f \in \operatorname{Hom}_R(P,M)$ and $p \in P$. It follows that we have a map from $\operatorname{Hom}_R(P,M)$ to $\operatorname{Hom}_A(P,M)$ defined by $f \to (\sum x_i \otimes y_i)\cdot f$. The lemma now results from consideration of the universal mapping property of projective modules.

2. Inertial subalgebras.

Definition 2.1. Let A be a finitely generated R-algebra with radical N. A subalgebra S of A is called an *inertial subalgebra* if S is a separable R-algebra such that $S + N = A$.

Remark 2.2. The radical of any inertial subalgebra S of A is equal to $S \cap N$, since $A/N \cong (S + N)/N \cong S/(S \cap N)$ is Jacobson semisimple, implying that $S \cap N \supseteq \operatorname{rad}(S)$, whereas the opposite inclusion follows from the corollary on p. 126 of [3]. Also, since S separable implies $S/(S \cap N)$ is separable, we see that the existence of an inertial subalgebra forces A/N to be R-separable.

Before investigating the existence of inertial subalgebras, we give a few results on their nature when they exist.

Lemma 2.3. *Let A be a finitely generated R-algebra such that A/N is R-projective. Then, if S is an inertial subalgebra of A, $S \cap N = (0)$, so $S \oplus N = A$ as R-modules.*

Proof. Since $S/(S \cap N) \cong A/N$, $S/(S \cap N)$ is R-projective. By Lemma 1.2,

$S/(S \cap N)$ is S-projective, so there exists a left ideal T of S with $S = (S \cap N) \oplus T$. Therefore $S \cap N$ is generated by an idempotent which must be 0 since 0 is the only idempotent in N.

REMARK 2.4. Lemma 2.3 allows us to conclude that any inertial subalgebra of an algebra over a field is isomorphic to the algebra modulo its radical.

LEMMA 2.5. *Suppose $S' \subseteq S$ are two inertial subalgebras of a finitely generated R-algebra A and suppose that S is finitely generated over R. Then $S' = S$.*

Proof. One observes that S' is an inertial subalgebra of S. By Lemma 1.1(d), $\mathrm{rad}(S) = \bigcap(\mathfrak{m}S)$, whence $S' + \mathfrak{m}S = S$ for every maximal ideal $\mathfrak{m}$ of R. Therefore $S' = S$ by $(*)$.

PROPOSITION 2.6. *Let A be a commutative, finitely generated R-algebra. Suppose S and S' are finitely generated inertial subalgebras of A. Then $S = S'$.*

Proof. Since $S \cdot S'$ is a ring homomorphic image of $S \otimes_R S'$ and the tensor product of two separable algebras is separable, $S \cdot S'$ is R-separable. [2, Propositions 1.4 and 1.5, pp. 370–371.] Hence $S \cdot S'$ is a finitely generated inertial subalgebra containing both S and S', so, by Lemma 2.5, $S = S \cdot S' = S'$.

COROLLARY 2.7. *Inertial subalgebras of finitely generated, commutative algebras over noetherian rings are unique.*

PROPOSITION 2.8. *Let A be a finitely generated, projective, commutative R-algebra. Then any separable subalgebra S of A is an S-direct summand of A and is therefore finitely generated and projective over R. In particular, if S is an inertial subalgebra, S is finitely generated, projective, and unique.*

Proof. Since every S-module which is R-projective is S-projective by Lemma 1.2, A is a finitely generated, projective, and faithful S-algebra. Hence S is an S-direct summand of A [4, Exercise 4, p. 176]. If S is an inertial subalgebra, uniqueness follows from Proposition 2.6.

We now turn to the question of the existence of inertial subalgebras in commutative algebras of a fairly general type. The setting is this: A is a commutative, faithful R-algebra possessing a finite group G of automorphisms with $A^G = R$, where $A^G = \{a \in A \mid \sigma(a) = a, \ \forall \sigma \in G\}$. We call A a *(G,R)-algebra.* We remark that if, in addition, A is R-separable, A is called a *Galois extension* of R [7, p. 20]. Such extensions have been thoroughly treated in [7]. However, our concern is with the case that A is not necessarily separable. The first corollary to our first theorem gives necessary and sufficient conditions for the existence of an inertial subalgebra in a connected, finitely generated (G,R)-algebra A.

Let $\mathfrak{m}$ be any maximal ideal of R and let M be any maximal ideal of A lying over $\mathfrak{m}$, i.e. $M \cap R = \mathfrak{m}$. We set

$$D_M = \{\sigma \in G \,|\, \sigma(M) = M\} \text{ (the decomposition group of } M\text{), and}$$

$$T_M = \{\sigma \in G \,|\, \sigma(a) - a \in M,\ \forall a \in A\} \text{ (the inertia group of } M\text{).}$$

It is easily checked that T_M is a normal subgroup of D_M. It is also clear that A/M can be considered as a field extension of $R/\mathfrak{m}$ on which D_M/T_M acts as a faithful group of $R/\mathfrak{m}$-automorphisms in a natural way.

The proof of the following lemma can be found in [5, p. 42].

Lemma 2.9. *Let A be a (G,R)-algebra.*

(a) *For any two maximal ideals M, M' of A lying over the same maximal ideal $\mathfrak{m}$ of R, there exists an element σ of G with $\sigma(M) = M'$.*

(b) *If M is a maximal ideal of A lying over $\mathfrak{m}$ in R, A/M is a normal algebraic field extension of $R/\mathfrak{m}$ whose full group of automorphisms is canonically isomorphic to D_M/T_M.*

We can now tackle

Theorem 2.10. *Let A be a finitely generated, connected (G,R)-algebra.*

(a) *If we denote by U the smallest subgroup of G containing T_M, for every maximal ideal M of A, then $S_* = A^U$ is Galois over R with group G/U. Moreover, if S is any R-separable subalgebra of $A, S \subseteq S_*$.*

(b) *Suppose A/N is R-separable. If we denote the intersection of all the T_M by I, then $S^* = A^I$ has the property that $S^* + N = A$. Moreover, if S is any subalgebra of A such that $S + N = A$, then, setting $T = \{\sigma \in G \,|\, \sigma(s) = s,\ \forall s \in S\}$, we have $T \subseteq I$.*

Proof. (a) For any maximal ideal M of A, let $g_R(M)$ (resp. $g_{S_*}(M)$, $g_R(S_* \cap M)$) denote the number of maximal ideals of A (resp. A, S_*) lying over $R \cap M$ (resp. $S_* \cap M, R \cap M$). By Lemma 2.9(a), $g_R(M) = [G\colon D_M]$, and by Lemma 2.9(b), $[D_M\colon T_M] = [A/M\colon R/(R \cap M)]_s =$ separable degree of A/M over $R/(R \cap M)$. Hence $|G| = [G\colon D_M] \cdot [D_M\colon T_M] \cdot |T_M| = g_R(M) \cdot [A/M\colon R/(R \cap M)]_s \cdot |T_M|$. Considering A as a (U,S_*)-algebra and noting that $\{\sigma \in U \,|\, \sigma(a) - a \in M, \forall a \in A\} = T_M$ since $T_M \subseteq U$, we have in a similar fashion that $|U| = g_{S_*}(M) \cdot [A/M\colon S_*/(S_* \cap M)]_s \cdot |T_M|$. But $g_R(M) = g_{S_*}(M) \cdot g_R(S_* \cap M)$ and $[A/M\colon R/(R \cap M)]_s = [A/M\colon S_*/(S_* \cap M)]_s \cdot [S_*/S_* \cap M)\colon R/(R \cap M)]_s$, so

$$\text{(I)} \qquad [G\colon U] = g_R(S_* \cap M) \cdot [S_*/(S_* \cap M)\colon R/(R \cap M)]_s.$$

It is easily seen that U is a normal subgroup of G, so we may apply Lemma 2.9 to the $(G/U,R)$-algebra S_* to obtain

$$\text{(II)} \quad |G/U| = [G\colon U] = g_R(S_* \cap M) \cdot [S_*/(S_* \cap M)\colon R/(R \cap M)]_s \cdot |T'_M|$$

where $T'_M = \{\sigma U \in G/U \,|\, \sigma(s) - s \in S_* \cap M, \forall s \in S_*\}$. It follows from (I) and (II) that $|T_M| = 1$, so by Theorem 1.3, p. 18 of [7], S_* is Galois over R with group G/U.

Now suppose S is any R-separable subalgebra of A. For every $\sigma \in G$, $\sigma(S)$ is an R-separable subalgebra. As in the proof of Proposition 2.6, we see that the product S' of all the images of S under G is an R-separable subalgebra. Moreover S' is normal in the sense that $\sigma(S') = S'$ for every $\sigma \in G$, whence $T' = \{\sigma \in G \mid \sigma(s) = s, \forall s \in S'\}$ is normal in G. Therefore S' is Galois over R with group G/T', so by Theorem 1.3 of [7], $\{\sigma \in G \mid \sigma(s) - s \in P, \forall s \in S'\} = T'$, for every maximal ideal P of S'. Setting $T = \{\sigma \in G \mid \sigma(s) = s, \forall s \in S\}$, we have $T \supseteq T' \supseteq U$, so $S \subseteq S_*$. This concludes the proof of (a).

(b) Assume A/N is R-separable. Consider the (I, S^*)-algebra A. For any maximal ideal M of A, define $D''_M = \{\sigma \in I \mid \sigma(M) = M\}$ and $T''_M = \{\sigma \in I \mid \sigma(a) - a \in M, \forall a \in A\}$. It follows from Lemma 2.9(b) that D''_M/T''_M is the full group of automorphisms of A/M over $S^*/(S^* \cap M)$. But, by definition of I, $D''_M = T''_M = I$. Moreover, A/N separable over R implies A/M is separable over $S^*/S^* \cap M)$. Therefore A/M is a Galois extension of $S^*/(S^* \cap M)$ whose Galois group is the identity, so $S^*/(S^* \cap M) = A/M$ under the natural map, or equivalently,

(III) $\qquad S^* + M = A$ for every maximal ideal M of A.

It follows immediately from Lemma 2.9(a) and the fact that $I \subseteq D_M$ that

(IV) $\qquad M$ is the only maximal ideal of A lying over $S^* \cap M$.

We now show that $S^* + N = A$. By $(*)$, it suffices to show that, for every maximal ideal $\mathfrak{m}$ of R, $S^* + N + \mathfrak{m}A = A$. Let $J_{\mathfrak{m}}$ denote the intersection of the maximal ideals of A lying over $\mathfrak{m}$. $A/\mathfrak{m}A$ is an algebra over $R/\mathfrak{m}$ whose radical is $J_{\mathfrak{m}}/\mathfrak{m}A$. Since $A/(\mathfrak{m}A + N)$ is a homomorphic image of A/N, $A/(\mathfrak{m}A + N)$ is $R/\mathfrak{m}$-separable, so it is Jacobson semisimple. Therefore $\mathfrak{m}A + N \supseteq J_{\mathfrak{m}}$. The opposite inclusion clearly obtains, so

(V) $$\mathfrak{m}A + N = J_{\mathfrak{m}}.$$

It is apparent that $J_{\mathfrak{m}}$ is the intersection of a finite number of maximal ideals of A, call them $M_1, \cdots, M_n$. Therefore, by (III) and (IV), we have

$$S^*/(S^* \cap J_{\mathfrak{m}}) \cong S^*/(S^* \cap M_1) \oplus \cdots \oplus S^*/(S^* \cap M_n) \cong A/M_1 \oplus \cdots \oplus A/M_n \cong A/J_{\mathfrak{m}},$$

so $S^* + J_{\mathfrak{m}} = A$. It now follows from (V) that $S^* + N + \mathfrak{m}A = A$. This proves that $S_* + N = A$.

Finally suppose S is an R-subalgebra with $S + N = A$. Then every $a \in A$ is expressible as $a = s + n$ for some $s \in S$, $n \in N$. Setting $T = \{\sigma \in G \mid \sigma(s) = s, \forall s \in S\}$, we have $\sigma(a) - a = \sigma(n) - n \in N$, for every $\sigma \in T$. Hence $T \subseteq I$ and the theorem is proved.

Corollary 2.11. *Let A be a finitely generated, connected (G,R)-algebra. Then the following are equivalent*:

(a) *A contains an inertial subalgebra S.*

(b) *A/N is R-separable and $T_M = T_{M'}$ for any two maximal ideals M and M' of A.*

If (a) *and* (b) *hold, denoting the common inertia group by T, we have $S = A^T$ and S is a Galois extension of R with group G/T. Hence S is finitely generated, projective, and is the unique inertial subalgebra of A.*

Proof. Clearly if S is an inertial subalgebra of A and $T = \{\sigma \in G \mid \sigma(s) = s, \forall s \in S\}$, the theorem yields $T \subseteq I \subseteq U \subseteq T$, so $T_M = T_{M'}$ for every two maximal ideals M and M' of A. Since the existence of an inertial subalgebra in general implies that A/N is separable, we have proved that (a) implies (b).

It follows immediately from the theorem that if A/N is separable and $T_M = T_{M'}$ for every M, M', $S_* = S^* = A^T$ is an inertial subalgebra.

Finally Theorem 2.10(a) combined with Lemma 2.5 shows uniqueness of inertial subalgebras. That $S = A^T$ is finitely generated and projective follows from the properties of a Galois extension [7, Theorem 1.3, p. 18].

Corollary 2.12. *Let A be a connected (G,R)-algebra. There exists a one-one correspondence (the usual) between the R-separable subalgebras of A and the subgroups of G containing U.*

Proof. Careful examination of the proof of Theorem 2.10(a) reveals that the hypothesis that A be finitely generated over R is not necessary. The corollary now follows from the Fundamental Theorem of Galois Theory [7, Theorem 2.3, p. 24].

Remark 2.13. We note for later use that in Corollary 2.11 (a) implies (b) under the slightly more general assumption that $A^G \supseteq R$. For if S is an R-inertial subalgebra, $A^G \cdot S$ is an A^G-inertial subalgebra [2, Propositions 1.4 and 1.5, pp. 370–371]. Then applying the theorem to A considered as a (G, A_G)-algebra, we see that $T_M = T_{M'}$ for any two maximal ideals M and M' of A.

Next we generalize Corollary 2.11 by assuming only that R, rather than A, is connected. We decompose A into an ideal direct sum of rings, each connected, and then apply Corollary 2.11 to each of these summands. The key to the decomposition is the following lemma.

Notation: For any idempotent e of A, set $H_e = \{\sigma \in G \mid \sigma(e) = e\}$.

Lemma 2.14. *Let A be a finitely generated (G,R)-algebra with R connected. Then A contains a primitive idempotent.*

Proof. For any maximal ideal $\mathfrak{m}$ of R, $A/\mathfrak{m}A$ contains only a finite number of idempotents because it is a finite-dimensional algebra over a field. Hence there exists an idempotent e in A such that for any idempotent e' of A with $ee' = e'$, either $\bar{e}' = \bar{O}$ or $\bar{e}' = \bar{e}$ in $A/\mathfrak{m}A$. To prove that e is primitive, it suffices therefore to show that 0 is the only idempotent in $\mathfrak{m}A$.

Suppose f' is a nonzero idempotent of $\mathfrak{m}A$. By $(*)$, $\mathfrak{m}A \neq A$, so f' is not a unit. It follows that $\prod_{\sigma \in G}\sigma(f')$, being an idempotent in R, equals 0. Let n be the largest integer such that there exist n distinct elements $\sigma_1, \cdots, \sigma_n$ in G with $\prod_{i=1}^{n}\sigma_i(f') \neq 0$. Call this latter product f. By the choice of n, f is a nonzero idempotent in $\mathfrak{m}A$ such that the distinct images of f under G are pairwise orthogonal. Hence, writing $G = \pi_1 H_f \cup \pi_2 H_f \cup \cdots \cup \pi_m H_f$ (disjoint with π_1 equal to the identity of G), we have $\sum_{i=1}^{m}\pi_i(f)$ is a nonzero idempotent of R and hence equals 1. But, since $\mathfrak{m}A$ is invariant (as a set) under G, $f \in \mathfrak{m}A$ implies $\sum \pi_i(f) = 1 \in \mathfrak{m}A$, a contradiction.

Theorem 2.15. *Let A be a finitely generated (G,R)-algebra with R connected. Then the following are equivalent*:

(a) *A contains an inertial subalgebra S.*

(b) *A/N is R-separable and $T_M = T_{M'}$ whenever M and M' are maximal ideals of A excluding the same primitive idempotent.*

In the event that (a) *and* (b) *hold, denoting the common inertia group of the maximal ideals of A not containing the primitive idempotent e by T_e, we have* that $(Ae)^{T_e}$ *is a Galois extension of Re with group H_e/T_e, and $S = \oplus \sum (Ae)^{T_e}$, where the summation runs over the primitive idempotents e of A. Finally, S is finitely generated, projective, and unique.*

Proof. Let e be any primitive idempotent of A, the existence of which is guaranteed by the preceding lemma. Writing $G = \sigma_1 H_e \cup \cdots \cup \sigma_n H_e$ (disjoint with σ_1 equal to the identity of G), we see that each $\sigma_i(e)$ is a primitive idempotent, $\sum_{i=1}^{n}\sigma_i(e) = 1$, and, if e' is a primitive idempotent, $e' = \sigma_i(e)$ for some i. Hence A is the direct sum of the ideals generated by its primitive idempotents.

We now consider the finitely generated, commutative, faithful Re-algebra Ae. Clearly Ae is connected. Moreover, H_e is a finite group of Re-automorphisms of Ae. Suppose $ae \in (Ae)^{H_e}$. Since $\sigma_i(e)e = 0$ for $i \neq 1$, $\sum_{i=1}^{n}\sigma_i(ae)e = \sum_{i=1}^{n}\sigma_i(a)\sigma_i(e)e = ae$. But $\sum_{i=1}^{n}\sigma_i(ae) \in R$, so $ae \in Re$. Therefore $(Ae)^{H_e} = Re$, so Ae is a finitely generated, connected (H_e, Re)-algebra.

Let M be a maximal ideal of A. Since M is a prime ideal and the product of any two distinct primitive idempotents is 0, we see that M contains all but one of the primitive idempotents. Therefore the maximal ideals of Ae are of the form Me where M is a maximal ideal of A not containing e. In this situation, set $T_{Me} = \{\sigma \in H_e \mid \sigma(ae) - ae \in Me, \forall a \in A\}$. For any $\sigma \in T_M$, we have $\sigma(e) - e \in M$, so both e and $\sigma(e)$ are primitive idempotents lying outside M. Therefore $\sigma(e) = e$ and $T_M \subseteq T_{Me}$. Conversely, $\sigma \in T_{Me}$ implies $\sigma(ae) - ae = (\sigma(a) - a)e \in Me, \forall a \in A$. Therefore, since M is prime and $e \notin M$, $\sigma(a) - a \in M$, $\forall a \in A$, so $\sigma \in T_M$. We have established that, for every primitive idempotent e and every maximal ideal M of A excluding e,

$$\text{(VI)} \qquad T_M = T_{Me}.$$

Proof that (a) implies (b). Suppose S is an inertial subalgebra of A. Then, since $Ne = \mathrm{rad}(Ae)$ and Se is separable over Re, Se is an Re-inertial subalgebra of Ae. Applying (VI) and Corollary 2.11 to Ae, we have that $T_M = T_{Me} = T_{M'e} = T_{M'}$ for any two maximal ideals M and M' of A not containing e. As usual, the existence of S implies A/N is separable.

(b) implies (a). Corollary 2.11 implies that Ae contains a unique Re-inertial subalgebra $(Ae)^{T_e}$which is Galois over Re with group H_e/T_e. Hence $(Ae)^{T_e}$is separable, projective, and finitely generated over Re. But, since the sum of the distinct images of e under G is 1, $re = 0$ only if $r = 0$, for every $r \in R$. Therefore, R is isomorphic to Re, whence each $(Ae)^{T_e}$ is separable, projective and finitely generated over R. It follows that $S = \oplus \sum (Ae)^{T_e}$ is an inertial subalgebra of A which is finitely generated and projective.

Finally let S' be any other inertial subalgebra. By the uniqueness assertion of Corollary 2.11, $S'e = Se = (Ae)^{T_e}$ for every primitive idempotent e, from which it follows that $S' \subseteq S$. Since S is finitely generated over R, we conclude from Lemma 2.5 that $S' = S$.

3. **Inertial coefficient rings.**

Definition 3.1. A commutative ring R is called an *inertial coefficient ring* (or *IC-ring*) if every finitely generated R-algebra A such that A/N is R-separable contains an inertial subalgebra. We say that the *uniqueness statement holds* for R if, for any two inertial subalgebras S and S' of a finitely generated R-algebra A, there exists an element n in N such that $(1-n)S(1-n)^{-1} = S'$.

We begin by giving some formal properties of inertial coefficient rings.

Proposition 3.2. *If R_1 and R_2 are IC-rings, then $R = R_1 \oplus R_2$ is an IC-ring. The uniqueness statement holds for R if it holds for both R_1 and R_2.*

Proof. Any R-algebra A is naturally the direct sum of an R_1-algebra A_1 and an R_2-algebra A_2. The direct sum of an inertial subalgebra of A_1 with an inertial subalgebra of A_2 is clearly an inertial subalgebra of A. The proposition now follows in an obvious manner.

Proposition 3.3. *If R is an IC-ring, then any separable, finitely generated, commutative R-algebra R' is an IC-ring. If the uniqueness statement holds for R, it holds for R'.*

Proof. Let A be a finitely generated R'-algebra with A/N separable over R'. We must show that A contains an R'-inertial subalgebra. Clearly A is a finitely generated R-algebra in a natural way. By the proof of Theorem 2.3, p. 374 of [2], separability is transitive, so A/N is R-separable. Therefore, since R is an IC-ring, A contains an R-inertial sublagebra S. But $R' \cdot 1$ is contained in the center of A, so $R' \cdot S$ is a ring homomorphic image of $R' \otimes_R S$. Hence $R' \cdot S$ is R'-separable [2, Propositions 1.4 and 1.5, pp. 370–371], and is therefore an R'-inertial subalgebra. Again using the transitivity of separability, we see that any R'-inertial subalgebra is an R-inertial subalgebra. Hence, if the uniqueness statement holds for R, it holds for R'.

Corollary 3.4. *If R is an IC-ring and R' is a ring homomorphic image of R, then R' is an IC-ring. Moreover, if the uniqueness statement holds for R, it holds for R'.*

Let R be a (not necessarily noetherian) local ring with maximal ideal $\mathfrak{m}$. For $f \in R[x]$, denote by $\bar{f}$ that element of $(R/\mathfrak{m})[x]$ obtained by replacing the coefficients of f by their residues modulo $\mathfrak{m}$. A local ring is called a *Hensel ring* [12, p. 103] if, for every monic polynomial $f \in R[x]$ such that $\bar{f} = g_0 h_0$ in $(R/\mathfrak{m})[x]$, where g_0 and h_0 are monic and relatively prime, there exist monic polynomials g and h in $R[x]$ with $f = gh$, $\bar{g} = g_0$ and $\bar{h} = h_0$. In 1951 G. Azumaya proved in [3] that every Hensel ring is an IC-ring for which the uniqueness statement holds.

Remark 3.5. It is well known that every (noetherian) complete semilocal ring is a finite direct sum of complete local rings [14, Corollary 2, p. 283] and that every complete local ring is a Hensel ring [12, (30.3), p. 104]. Hence, by Proposition 3.2 and Azumaya's result, every complete semilocal ring is an IC-ring for which the uniqueness statement holds. In particular, every finite commutative ring is such a ring.

We now set out to prove that certain commutative rings are IC-rings only if they are Hensel rings.

Theorem 3.6. *Let R be a noetherian, connected, semilocal ring. Then, if R is an IC-ring, R is local.*

Proof. The proof is by contradiction. Under the assumption that R contains more than one maximal ideal, we construct a finitely generated, connected (G, A^G)-algebra A having the property that A/N is separable but containing two maximal ideals whose inertia groups differ. Applying Corollary 2.11, we can then assert that A contains no inertial subalgebra, so R is not an IC-ring.

In order to construct the required extensions, we need the following lemmas.

Lemma 3.7. *Let R be a connected, noetherian ring. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals of R such that $\mathfrak{a} \nsubseteq \mathfrak{b}$. Let n be any positive integer. Then there exists an element α in R such that α is not a unit of $R, \alpha \notin \mathfrak{b}$, and $r \neq \alpha$ for every $r \in R$. Moreover, if $\mathfrak{a}$ is an intersection of prime ideals, α can be chosen in $\mathfrak{a}$.*

Proof. Since $\mathfrak{a} \nsubseteq \mathfrak{b}$, there exists $a_1 \in \mathfrak{a}$ with $a_1 \notin \mathfrak{b}$. Supposing the conclusion of the lemma false, we can construct a sequence $\{a_i\}$ such that $a_i^n = a_{i-1}, i = 2, 3, \cdots$. Then letting (a_i) denote the principal ideal generated by a_i, we have $(a_1) \subseteq (a_2) \subseteq \cdots$ so there exists an integer i such that $(a_i) = (a_{i-1}) = (a_i) = (a_i)^n$. But by (*) and the fact that R is connected, we have that $(a_i)^2 \neq (a_i)$ unless $(a_i) = (0)$ or $(a_i) = R$. This contradicts the choice of a_i. Finally, it is clear that if $\mathfrak{a}$ is an intersection of prime ideals, $a_i \in \mathfrak{a}$.

LEMMA 3.8 (G. J. JANUSZ). *Let R be a connected ring. Let $A = R[x]/(f(x))$ where $f(x)$ is a monic polynomial containing no roots in R. Then A contains no rank* 1 *idempotents; that is, there exists no idempotent $e \in A$ such that Ae is rank one projective over R.*

Proof. Suppose Ae is projective of rank 1 over R for some idempotent e. Since R is connected, we have by (*) and [1, Theorem A.2(d), p. 21] that Ae is faithful over R, whence $Ae = Re$. Therefore, if we denote the image of x in A by $\bar{x}$, $\bar{x}e = re$ for some $r \in R$. It follows that $0 = f(\bar{x})e = f(r)e$, so $f(r) = 0$. This contradicts the assumption that R contains no root of $f(x)$.

COROLLARY 3.9. *In Lemma* 3.8 *if $f(x)$ is of degree $\leqq 3$, A is connected.*

LEMMA 3.10. *Let R be a connected noetherian ring such that* $2 = 1 + 1 \in \mathrm{rad}(R)$. *Then there exists a separable, finitely generated, commutative R-algebra R' containing a primitive cube root γ of* 1. *Moreover, R' can be chosen to be connected. Finally $1 - \gamma$ is a unit in R'.*

Proof. We shall show that γ can be taken to be a root of $x^2 + x + 1$ in R'. Assuming this, we see that $(1 - \gamma)\gamma = 2\gamma + 1$ is a unit in R', since $2 \in \mathrm{rad}(R')$ by Lemma 1.1(a). Hence $1 - \gamma$ is a unit. It is now clear that if R contains a root of $x^2 + x + 1$, we can take $R = R'$.

Assume therefore that $x^2 + x + 1$ does not have a root in R. Set

$$R' = \frac{R[x]}{(x^2 + x + 1)}.$$

By Corollary 3.9, R' is connected. Clearly R' is finitely generated over R. Furthermore, R' is a homomorphic image of $R[x]/(x^3 - 1)$ which is the group ring of the cyclic group of order 3 over R. But 3 is a unit since $2 \in \mathrm{rad}(R)$, so it follows from Theorem 4.7, p. 379 of [2] and Maschke's Theorem that this group ring and hence R' are R-separable. This completes the proof of the lemma.

We now prove the theorem. We treat two cases: (1) $2 \notin \mathrm{rad}(R)$; (2) $2 \in \mathrm{rad}(R)$.

Case 1. $2 \notin \mathrm{rad}(R)$. Let $\mathfrak{m}$ be a maximal ideal of R with $2 \notin \mathfrak{m}$. Suppose R contains another maximal ideal $\mathfrak{m}' \neq \mathfrak{m}$. Let $\mathfrak{a}$ be the intersection of all the maximal ideals of R not equal to $\mathfrak{m}$. Since R is semilocal, $\mathfrak{a} \nsubseteq \mathfrak{m}$, so by Lemma 3.7, there exists $\alpha \in \mathfrak{a}$ such that $\alpha \notin \mathfrak{m}$ and $r^2 \neq \alpha$, for every $r \in R$. Set $A = R[x]/(x^2 - \alpha)$. By Corollary 3.9, A is connected. Letting $M_1,\cdots,M_n$ be the maximal ideals of A, we have $A/N \cong A/M_1 \oplus \cdots \oplus A/M_n$, where A/M_i is a field extension of degree 1 or 2 over $R/(R \cap M_i)$, $i = 1,\cdots,n$. We observe that, by the choice of α, either the characteristic of $R/(R \cap M_i)$ is not equal to 2 or A/M_i is isomorphic to $R/(R \cap M_i)$. In either case, A/M_i is separable over $R/(R \cap M_i)$, $i = 1, \cdots, n$, so A/N is separable over R.

By the choice of α, we can view A as the free R-module $R \cdot u \oplus R \cdot 1$ where $u^2 = \alpha$. One can check that $\sigma : (ru + s) \to (-ru + s)$ is an automorphism of A of order 2. If we let G denote the group of automorphisms made up of σ and the identity, we have $A^G \supseteq R$. Now let M (resp. M') be a maximal ideal of A lying over $\mathfrak{m}$ (resp. $\mathfrak{m}'$). Clearly $u^2 = \alpha \in \mathfrak{m}'$ implies $u \in M'$ implies $-2ru \in M'$ for every $r \in R$, so, letting $a = ru + s$ be a general element of A, we have $\sigma(a) - a = -2ru \in M'$. Hence $T_{M'} = G$. On the other hand, $u^2 = \alpha \notin \mathfrak{m}$ means $u \notin M$, so $2u \notin M$ since $2 \notin \mathfrak{m}$. Therefore $\sigma(u) - u \notin M$, whence $T_M \neq G$. Taking Remark 2.13 into account, we can apply Corollary 2.11 to conclude that, under the assumption of Case 1, A contains no inertial subalgebra, so R is not an IC-ring.

Case 2. $2 \in \operatorname{rad}(R)$. By Lemma 3.10 and Proposition 3.3, we can assume that R contains a root γ of $x^2 + x + 1$. As in Case 1, we suppose that R contains at least two distinct maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$. By Lemma 3.7, there exists $\alpha \in \mathfrak{m}'$ with $\alpha \notin \mathfrak{m}$ and $r^3 \neq \alpha$, for every $r \in R$. Set $A = R[x]/(x^3 - \alpha)$. As above, A is connected. We can identify A with the free R-module $R \cdot u^2 \oplus R \cdot u \oplus R \cdot 1$ with $u^3 = \alpha$. One checks that the map σ from A to A induced by $u \to \gamma u$ is an automorphism which generates a group G of order 3. Clearly $A^G \supseteq R$.

We need to show that A/N is separable. It is not difficult to see that, for any maximal ideal M of A, $A/(R \cap M)A$ is isomorphic to $R/(R \cap M)$, to $R/(R \cap M) \oplus R/(R \cap M) \oplus R/(R \cap M)$, or to a 3-dimensional field extension of $R \cap M$ according as $x^3 - \bar{\alpha}$ equals x^3, is the product of 3 distinct linear factors, or is irreducible, where $x^3 - \bar{\alpha}$ is the image of $x^3 - \alpha$ in $(R/(R \cap M))[x]$. (Since $R/(R \cap M)$ contains a primitive cube root of 1, these are the only possibilities.) In each case, A/M is separable over $R/(R \cap M)$, so A/N is separable over R.

Again as in Case 1, we need only to find two unequal inertia groups to prove that R is not an IC-ring. Let M (resp. M') be a maximal ideal of A lying over $\mathfrak{m}$ (resp. $\mathfrak{m}'$). For any $a = ru^2 + su + t$ in A, $\sigma(a) - a = (\gamma^2 - 1)ru^2 + (\gamma - 1)su = [(\gamma + 1)ru + s](\gamma - 1)u$. Therefore, since $u^3 = \alpha \in \mathfrak{m}'$ implies $u \in M'$, $\sigma(a) - a \in M'$, for every $a \in A$. Consequently $T_{M'} = G$. However, $u^3 = \alpha \notin \mathfrak{m}$ means $u \notin M$, so $\sigma(u) - u = (\gamma - 1)u \notin M$ since $\gamma - 1$ is a unit. Hence $\sigma \notin T_M$ and $T_M \neq T_{M'}$. This concludes the proof of Theorem 3.6.

We next consider a non-Henselian local ring R with maximal ideal $\mathfrak{m}$. Since R is not a Hensel ring, $R[x]$ contains a monic polynomial f such that $\bar{f} = g_0 h_0$, where g_0 and h_0 are relatively prime monic polynomials of positive degree in $(R/m)[x]$, but such that there do not exist monic polynomials g and h in $R[x]$ with $f = gh$, $\bar{g} = g_0$, and $\bar{h} = h_0$. Let J denote the set of all such polynomials f in $R[x]$. It is a straightforward exercise to verify that an element f of J of minimal degree does not factor into the product of two monic polynomials, each of positive degree.

THEOREM 3.11. *Let R be a noetherian local ring such that either R has a perfect residue class field or R is an integrally closed domain. Then, if R is an IC-ring, R is a Hensel ring.*

Proof. We assume that R is both non-Henselian and an IC-ring and proceed to a contradiction.

First we consider the case that the residue class field $R/\mathfrak{m}$ of R is perfect. Let f be an element of J of minimal degree. Set $A = R[x]/(f)$. It is known [12, (43.14), p. 184] that the irreducibility of f guarantees that A is connected. It is clear that A is a finitely generated, semilocal R-algebra. Therefore A/N is the direct sum of the residue class fields of A, each of which is separable over $R/\mathfrak{m}$ since $R/\mathfrak{m}$ is perfect. Hence A/N is R-separable. It follows from the assumption that R is an IC-ring that A contains an inertial subalgebra S. Since R is noetherian, S is finitely generated, so S is an IC-ring by Proposition 3.3. Hence, by Theorem 3.6, S is local. We show that this is impossible. Since $f \in J$, $\bar{f} = g_0 h_0$ where g_0 and h_0 are monic, relatively prime, and of positive degree. Hence

$$A/\mathfrak{m}A \cong \frac{(R/\mathfrak{m})[x]}{(g_0)} \oplus \frac{(R/\mathfrak{m})[x]}{(h_0)}.$$

By looking at the inverse images of these direct summands under the natural homomorphism of A onto $A/\mathfrak{m}A$, we see that A contains more than one maximal ideal. Since every maximal ideal of S comes by intersection from a maximal ideal of A (A is integral over S), and since $S/\text{rad}(S) \simeq A/N$ by Remark 2.2, we see that S contains precisely the same number of maximal ideals as does A and is therefore not local. This is the desired contradiction.

Now consider the case that R is an integrally closed local domain. By (43.2), p. 179 of [12], there exists, under the assumption that R is non-Henselian, a monic polynomial $f(x) = x^r + d_1 x^{r-1} + \cdots + d_r$ over R such that $d_1 \notin \mathfrak{m}$ and $d_2, \cdots, d_r \in \mathfrak{m}$ but such that $f(x)$ has no linear factor of the form $x + b$ with $b - d_1 \in \mathfrak{m}$. It is not difficult to show that, if we choose $f(x)$ of minimal degree among those polynomials having this property, $f(x)$ is monically irreducible. Hence, setting $A = R[x]/(f)$, we have as above that A is connected. Moreover, since $\bar{f}(x) = x^{r-1}(x - \bar{d}_1)$, $A/N \cong R/\mathfrak{m} \oplus R/\mathfrak{m}$ is R-separable. Therefore we can proceed to a contradiction exactly as in the case that $R/\mathfrak{m}$ is perfect.

COROLLARY 3.12. *Let R be a semi-local, noetherian ring such that either* (i) *all residue class fields of R are perfect, or,* (ii) *R is an integrally closed domain. Then R is an IC-ring if and only if R is a finite direct sum of Hensel rings.*

Proof. By Azumaya's result [3, pp. 145–146] and Proposition 3.2, a finite direct sum of Hensel rings is an IC-ring. Since any noetherian ring can be written as a finite direct sum of connected rings, the converse follows from Theorems 3.6 and 3.11.

Example. It is now apparent that there are many commutative rings which are not IC-rings. For example, the localization of the ring of rational integers over any prime p is an integrally closed, noetherian, local domain which is not a Hensel ring, since $x^2 + x + p$ is irreducible over the integers but factors into $x(x+1)$ modulo p. It is interesting to note that this is an example of a ring which is not an IC-ring but such that every proper homomorphic image is. [See Remark 3.5.]

To conclude this paper, we determine exactly which Dedekind domains are IC-rings. In particular, we show that every Dedekind domain with zero radical (e.g., the rational integers) is an IC-ring for which the uniqueness statement holds. This result indicates that the semilocal requirement in Corollary 3.12 can not in general be removed.

We begin our discussion with the following generalization of the Wedderburn-Malcev Theorem.

Theorem 3.13. *Let A be a finitely generated R-algebra such that A/N is separable and projective over R. In addition, suppose that $\bigcap_{i=1}^{\infty} N^i = (0)$ and that A is complete in its N-topology. Then A contains an inertial subalgebra S. Moreover S is determined up to inner automorphisms generated by elements of the form* $1 - n$, $n \in N$.

Proof. Since A/N is separable, $H_R^1(A/N, U) = 0$ for every two-sided A/N-module U [6, Chapter IX, p. 176]. Also A/N projective over R implies that N is an R-direct summand of A. Therefore we can follow the Hochschild-Curtis methods [8] and [10] exactly as they appear in [8, p. 81] to prove the existence of an inertial subalgebra S. By Lemma 2.3, any interial subalgebra S of A has the property that $S \cap N = (0)$, so again following Curtis [8], we get the uniqueness statement.

For any module U over an integral domain R, we denote the torsion part of U by U_T; i.e., $U_T = \{u \in U \mid ru = 0 \text{ for some } r \neq 0 \text{ in } R\}$. It is evident that if A is an algebra over an integral domain, A_T is a two-sided ideal of A.

The author gratefully acknowledges that the essential points of the following proof are due to G. J. Janusz.

Proposition 3.14. *Let S be a finitely generated, separable R-algebra, where R is a Dedekind domain. Then there exists a two-sided ideal S_P of S with* $S = S_P \oplus S_T$.

Proof. By Theorem 2.3, p. 374 of [2], S is separable over C and C is separable over R, where C denotes the center of S. Since C is finitely generated as an R-module, it follows that C/C_T is finitely generated and torsion-free, hence R-projective. Therefore, since every C-module which is R-projective is C-projective, the map $C \to C/C_T$ C-splits, implying the existence of an ideal C_P of C with $C = C_P \oplus C_T$.

Let e_P and e_T be idempotents in C with $Ce_P = C_P$ and $Ce_T = C_T$. Clearly $Se_T \subseteq S_T$. By Proposition 1.4, p. 370 of [2], Se_p is central separable over $Ce_P = C_P$, and, since C_P is torsion-free, the one-one correspondence between ideals of C_P and the two-sided ideals of Se_P [2, Corollary 3.2, p. 375] gives us that Se_p is torsion-free. It follows easily that $S_T = Se_T$, so taking $S_P = Se_P$, we have $S = S_P \oplus S_T$.

Proposition 3.15. *Let A be a finitely generated R-algebra, where R is a Dedekind domain with* $\mathrm{rad}(R) = (0)$. *Then the radical N of A is nilpotent.*

Proof. A/A_T is a finitely generated, torsion-free R-algebra and hence is projective. Therefore, by Lemma 1.1(b) and (c), there exists a positive integer n such that $[\mathrm{rad}(A/A_T)]^n = \mathrm{rad}(R)\cdot(A/A_T) = (0)$. Since $(N + A_T)/A_T \subseteq \mathrm{rad}(A/A_T)$, we see that $N^n \subseteq A_T$. Because A_T is a finitely generated torsion module over R, it is seen that $\mathfrak{a} = \mathrm{annih}_R(A_T)$ is a nonzero ideal of R. Hence A_T is a finitely generated $R/\mathfrak{a}$-module. Clearly unique factorization of ideals implies that $R/\mathfrak{a}$ has only a finite number of ideals, whence A_T has the descending chain condition on submodules. Therefore $N^n \subseteq A_T$ implies that there exists an integer m with $(N^n)^m = (N^n)^{m+1}$. It now follows from Nakayama's lemma that N is nilpotent.

Theorem 3.16. *Every Dedekind domain with zero radical is an IC-ring or which the uniqueness statement holds.*

Proof. Let R be a Dedekind domain with $\mathrm{rad}(R) = (0)$. Suppose A is a finitely generated R-algebra such that A/N is R-separable. By Proposition 3.14, there exist central idempotents $\bar{e}_P$ and $\bar{e}_T$ in A/N such that $(A/N)\bar{e}_T = (A/N)_T$ $(A/N)\bar{e}_P = (A/N)_P$ is R-projective, and $1 = \bar{e}_T + \bar{e}_P$. From Proposition 3.15, N is nilpotent, so there exist orthogonal idempotents e_T and e_P in A with $e_T + e_P = 1$ and $\psi(e_T) = \bar{e}_T$, $\psi(e_P) = \bar{e}_P$, where ψ is the natural homomorphism of A onto A/N. [11, Proposition 5, p. 54.]

We wish to consider the rings e_TAe_T and e_PAe_P. If we denote by ψ_T the homomorphism of e_TAe_T onto $(A/N)\bar{e}_T$ induced by restriction from ψ, we have by Proposition 1, page 48 of [11] that $\mathrm{kernel}(\psi_T) = \mathrm{rad}(e_TAe_T) = e_TNe_T$. The analogous statement holds for e_PAe_P.

Consider e_TAe_T. Since $\bar{e}_T \in (A/N)_T$ and $\psi(e_T) = \bar{e}_T$, there exists an element $r \neq 0$ in R with $re_T \in N$. But $N^n = (0)$ for some integer n, so $(re_T)^n = r^n e_T = 0$. Hence $e_T \in A_T$ and $e_TAe_T \subseteq A_T$. We can therefore consider e_TAe_T as a finitely generated $R/\mathfrak{a}$-algebra where $\mathfrak{a} = \mathrm{annih}_R(A_T) \neq (0)$. Moreover, e_TAe_T modulo its radical is isomorphic to $(A/N)\bar{e}_T$ which is $R/\mathfrak{a}$-separable, since $A'N$ is R-separable. Again by unique factorization of ideals, $R/\mathfrak{a}$ is a semilocal ring with nilpotent radical and so is a complete semilocal ring. It follows by Remarks 3.5 that $R/\mathfrak{a}$ is an IC-ring, so e_TAe_T contains an inertial subalgebra S_T.

Next consider e_PAe_P. It is a finitely generated R-algebra with nilpotent radical.

Furthermore, it modulo its radical is isomorphic to $(A/N)_P$, which is separable and projective over R. Applying Theorem 3.13, we conclude that $e_P A e_P$ contains an inertial subalgebra S_P.

One can now easily check that $S = S_P + S_T$ is an inertial subalgebra of A.

It only remains to show that the uniqueness statement holds for R. Suppose S and S' are two inertial subalgebras of A. By Proposition 3.14, there exist idempotents e_T, e_P in S, and e'_T, e'_P in S' with $Se_T = S_T$, $S'e'_T = S'_T$ and both $S_P = Se_P$ and $S'_P = S'e'_P$ projective over R. Since, by Lemma 1.1(c) and (d)), $\mathrm{rad}(S_P) = \mathrm{rad}(S'_P) = (0)$, the natural map ψ of A onto A/N restricted to S_P (resp. S'_P) is an isomorphism of S_P (resp. S'_P) onto $(A/N)_P$. Therefore, following exactly the uniqueness arguments in Theorem 1, p. 81 of [8], we can conclude that there exists an element $n \in N$ such that

$$\text{(VII)} \qquad (1-n)S_P(1-n)^{-1} = S'_P.$$

One checks that $(1-n)e_T(1-n)^{-1} = e'_T$, so $(1-n)S_T(1-n)^{-1}$ and S'_T are both inertial subalgebras of $e'_T A e'_T$. Since the uniqueness statement holds for $R/\mathfrak{a}$, we see that there exists $n' \in e'_T N e'_T = \mathrm{rad}(e'_T A e'_T)$ such that

$$\text{(VIII)} \qquad (1-n')(1-n)S_T(1-n)^{-1}(1-n')^{-1} = S'_T.$$

Finally, because $(1-n')^{-1}$ is of the form $(1-n'')$ for some $n'' \in e'_T N e'_T$, and e'_T and e'_P are orthogonal, S_P remains invariant under the inner automorphism induced by $(1-n')$. Therefore, from (VII) and (VIII), $[(1-n')(1-n)] S[(1-n')(1-n)]^{-1} = S'$, which proves that the uniqueness statement holds for R.

COROLLARY 3.17. *Let R be a Dedekind domain. Then R is an IC-ring for which the uniqueness statement holds if and only if R is a Hensel ring or* $\mathrm{rad}(R) = (0)$.

Proof. Aside from fields, the Dedekind domains with zero radical are just those containing an infinite number of maximal ideals. Hence, if R has a nonzero radical, R is semilocal and we can apply Corollary 3.12, recalling that every Dedekind domain is integrally closed.

BIBLIOGRAPHY

1. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24.

2. ———, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

3. G. Azumaya, *On maximally central algebras*, Nagoya Math. J. **2** (1951), 119–150.

4. N. Bourbaki, *Algèbre commutative*, Chapter I–II, Actualités Sci. Ind. No. 1290, Hermann, Paris, 1962.

5. ———, *Algèbre commutative*, Chapter V–VI, Actualités Sci. Ind. No. 1308, Hermann, Paris, 1964.

6. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.

7. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 19 pp.

8. C. W. Curtis, *The structure of non-semisimple algebras*, Duke Math. J. **21** (1954), 79–85.

9. M. Deuring, *Algebren*, Springer Berlin, 1935.

10. G. Hochschild, *Cohomology groups of an associative algebra*, Ann. of Math. **46** (1945), 58–67.

11. N. Jacobson, *Structure of rings*, rev. ed., Amer. Math. Soc. Colloq. Publ. Vol. 37, Amer. Math. Soc., Providence, R. I., 1964.

12. M. Nagata, *Local rings*, Interscience, New York, 1962.

13. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, N. J., 1958.

14. ———, *Commutative algebra*, Vol. II, Van Nostrand, Princeton, N. J., 1960.

Michigan State University,
East Lansing, Michigan