SEPARABLE ALGEBRAS OVER COMMUTATIVE RINGS

BY
G. J. JANUSZ(1), (2)

Introduction. The main objects of study in this paper are the commutative separable algebras over a commutative ring. Noncommutative separable algebras have been studied in [2]. Commutative separable algebras have been studied in [1] and in [2], [6] where the main ideas are based on the classical Galois theory of fields. This paper depends heavily on these three papers and the reader should consult them for relevant definitions and basic properties of separable algebras.

We shall be concerned with commutative separable algebras in two situations. Let R be an arbitrary commutative ring with no idempotents except 0 and 1. We first consider separable R-algebras that are finitely generated and projective as an R-module. We later drop the assumption that the algebras are projective but place restrictions on R — e.g., R a local ring or a Noetherian integrally closed domain.

In §1 we give a proof due to D. K. Harrison that any finitely generated, projective, separable R-algebra without proper idempotents can be imbedded in a Galois extension of R also without proper indempotents. We also give a number of preliminary results to be used in later sections.

In §2 we generalize some of the results about polynomials over fields to the case of a ground ring R with no proper idempotents. We show that certain polynomials (called "separable") admit "splitting rings" which are Galois extensions of the ground ring. We apply this to show that any finitely generated, projective, separable homomorphic image of $R[X]$ has a kernel generated by a separable polynomial.

In §3 we restrict our attention to separable algebras over a local ring. (The term "local" will not imply any finiteness conditions.) In certain cases every finitely generated, separable algebra is a homomorphic image of a finitely generated, projective, separable algebra. This gives an external characterization of the separable algebras. In §4 we consider the internal structure of seperable algebras over a Noetherian integrally closed domain. We show that a finitely generated separable algebra is the direct sum of projective, separable domains containing the ground ring and an algebra that is separable but not faithful over the ground ring. For the case of a Dedekind domain we can obtain specific infor-

Presented to the Society, April 24, 1965 under the title *Separable polynomials over commutative rings*: received by the editors October 6, 1965.

(1) The material in this paper is taken from the author's doctoral thesis written under the direction of Professor C. W. Curtis at the University of Oregon.

(2) This work was partially supported by the National Science Foundation.

mation about the nonfaithful separable algebras (Theorem 4.4). We include also in this section some results about finite rings that are separable over the subring generated by the identity element. We find a close analogy with finite fields — namely for any positive integers (n, r) and a prime p there is exactly one ring (up to isomorphism) of characteristic p^n which is separable over the subring generated by the identity element, has no idempotents except 0 and 1, and is of rank r.

We conclude in §5 with an application of the preceding theory to the problem of the existence of separable splitting rings for a group algebra of a finite group.

In order to avoid repetition we shall assume that all rings and algebras have identities and except in §5, all rings and algebras are commutative. The phrase "S is a finitely generated R-algebra" means S is an R-algebra which is finitely generated as an R-module. The symbol "$\otimes$" will mean "$\otimes_R$".

1. **Preliminaries.** Let R denote a commutative ring with no proper idempotents (no idempotents except 0 and 1).

DEFINITION 1. An R-algebra S is called *strongly separable* if it is finitely generated, projective, and separable over R.

Most of this section is devoted to proving a theorem due to D. K. Harrison. The author is grateful for his permission to reproduce this result here. The theorem we want to prove is the following improvement of Theorem A.7 in [2].

THEOREM 1.1. *Every strongly separable R-algebra without proper idempotents can be imbedded in a Galois extension of R without proper idempotents.*

The proof is quite long and involves some auxiliary concepts. For convenient reference we state a proposition proved in [6, p. 17].

PROPOSITION 1.2. *Let S be a separable R-algebra and $f: S \to R$ be an R-algebra homomorphism. Then there exists a unique idempotent e in S such that $f(e) = 1$ and $se = f(s)e$ for all s in S. Furthermore, if $f_1, \cdots, f_n$ are pairwise distinct R-algebra homomorphisms from S to R, then the corresponding idempotents $e_1, \cdots, e_n$ are pairwise orthogonal and $f_i(e_j) = \delta_{ij}$, the latter denoting the Kronecker delta.*

We shall make use of the following concept.

DEFINITION 2. An R-algebra A is called *locally strongly separable* if every finite set of elements in A is contained in a strongly separable R-subalgebra of A.

Notice that when S is a finitely generated R-subalgebra of a locally strongly separable R-algebra A, then S is contained in a strongly separable R-subalgebra of A.

LEMMA 1.3. *Let A and S be R-algebras with no proper idempotents and with S strongly separable over R. Then there are at most $n = \operatorname{rank}_R(S)$ distinct algebra homomorphisms from S to A.*

REMARK. We will frequently make use of the fact that the rank of a projective R-module is well defined. See [4, p. 132 and p. 138] for more information.

Proof. From each R-algebra homomorphism $f: S \to A$ we obtain an A-algebra homomorphism $F: A \otimes S \to A$ defined by $F(a \otimes s) = af(s)$. From Corollary 1.6 of [2] we know $A \otimes S$ is a strongly separable A-algebra. If $f_1, \cdots, f_m$ are distinct R-algebra homomorphisms from S to A we can apply (1.2) to $A \otimes S$ and the homomorphisms $F_1, \cdots, F_m$ to get orthogonal idempotents $e_1, \cdots, e_m$ in $A \otimes S$. We compute the rank of $A \otimes S$ by adding the ranks of the summands in a direct sum decomposition. Since there are at least m direct summands we conclude $\text{rank}_A(A \otimes S) \geqq m$. However $\text{rank}_R(S) = \text{rank}_A(A \otimes S)$ so we are done.

PROPOSITION 1.4. *There is a locally strongly separable R-algebra, Ω, such that Ω has no proper idempotents and if Γ is a strongly separable Ω-algebra with no proper idempotents then $\Omega = \Gamma$.*

Proof. One first shows that the property of being locally strongly separable is transitive. That is if $A \subseteq B \subseteq C$ are commutative rings with B locally strongly separable over A, and C locally strongly separable over B, then C is locally strongly separable over A. This follows easily from the fact that separability is transitive (see proof of Theorem 2.3 [2, p. 374]).

Now suppose the proposition is false. We then can construct a transfinite collection $\{\Omega_\alpha\}$ of R-algebras, indexed by a class $\{\alpha\}$ of ordinals, with the following properties:

(1) When α is a nonlimit ordinal, Ω_α is a strongly separable $\Omega_{\alpha-1}$-algebra; when α is a limit ordinal $\Omega_\alpha = \text{injlim}\{\Omega_\beta\}$, where the direct limit is taken over all $\beta < \alpha$;

(2) Ω_α is a locally strongly separable R-algebra;

(3) for $\alpha < \beta$, $\Omega_\alpha \subset \Omega_\beta$ (proper inclusion);

(4) Ω_α has no proper idempotents.

We reach a contradiction by showing there is an ordinal λ with $\alpha < \lambda$ for all $\alpha \in \{\alpha\}$. This allows us to form the direct limit of all Ω_α in $\{\Omega_\alpha\}$. First observe that the class of isomorphism types of strongly separable R-algebras without proper idempotents is a set. For a given R-algebra S of this kind there are at most $\text{rank}_R(S)$ possible imbeddings of S into any given Ω_α. Hence no Ω_α has cardinality greater than $\Sigma\, \text{rank}_R(S) \cdot \text{card}(S)$ where the sum is taken over the distinct isomorphism types of strongly separable R-algebras S without proper idempotents. To complete the proof we take λ any ordinal with cardinality greater than $\Sigma\, \text{rank}_R(S) \cdot \text{card}(S)$.

DEFINITION 3. An R-algebra Ω will be called a *separable closure* of R if Ω is locally strongly separable, has no proper idempotents, and if the only strongly separable Ω-algebra without proper idempotents is Ω itself.

The last proposition assures us that R has a separable closure.

Now suppose S is a strongly separable R-algebra without proper idempotents and Ω is a separable closure of R. Then $\Omega \otimes S \cong \Omega \oplus \cdots \oplus \Omega$ where there are $n = \operatorname{rank}_R(S)$ copies of Ω on the right. If π_i is the projection onto the ith coordinate then the map $f_i: s \to \pi_i(1 \otimes s)$ is an R-algebra homomorphism of S into Ω. These are mutually distinct and give all possible homomorphisms of S into Ω because of (1.3). Let $N = f_1(S) \cdot f_2(S) \cdots f_n(S)$. N is the smallest subalgebra of Ω containing all the homomorphic images of S. We shall prove that N is a Galois extension of R containing S. We shall use the criterion given in Theorem 3.5 of [6]. Clearly N is finitely generated since S is. N is separable over R because it is a homomorphic image of $S \otimes \cdots \otimes S$ (n-times). It remains to show that S is actually imbedded in N and that only the elements in R are left fixed by the full group of R-automorphisms of N.

Before proving that all of the f_i are monomorphisms we need the following.

PROPOSITION 1.5. *Let S be a strongly separable R-algebra and T an R-subalgebra of S.*

(1) *If T is separable over R then T is strongly separable over R and S is strongly separable over T.*

(2) *If S is projective over T, then T is separable over R.*

Proof. Part (2) follows from Proposition 4.8 of [1]. To prove (1) we need the following fact that will be used later on also. When S is separable over R, then any R-projective S-module is also S-projective. This follows from the vanishing of the Hochschild cohomology groups (see [5, p. 176]) but for completeness we sketch a proof in the next paragraph. Now for the proof of (1) we have S is R-projective and S is a T-module so S is T-projective. Thus S is strongly separable over T. T must be a T-direct summand of S so T is R-projective and hence strongly separable over R.

Now to prove that any R-projective S-module is also S-projective it is sufficient to show that any exact sequence of S-modules

$$0 \to M \to N \to W \to 0$$

that splits as a sequence of R-modules also splits over S. Let $\beta: S \otimes S \to S$ be the map defined by $\beta(a \otimes b) = ab$ and let e be the element in the annihilator of $\ker \beta$ such that $\beta(e) = 1$ [5, p. 179, Proposition 7.7]. $\operatorname{Hom}_R(N, N)$ is an $S \otimes S$-module when we define $a \otimes b \cdot f$ by $a \otimes b \cdot f: x \to af(bx)$ for $f \in \operatorname{Hom}_R(N, N)$ and $x \in N$. Now if f is the idempotent R-projection of N onto M, then $e \cdot f$ is an S-projection of N onto M. Hence M has an S-complement in N and the sequence splits over S.

LEMMA 1.6. *If S is a separable R-algebra and N a strongly separable R-algebra, then the kernel of any R-algebra homomorphism from S into N is generated by an idempotent.*

Proof. Let $f: S \to N$ be an R-algebra homomorphism. The R-algebra $f(S)$ is separable so by (1.5) $f(S)$ is strongly separable. Since $f(S)$ is an S-module which is projective over R, $f(S)$ is projective over S and hence the sequence of S-modules

$$0 \to \ker f \to S \to f(S) \to 0$$

is split. Thus $\ker(f)$ has an idempotent generator.

Returning to the context of the discussion above Proposition 1.5 we see the maps $f_i: S \to N$ are monomorphisms because S has no proper idempotents. In order to apply (1.6) here we need to know that N is strongly separable. But $N \subseteq \Omega$ implies N is contained in a strongly separable R-algebra so by (1.5) N is strongly separable.

Next we prove the uniqueness of the separable closure. Let Ω be a separable closure of R and Ω' any locally strongly separable R-algebra. Denote by $\mathscr{S}_R(\Omega')$ or $\mathscr{S}$ the collection of strongly separable R-subalgebras of Ω'. For each $S \in \mathscr{S}$ let $G(S) = \mathrm{Alg}_R(S, \Omega)$ = set of R-algebra homomorphisms of S into Ω. $G(S)$ is a finite set by (1.3) to which we assign the discrete topology. One can show $\mathscr{S}$ is a directed set (by inclusion) and for $S, T \in \mathscr{S}$ with $T \subseteq S$ we have a natural map from $G(S)$ to $G(T)$, the restriction map. Thus we may form the inverse limit, $L = \mathrm{projlim}\{G(S)\}$ over all $S \in \mathscr{S}$. L is a closed, nonempty subset of the compact space $\Pi G(S)$. (See [8, p. 215 and p. 217].) It is not difficult to verify that $L \cong \mathrm{Alg}_R(\Omega', \Omega)$. In particular $\mathrm{Alg}_R(\Omega', \Omega)$ is not empty.

PROPOSITION 1.7. *The separable closure of R is unique up to isomorphism.*

Proof. Let Ω and Ω' be separable closures of R. From the above remarks we know there are R-algebra homomorphisms $f: \Omega' \to \Omega$ and $g: \Omega \to \Omega'$. We shall prove that every endomorphism of Ω is an automorphism. From this it follows that $f \circ g$ and $g \circ f$ are one-to-one and onto. In particular f and g are isomorphisms. Let σ be an R-algebra endomorphism of Ω. Suppose $a \in \ker \sigma$. Let S be a strongly separable R-subalgebra of Ω with $a \in S$ and let T be a strongly separable R-subalgebra of Ω containing $\sigma(S)$. Applying (1.6) we see $\ker(\sigma \mid S)$ is generated by an idempotent. Since S has no proper idempotents $\ker(\sigma \mid S) = 0$ and hence $a = 0$. Thus σ is one-to-one. Now take $b \in \Omega$ and let S be a strongly separable R-subalgebra of Ω containing b. Let $f_1, \cdots, f_n$ be all the imbeddings of S into Ω. Suppose $f_1(s) = s$ for all $s \in S$. Then $\{\sigma \circ f_1, \cdots, \sigma \circ f_n\} = \{f_1, \cdots, f_n\}$ so that $\sigma \circ f_j = f_1$ for some j. In particular $b = f_1(b) = \sigma(f_j(b))$. Hence σ is onto. This completes the proof.

COROLLARY 1.8. *Let S be any strongly separable R-subalgebra of Ω. Any algebra homomorphism from S into Ω is induced by an automorphism of Ω.*

Proof. Let $f: S \to \Omega$ be an algebra homomorphism. View Ω as an S-algebra in the natural way and let Ω' denote Ω as an S-algebra with the operation

$s \cdot w = f(s)w$. Then Ω and Ω' are separable closures of S. By (1.7) there is an S-isomorphism $h: \Omega \to \Omega'$. That is $h(sw) = s \cdot h(w) = f(s)h(w)$ for s in S and w in Ω. In particular $h(s) = f(s)$ for s in S and h is an R-automorphism of Ω.

We are now able to complete the proof of (1.1). We must show that the automorphism group of N leaves only R fixed. In view of (1.8) it is sufficient to prove the following.

PROPOSITION 1.9. *Let Ω be a separable closure of R. Then only the elements of R are left fixed by all the R-automorphisms of Ω.*

Proof. Let $s \in \Omega$ and suppose $\sigma(s) = s$ for each $\sigma \in \mathrm{Aut}_R(\Omega)$. Let S be a strongly separable R-subalgebra of Ω with $s \in S$. We have $f(s) = s$ for each $f \in \mathrm{Alg}_R(S, \Omega)$ because each such f is induced from an automorphism of Ω. Thus for any element $g \in \mathrm{Alg}_\Omega(\Omega \otimes S, \Omega)$ we must have $g(1 \otimes s) = s$ because $s' \to g(1 \otimes s')$ is an element of $\mathrm{Alg}_R(S, \Omega)$. The Ω-algebra $\Omega \otimes S$ is the ring direct sum of copies of Ω. Thus the elements of $\mathrm{Alg}_\Omega(\Omega \otimes S, \Omega)$ separate points of $\Omega \otimes S$ from zero. But we have for $g \in \mathrm{Alg}_\Omega(\Omega \otimes S, S)$ the equation $g(s \otimes 1) - g(1 \otimes s) = s - s = 0$. Hence $1 \otimes s = s \otimes 1$.

Now consider the diagram below

$$\begin{array}{ccc} R \otimes S & \xrightarrow{\alpha_3} & R \otimes (S/R) \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_4} \\ \Omega \otimes S & \xrightarrow{\alpha_2} & \Omega \otimes (S/R). \end{array}$$

Here α_1 and α_4 are induced by the imbedding of R in Ω while α_2 and α_3 are induced by the projection of S onto S/R. Since S is strongly separable over R, R is an R-direct summand of S so that S/R is a projective R-module. Hence α_4 is one-to-one. We now have $\alpha_2 \circ \alpha_1(1 \otimes s) = \alpha_2(1 \otimes s) = \alpha_2(s \otimes 1) = 0$ because $1 \in \ker(S \to S/R)$. Thus $\alpha_4 \circ \alpha_3(1 \otimes s) = 0$. Since α_4 is one-to-one we have $\alpha_3(1 \otimes s) = 0$. Hence $s \in \ker(S \to S/R) = R$ which is what we wanted to prove.

REMARKS. 1. Using the notions described here one can develop an infinite Galois theory for a ring R with no proper idempotents. One defines the infinite Galois group to be $\mathrm{Aut}_R(\Omega)$ = group of R-automorphisms of a separable closure of R. There is a one-to-one correspondence between the closed subgroups of the topological group $\mathrm{Aut}_R(\Omega)$ and the locally strongly separable R-subalgebras of Ω.

2. We have used several times that $\Omega \otimes S \cong \Omega \oplus \cdots \oplus \Omega$ when S is a strongly separable R-algebra and Ω is a separable closure of R. The idempotents in $\Omega \otimes S$ which induce this decomposition can be written with only a finite number of elements from Ω and S. Hence there is a strongly separable R-algebra, T say, with no proper idempotents and such that $T \otimes S \cong T \oplus \cdots \oplus T$. This fact will be useful in the next section.

2. **Separable polynomials.** We continue to let R denote a commutative ring with no proper idempotents.

DEFINITION 4. A polynomial $f(X) \in R[X]$ is called separable if it is monic and if $R[X]/(f(X))$ is a separable R-algebra.

In this section we establish several properties of separable polynomials and show that they play an important part in the classification of the separable homomorphic images of $R[X]$. We begin with some properties of the roots of a separable polynomial.

LEMMA 2.1. *Let S be a separable R-algebra without proper idempotents. A polynomial $f(X)$ of degree n which is separable over R cannot have more than n roots in S. Moreover if α and β are distinct roots of $f(X)$ in S, then $\alpha - \beta$ is invertible in S.*

Proof. Let $\alpha_1, \cdots, \alpha_m$ be distinct roots of $f(X)$ in S. Since $f(X)$ is separable over R, the S-algebra $S \otimes \{R[X]/(f)\} \cong S[X]/(f)$ is separable. For each i, $1 \leqq i \leqq m$, the map $h_i: S[X] \to S$ defined by setting $h_i(X) = \alpha_i$ induces an S-algebra homomorphism, g_i, from $S[X]/(f)$ to S. Since the g_i are distinct we apply (1.2) to obtain orthogonal idempotents $e_1, \cdots, e_m$ in $S[X]/(f)$. This algebra is a free S-module of rank n so we must have $m \leqq n$ as required.

Applying (1.2) again we see $\{X + (f)\}e_i = \alpha_i e_i$ so that the ideal $(X - \alpha_i)$ of $S[X]$ maps onto the annihilator of e_i under the natural projection of $S[X]$ onto $S[X]/(f)$. Hence for $i \neq j$, $(X - \alpha_i)$ and $(X - \alpha_j)$ are comaximal ideals of $S[X]$. There exist polynomials $p(X)$, $q(X) \in S[X]$ with

$$p(X)(X - \alpha_i) + q(X)(X - \alpha_j) = 1.$$

Thus $q(\alpha_i)(\alpha_i - \alpha_j) = 1$ and $\alpha_i - \alpha_j$ is invertible.

We can now characterize the separable polynomials over R in several ways.

THEOREM 2.2. *Let $f(X)$ be a monic polynomial in $R[X]$. The following statements are equivalent.*

(1) *$f(X)$ is a separable polynomial.*

(2) *There is a strongly separable R-algebra S with no proper idempotents which contains elements $\alpha_1, \cdots, \alpha_n$ such that $f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ and for $i \neq j$, $\alpha_i - \alpha_j$ is invertible in S.*

(3) *For each maximal ideal $\mathfrak{m}$ of R, $f(X)$ is separable when viewed as a polynomial over the local ring $R_{\mathfrak{m}}$.*

(4) *For each maximal ideal $\mathfrak{m}$ of R, the polynomial obtained from $f(X)$ by reducing the coefficients modulo $\mathfrak{m}$ has no repeated roots in an algebraic closure of $R/\mathfrak{m}$.*

(5) *Let t denote the trace map of the free R-module $R[X]/(f)$ and let x denote the coset of X modulo (f). Then the determinant of the matrix $\| t(x^i x^j) \|$, $0 \leqq i, j < \deg f$, is an invertible element of R.*

Proof. (1) $\rightarrow$ (2). By the remark at the end of §1 we know there is a strongly separable R-algebra S without proper idempotents such that

$$S[X]/(f) \cong S \otimes \{R[X]/(f)\} \cong Se_1 \oplus \cdots \oplus Se_n$$

where the e_i are orthogonal idempotents. If $\{X + (f)\}e_i = \alpha_i e_i$ with $\alpha_i \in S$, then $\alpha_1, \cdots, \alpha_m$ are roots of $f(X)$. The argument used in (2.1) shows $\alpha_i - \alpha_j$ is invertible for $i \neq j$. The invertibility of $\alpha_i - \alpha_j$ implies $f(X)$ can be factored as $f(X) = (X - \alpha_1)\cdots(X - \alpha_n)$.

(2) $\rightarrow$ (1). Let S have the properties stated in (2). The ideals $(X - \alpha_i)$ in $S[X]$ are pairwise comaximal so that

$$S[X]/(f) \cong S \oplus \cdots \oplus S \qquad (n \text{ copies of } S).$$

Thus $f(X)$ is separable over S. Then $S \otimes \{R[X]/(f)\}$ is separable over S so by Proposition 7.1, p. 177 of [5] we have $R[X]/(f)$ is separable over R.

(1) $\leftrightarrow$ (5). The free R-module $R[X]/(f)$ has a basis $x^0 = \bar{1}, x, x^2, \cdots, x^{n-1}$ where $n =$ degree of $f(X)$. Let π_i be the projection onto the coefficient of x^i. The trace map t is defined by $t(z) = \sum \pi_i(zx^i)$. Let T denote $R[X]/(f)$. T will be separable over R if and only if $\mathrm{Hom}_R(T, R)$ is a free T-module of rank 1 with t as free generator (Proposition A.4 of [2, p. 397]). Thus T is separable if and only if there are elements $z_i \in T$ with $z_i t = \pi_i$. Suppose T is separable so that such z_i exist. Let $z_i = \sum \alpha_{ij} x^j$ for $\alpha_{ij} \in R$. Then we have $\pi_i(x^j) = \delta_{ij} = t(z_i x^j) = \sum_k \alpha_{ik} t(x^k x^j)$. In matrix notation we have $\| \alpha_{ij} \| \cdot \| t(x^i x^j) \| =$ identity matrix. Hence $\det \| t(x^i x^j) \|$ is invertible in R. The steps are reversible for the converse. We shall call $\det \| t(x^i x^j) \|$ the *discriminant of* $f(X)$.

The proof that (1), (3) and (4) are equivalent is not difficult if one uses the following proposition which is similar to Corollary 4.5 and Theorem 4.7 of [2].

PROPOSITION 2.3. *Let S be a commutative R-algebra that is finitely generated and projective as an R-module.*

(1) *S is separable over R if and only if $R_{\mathfrak{m}} \otimes S$ is separable over the local ring $R_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$ of R.*

(2) *S is separable over R if and only if $S/\mathfrak{m}S$ is separable over $R/\mathfrak{m}$ for each maximal ideal $\mathfrak{m}$ of R.*

Proof. Both parts of the proposition are easily proved using the test for separability given in Theorem A.4 of [2].

COROLLARY 2.4. *For $n > 1$ and $\alpha \in R$, the polynomial $X^n - \alpha$ is separable if and only if $n \cdot 1$ and α are invertible elements of R.*

Proof. A direct computation shows that the discriminant of $X^n - \alpha$ is $\pm n(n\alpha)^{n-1}$. The result now follows from part (5) of the theorem.

Combining this with (2.1) we obtain the following.

COROLLARY 2.5. *If R is a commutative ring with no proper idempotents in which $n \cdot 1$ is invertible, for an integer $n > 1$, then R has at most n nth roots of unity.*

This corollary is false if we replace the assumption that $n \cdot 1$ be invertible with the assumption that $n \cdot 1$ be a nonzero divisor. Consider the group ring $Z(G)$ of a finite abelian group G of exponent n and order greater than n over the ring of integers. Every element of G is an nth root of unity and $n \cdot 1$ is a nonzero divisor. The fact that $Z(G)$ has no proper idempotents is proved in [7, p. 557]. Other examples are easily found with $n \cdot 1$ a zero divisor.

Following the classical terminology we introduce a definition.

DEFINITION 5. A strongly separable R-algebra, S, without proper idempotents is called a *splitting ring* for the separable polynomial $f(X)$ if $f(X)$ is a product of linear factors from $S[X]$ and if S is generated over R by the roots of $f(X)$.

The next proposition along with (2.2), part (2) shows that splitting rings exist.

PROPOSITION 2.6. *Let $f(X)$ be a separable polynomial over R and T a Galois extension of R with no proper idempotents. If $\alpha_1, \cdots, \alpha_n$ are all the roots of $f(X)$ in T, then $S = R[\alpha_1, \cdots, \alpha_n]$ is a Galois extension of R.*

Proof. We first show S is separable over R. Let $S_i = R[\alpha_1, \cdots, \alpha_i]$. S_1 is separable over R because it is a homomorphic image of $R[X]/(f)$. $S_{j+1} = S_j[\alpha_{j+1}]$ is separable over S_j because it is a homomorphic image of the separable S_j-algebra $S_j \otimes \{R[X]/(f)\}$. Hence the transitivity of separability gives S_j separable over R for each $j = 1, \cdots, n$. Now $S = S_n$ is strongly separable because it is a separable R-algebra contained in a strongly separable R-algebra (1.5). Now to show S is Galois over R, let G be the Galois group of T over R. Let H be the subgroup of G leaving S fixed. Since the elements of G permute the roots of $f(X)$ we conclude H is a normal subgroup of G. Thus Theorem 2.3 of [6] tells us S is a Galois extension of R.

The next goal is to see how the separable polynomials fit into a classification of the separable homomorphic images of $R[X]$. We begin with a lemma.

LEMMA 2.7. *Let T be a strongly separable R-algebra with no proper idempotents and let α be an element of T. Then $R[\alpha]$ is a separable subalgebra of T if and only if α is a root of a separable polynomial over R.*

Proof. By (1.1) we see there is no loss in generality if we assume T is a Galois extension of R with group G. Suppose $R[\alpha]$ is separable. Then $R[\alpha]$ is left fixed by a subgroup H of G which leaves only $R[\alpha]$ fixed (Theorem 2.3 of [6]). Let $H\sigma_1, \cdots, H\sigma_r$ be all the distinct cosets of H in G and let $f(X) = (X - \sigma_1(\alpha)) \cdots (X - \sigma_r(\alpha))$. Since the coefficients of $f(X)$ are left fixed by all of G, $f(X)$ is in $R[X]$. We shall prove $f(X)$ is a separable polynomial. By (2.2) it is sufficient to prove that $\sigma_i(\alpha) - \sigma_j(\alpha)$ is invertible in T for $i \neq j$. Suppose for some pair (i,j) with $i \neq j$

that $\sigma_i(\alpha) - \sigma_j(\alpha)$ is not invertible. If we let $\sigma = \sigma_i^{-1}\sigma_j$, then there is a maximal ideal M of T containing $\alpha - \sigma(\alpha)$. We also have

$$\alpha^m - \sigma(\alpha^m) = [\alpha - \sigma(\alpha)][\alpha^{m-1} + \cdots + \sigma(\alpha)^{m-1}]$$

in M for each positive integer m. Thus $\beta - \sigma(\beta)$ is in M for each β in $R[\alpha]$. We shall prove that this implies σ is in H contrary to the choice of i and j.

Theorem 1.3 of [6] assures us that there are elements $x_1, \cdots, x_n; y_1, \cdots, y_n$ in T such that $\Sigma x_i \pi(y_i) = 1$ or 0 according as $\pi = 1$ or $\pi \neq 1$ for $\pi \in G$. Lemma 1.3 of [6] says there is an element c_0 in T with $\Sigma_{\pi \in G} \pi(c_0) = 1$. Now let $c = \Sigma_i \sigma_i(c_0)$,

$$u_i = \sum_{\mu \in H} \mu(cx_i), \quad \text{and} \quad v_i = \sum_{\mu \in H} \mu(y_i).$$

The elements u_i and v_i are in $R[\alpha]$ because they are left fixed by H. One verifies directly that $\Sigma_i u_i \pi(v_i) = 1$ or 0 according as $\pi \in H$ or $\pi \notin H$.

Now if the particular σ selected above is not in H, then

$$1 = \Sigma u_i v_i - \Sigma u_i \sigma(v_i) = \Sigma u_i (v_i - \sigma(v_i)).$$

From above we know this element belongs to M and this is a contradiction so this part of the lemma is true. The converse follows at once since $R[\alpha]$ is a homomorphic image of $R[X]/(f)$.

COROLLARY 2.8. *Let T be a Galois extension of R without proper idempotents and suppose $\alpha \in T$ with $R[\alpha]$ a separable R-algebra. Let $\alpha = \alpha_1, \cdots, \alpha_m$ be all the distinct images of α under the Galois group of T. If $g(X)$ is any polynomial in $R[X]$ such that $g(\alpha) = 0$, then $g(X)$ is a multiple of $f(X) = (X - \alpha_1) \cdots (X - \alpha_m)$ by an element of $R[X]$.*

Proof. From the proof of (2.7) we know $f(X)$ is a separable polynomial. Hence $\alpha_i - \alpha_j$ is invertible for $i \neq j$. If $g(\alpha) = 0$ then $g(\alpha_i) = 0$ for each i. We can find $p_1(X) \in T[X]$ with $g(X) = (X - \alpha_1)p_1(X)$. Since $\alpha_2 - \alpha_1$ is invertible, $p_1(\alpha_2) = 0$ so there is a $p_2(X) \in T[X]$ with $p_1(X) = (X - \alpha_2)p_2(X)$. Continuing this way we reach $g(X) = f(X)p_n(X)$. Since $g(X), f(X) \in R[X]$ and $f(X)$ is monic, we can conclude $p_n(X) \in R[X]$.

We use this corollary in the next theorem.

THEOREM 2.9. *If M is an ideal of $R[X]$ such that $R[X]/M$ is a strongly separable R-algebra then M is a principal ideal generated by a separable polynomial.*

Proof. Let A denote the strongly separable R-algebra $R[X]/M$. Since rank over R is defined for direct summands of A there exist orthogonal idempotents $e_1, \cdots, e_m$ in A with $A = Ae_1 \oplus \cdots \oplus Ae_m$ and such that Ae_i is a ring with no idempotents except 0 and e_i. In fact Ae_i is a strongly separable R-algebra. Let x denote the coset of X modulo M. Then we have $Ae_i = R[xe_i]$ (where we identify

R with Re_i). By (2.7) xe_i is a root of a separable polynomial over R. Let $g_i(X)$ be one of least degree. Then Corollary 2.8 implies that the ideal generated by $g_i(X)$ is the kernel of the map $R[X] \to R[xe_i]$. Each ideal (g_i) contains M and the ideals $(g_i)/M$ are pairwise comaximal in A. Hence the (g_i) are pairwise comaximal in $R[X]$. In particular the intersection of the ideals (g_i) is equal to the product. But M is the intersection of the (g_i) so $M = (g_1)\cdots(g_m) = (g)$ where $g = g(X) = g_1(X)\cdots g_m(X)$.

COROLLARY 2.10. *If $f(X)$ is a separable polynomial over R then there exist separable polynomials $g_1(X), \cdots, g_m(X)$ in $R[X]$ such that $f(X) = g_1(X)\cdots g_m(X)$ and $R[X]/(g_i)$ has no proper idempotents.*

Proof. Take $(f) = M$ in the theorem.

3. **Local rings.** In this section we let R denote a (not necessarily Noetherian) local ring with unique maximal ideal $\mathfrak{m}$. We adopt the terminology of field theory and say that an R-algebra A has a primitive element θ if $A = R[\theta]$. Clearly the R-algebras with a primitive element are those which are homomorphic images of $R[X]$.

We first consider what is required for a separable R-algebra S to have a primitive element. A standard Nakayama's lemma argument shows that S has a primitive element over R if and only if $S/\mathfrak{m}S$ has a primitive element over $R/\mathfrak{m}$. Thus the question reduces to the field case. However in this case it is known that every separable algebra over an infinite field has a primitive element. Hence we obtain the following.

LEMMA 3.1. *If $R/\mathfrak{m}$ is an infinite field, then every finitely generated separable R-algebra has a primitive element.*

An example due to Dedekind shows that some restriction on the local ring R is necessary for the validity of (3.1). (See [12, p. 170], for the example and some details.)

We have seen in (2.9) that when $R[X]/M$ is strongly separable over R, then M is a principal ideal. This need not be the case if we assume that $R[X]/M$ is only separable over R. However we can obtain some information about M as follows.

LEMMA 3.2. *Suppose M is an ideal of $R[X]$ such that the R-algebra $A = R[X]/M$ is finitely generated and separable over R. Then M contains a monic polynomial $f(X)$ which is separable over R. Moreover we can choose $f(X)$ so that A is a homomorphic image of the strongly separable R-algebra $T = R[X]/(f)$ and the kernel of this homomorphism is contained in $\mathfrak{m}T$.*

Proof. Since A is finitely generated as an R-module every element satisfies a monic polynomial in $R[X]$. In particular the monic polynomial satisfied by

$X + M$ belongs to M. Let $f(X)$ be a monic polynomial of least degree in M. We show first that any polynomial in M with degree less than the degree of $f(X)$ has all its coefficients in $\mathfrak{m}$. Suppose this is not the case. Then there is a polynomial $p(X)$ in M such that

(1) $p(X) = \alpha_r X^r + \cdots + \alpha_j X^j + \cdots + \alpha_0 \neq 0$ where $r < \deg(f)$ and $\alpha_j \notin \mathfrak{m}$;

(2) the integer $\beta(p(X)) = r - j$ is as small as possible.

We cannot have $\beta(p(X)) = 0$ because $f(X)$ has least degree for monic polynomials in M. (Recall that $\alpha_j \notin \mathfrak{m}$ implies α_j is invertible in R.) Now consider the polynomial $h(X) = X^{n-r} \cdot p(X) - \alpha_r f(X)$. Then $h(X)$ belongs to M and has degree $< \deg(f)$. If λ_j is the coefficient of X^j in $f(X)$, then the coefficient of X^{n-r+j} in $h(X)$ is $\alpha_j - \alpha_r \lambda_j$. Since α_r is in $\mathfrak{m}$ we see $\alpha_j - \alpha_r \lambda_j$ is not in $\mathfrak{m}$. Thus $\beta(h(X)) \leqq n - 1 - (n - r + j) = r - j - 1 < \beta(p(X))$. By choice of $p(X)$ we must have $h(X) = 0$. That is $\alpha_r f(X) = X^{n-r} \cdot p(X)$. This implies every coefficient of $p(X)$ belongs to $\mathfrak{m}$. This contradiction establishes the claim above. Now we can show $f(X)$ is a separable polynomial. By part (4) of (2.2) it is sufficient to show that $f(X)$ is separable modulo $\mathfrak{m}$. The claim established above proves that the ideal M maps onto the principal ideal $(\bar{f})$ when the coefficients are reduced modulo $\mathfrak{m}$. Thus $A/\mathfrak{m}A \cong \bar{R}[X]/(\bar{f})$ where $\bar{R} = R/\mathfrak{m}$. Since A is separable over R, $A/\mathfrak{m}A$ is separable over $\bar{R}$ and thus $\bar{f}(X)$ is separable over $\bar{R}$ as required. Thus the R-algebra $T = R[X]/(f)$ is strongly separable and A is a homomorphic image of T. The kernel is in $\mathfrak{m}T$ because $(f) \subseteq M \subseteq (f) + \mathfrak{m} \cdot R[X]$.

We can state this more abstractly as follows.

COROLLARY 3.3. *Let S be a finitely generated separable R-algebra and suppose either $R/\mathfrak{m}$ is an infinite field or that S is a direct sum of local rings. Then there is a strongly separable R-algebra T such that S is a homomorphic image of T with kernel contained in $\mathfrak{m}T$. Moreover if S has no proper idempotents we can choose T without proper idempotents also.*

Proof. The hypothesis insures that S has a primitive element or else S is a direct sum of rings with a primitive element. In either case we apply (3.2) to get the algebra T. In case S has no proper idempotents, T will not have any either because $\mathfrak{m}T$ cannot contain an idempotent.

REMARK. The restriction on the residue field of R is probably unnecessary, but a proof of the result in general is lacking. An earlier version of this paper contained a "proof" but an error was pointed out by Michael Wichman.

Theorem 3.3 is false without some assumption on the ring R. Consider the ring Z of integers. The only strongly separable Z-algebras are direct sums of copies of Z. Hence the separable Z-algebra $GF(p^2)$ is not a homomorphic image of any strongly separable Z-algebra.

4. **Integrally closed domains.** In the last section we gave an external characterlization of the separable algebras over a local ring as homomorphic images of the

strongly separable algebras. We now let R denote a Noetherian integrally closed domain and consider the internal structure of separable algebras over R. We first state a lemma that is proved in [1].

LEMMA 4.1. *If S is a domain containing R which is finitely generated and separable over R, then S is projective over R.*

We shall make use of this lemma to obtain more precise information about separable R-algebras.

COROLLARY 4.2. *Let S be a finitely generated, separable R-algebra containing R but not containing proper idempotents. Then S is a domain and is projective over R.*

Proof. Let K be the quotient field of R. $K \otimes S$ is a separable K-algebra and so it is a direct sum of fields. Let e be the identity of one of the fields in this decomposition. The map $s \to (1 \otimes s)e$ from S onto $(1 \otimes S)e$ is an R-algebra homomorphism onto a separable domain containing R. By the lemma $(1 \otimes S)e$ must be projective over R. Thus by (1.6) $\ker(S \to (1 \otimes S)e)$ has an idempotent generator. Since S has no proper idempotents the map $S \to (1 \otimes S)e$ is a monomorphism. This implies that $K \otimes S$ has only one direct summand. That is $K \otimes S$ is a field and since $S \to K \otimes S$ is a monomorphism, S is a domain.

EXAMPLE. This corollary is false without the assumption that R be integrally closed. Let $Z_{(2)}$ be the localization at 2 in the ring of integers. Let $R = Z_{(2)} + Z_{(2)}5^{1/2}$. Then R is a Noetherian domain which is not integrally closed. Consider the separable R-algebra $S = R[X]/(X^2 + X - 1)$. S has no proper idempotents and is not a domain. There is a natural map from S onto $R[\frac{1}{2}(1 - 5^{1/2})]$ which takes X onto $-\frac{1}{2}(1 - 5^{1/2})$. This shows $R[\frac{1}{2}(1 - 5^{1/2})]$ is a domain that is separable but not projective over R. Thus (4.1) is also false without integral closure.

We now have enough information to describe the separable algebras over R.

THEOREM 4.3. *Let R be a Noetherian integrally closed domain and S a finitely generated, separable R-algebra. There is an idempotent e in S such that $S = Se \oplus t(S)$ where $t(S)$ is the R-torsion submodule of S and Se is a strongly separable R-algebra with identity e. Moreover Se is the direct sum of Noetherian integrally closed domains each of which is strongly separable over R.*

Proof. The set $t(S)$ of R-torsion elements of S is an ideal of S. Hence the factor algebra $S/t(S)$ is separable and torsion free over R. $S/t(S)$ decomposes into the direct sum of R-algebras which have no proper idempotents. By (4.2) these summands are projective so $S/t(S)$ is projective over R. Now by (1.6) the kernel of the map $S \to S/t(S)$ has an idempotent generator, say $1 - e$. Thus $S = Se \oplus t(S)$. It is clear from (4.2) that Se is the direct sum of Noetherian domains

each separable over R. It remains to show these are integrally closed. Suppose first that T is an integral domain which contains R and which is Galois over R with group G. Let T' denote the integral closure of T in its quotient field. One checks easily that G is also a group of automorphisms of T'. Using Theorem 1.3, part (b), [6, p. 18] we see that T' is Galois over R with group G. By the fundamental theorem of Galois theory [6], T must be left fixed by a subgroup of G. This subgroup must consist of only the identity so $T = T'$. For the case of a domain T which is strongly separable over R but not necessarily Galois over R, we first imbed T in a Galois extension of R with no proper idempotents (1.1). This extension is a domain by (4.2) and we may proceed as in the above argument. This completes the proof.

This theorem shows that the study of separable algebras over a Noetherian integrally closed domain is reduced to two cases: the study of strongly separable domains over R and the study of separable algebras over a proper homomorphic image of R. That is the torsion part, $t(S)$ in (4.3) can be viewed as an algebra over R/a where a is the annihilator in R of $t(S)$. We shall not discuss the first case. For general Noetherian integrally closed the second case is difficult because the domains have a rather complicated ideal structure. In what follows we restrict ourselves to the case of a Dedekind domain. Here the ideal structure is well known.

Let R be a Dedekind domain and T a finitely generated, separable R-algebra with a nonzero annihilator a in R. We may assume that a is a power, p^e, of a prime ideal p in R since the general case can be reduced to this by a direct sum argument. We may also assume T has no proper idempotents for the same reason. Let A denote R/p^e. We shall establish a number of properties of the A-algebra T.

I. *T has a primitive element over A.*

Proof. A is a ring with descending chain condition and radical pA. Since T/pT is separable over the field A/pA, T/pT is a semisimple ring. Thus the radical of T is pT. It is well known that orthogonal idempotents in T/pT can be lifted to orthogonal idempotents in T. Since T has no proper idempotents, T/pT is a field. By the primitive element theorem for fields, there is an element θ in T such that $A[\theta] + pT = T$. Applying Nakayama's lemma we see that we must have $A[\theta] = T$.

II. *T is a homomorphic image of a Dedekind domain D which is strongly separable over the local ring R_p.*

Proof. By (I) we have $T \cong A[X]/M$ for some ideal M of $A[X]$. Let $f(X)$ be a monic polynomial of least degree in M and let $F(X)$ be a monic polynomial in $R_p[X]$ which maps onto $f(X)$ modulo p^e. By the proof of (3.2) we know $f(X)$

is a separable polynomial over A and hence $F(X)$ is a separable polynomial over R_p (by (2.2), part 4). Thus $D = R_p[X]/(F)$ is a strongly separable R_p-algebra having T as a homomorphic image. We show D is a Dedekind domain. If D has proper idempotents, then so does D/pD. This is not the case since $D/pD \cong T/pT$ which is a field. Hence by (4.2) D is a domain. If L is any ideal $\neq 0$ in D then L is a projective R_p-module because it is a submodule of the projective R_p-module D. Since D is separable over R_p, L is projective over D and hence every ideal of D is D-projective. Thus D is a Dedekind domain [5, p. 134].

III. *If T is a faithful A-algebra, then T is projective over A.*

Proof. Let D be as in II. We have seen that pD is a maximal ideal of D and that T is a homomorphic image of D/p^eD. Since D is a Dedekind domain, the only ideals between D and p^eD are p^iD for $0 \leqq i \leqq e$. Thus if T is faithful over A we must have $T \cong D/p^eD$. But now D is projective over R_p so $T \cong D/p^eD$ is projective over $R_p/p^eR_p \cong A$.

IV. *T is a self-injective, local, principal ideal ring.*

Proof. That T is a local ring follows from the fact that pT is a maximal ideal and is also equal to the radical. To show T is self-injective it is sufficient to prove $L = \operatorname{ann}(\operatorname{ann} L)$ for each ideal L of T where $\operatorname{ann}(L)$ is the annihilator in T of L. (See [7, p. 396].) Since T is a homomorphic image of D, this follows from the multiplicative properties of the ideals in D. Finally T is a principal ideal ring by Corollary 1, p. 278, of [13].

With this list of facts we can now describe the separable algebras over a Dedekind domain.

THEOREM 4.4. *Let R be a Dedekind domain and S a finitely generated, separable R-algebra. Then S is the direct sum of Dedekind domains each of which is strongly separable over R, and self-injective, local, principal ideal rings each of which is strongly separable over a suitable local homomorphic image of R.*

Proof. The theorem follows from the decomposition of (4.3) and from the properties established above.

We can obtain still more information about the strongly separable algebras over $A = R/p^e$ if we assume R/p is a finite field, say with q elements. Since p^i/p^{i+1} is a 1-dimensional vector space over R/p we see that A must have q^e elements. Suppose T is a strongly separable A-algebra with no proper idempotents. We have seen above that pT is a maximal ideal of T so $T/pT \cong GF(q^r)$ for some positive integer r. We shall sketch a proof that T is uniquely determined up to isomorphism by A and the integer r. T is a free A-module of rank r so T has q^{er} elements and pT has $q^{r(e-1)}$ elements. If there are m primitive elements

for $GF(q^r)$ over $GF(q)$ then there are $m \cdot q^{r(e-1)}$ primitive elements for T over A. Next we count the irreducible monic polynomials in $A[X]$ with degree r. There are m/r irreducible monic polynomials over $GF(q)$ with degree r. A is a complete local ring so by Hensel's Lemma [13, vol. II, p. 279], irreducible monic polynomials over A remain irreducible over A/pA. Thus there are $(m/r)q^{r(e-1)}$ monic irreducible polynomials over A with degree r. This counting argument shows that up to isomorphism there is only one strongly separable A-algebra without proper idempotents with the form $A[X]/(f)$ where $f(X)$ is a polynomial of degree r. However property (I) above shows T must be of this form. We summarize these remarks as follows.

PROPOSITION 4.5. *Let R be a Dedekind domain with maximal ideal p such that R/p is finite. Let $A = R/p^e$ for some positive integer e. Then for each positive integer r there is one and (up to isomorphism) only one strongly separable A-algebra without proper idempotents and with rank r over A.*

We can say a little more about a strongly separable A-algebra T without proper idempotents — namely it is a Galois extension of A. To prove this first imbed T in a Galois extension without proper idempotents. Its Galois group is the same as the Galois group of its residue field. Since the residue field is finite, its Galois group is abelian. Hence the subgroup leaving T fixed is normal and so T is Galois over A.

If we consider the special case of $R = Z =$ the ring of integers, this proposition shows there is no ambiguity in the notation $GR(p^n, r)$ for a strongly separable $Z/(p^n)$-algebra of rank r having no proper idempotents (the letters "GR" for Galois ring). Notice $GR(p, r) = GF(p^r)$ in the usual notation for Galois fields.

There are certain natural maps between the rings $GR(p^n, r)$ that are worth noting. For any positive integer d there is an inclusion of $GR(p^n, r)$ into $GR(p^n, dr)$. This can be proved using the uniqueness property and Galois theory just as for finite fields. Another map is the natural projection

$$h_n : GR(p^n, r) \to GR(p^{n-1}, r)$$

having kernel $p^{n-1} \cdot GR(p^n, r)$. (The map h_n depends also on r but we omit the additional subscript.) The collection $\{GR(p^n, r); h_n\}$ with r fixed, is an inverse mapping system and we can form the inverse limit, $D_p(r) = \operatorname{proj\,lim}\{GR(p^n, r); h_n\}$, of the system. One can show that $D_p(1)$ is the ring of p-adic integers and that $D_p(r)$ is the unique strongly separable extension of $D_p(1)$ with no proper idempotents and with rank r over $D_p(1)$. See [11, Theorem 3, p. 45] for further remarks about these rings. This construction suggests the following theorem.

THEOREM 4.6. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let R^* denote the completion of R. Then the strongly separable R^*-algebras*

without proper idempotents are in one to-one correspondence with the finite dimensional, separable field extensions of $R/\mathfrak{m}$.

Proof. Since $R/\mathfrak{m} \cong R^*/\mathfrak{m}R^*$, we may assume that R is complete. If E is a finite dimensional, separable field extension of $R/\mathfrak{m}$, then there is a separable polynomial $f(X)$ in $R[X]$ such that $E \cong R[X]/(\mathfrak{m},f)$. It is not difficult to verify that the R-algebra

$$D = \operatorname{proj\,lim}\{R[X]/(\mathfrak{m}^i,f)\}$$

is strongly separable, has no proper idempotents, and is isomorphic to $R[X]/(f)$.

On the other hand, if D is a strongly separable R-algebra with no proper idempotents, then $E = D/\mathfrak{m}D$ is a finite dimensional, separable field extension of $R/\mathfrak{m}$. Proceeding as above we associate a D' with E. In order to prove the theorem, it is sufficient to prove the following.

LEMMA 4.7. *Let* $f(X)$ *and* $g(X)$ *be separable polynomials over* R *which are irreducible modulo* $\mathfrak{m}$. *Suppose that* $R[X]/(\mathfrak{m},f)$ *is isomorphic to* $R[X]/(\mathfrak{m},g)$ *as* $R/\mathfrak{m}$*-algebras. Then* $R[X]/(f) \cong R[X]/(g)$ *as* R*-algebras.*

Proof. Let $D = R[X]/(f)$. The hypothesis implies D is a strongly separable R-algebra without proper idempotents. View f and g as polynomials over the complete local ring D. Because $D/\mathfrak{m}D \cong R[X]/(\mathfrak{m},g)$, we see that f and g have a common root in $D/\mathfrak{m}D$. We may apply Corollary 1 [13, p. 279] to conclude that there exist elements $\alpha_1, \alpha_2 \in D$ such that $f(\alpha_1) = g(\alpha_2) = 0$ and $\alpha_1 - \alpha_2 \in \mathfrak{m}D$. We have $D = R[\alpha_1]$. Since g is a separable polynomial, $R[\alpha_2]$ is a strongly separable subalgebra of D. By (1.5) D is strongly separable over $R[\alpha_2]$. Thus $R[a_2]$ is an R-direct summand of D. However $R[\alpha_2]$ and D have the same rank over R and so $D = R[\alpha_2]$. Clearly $R[\alpha_2] \cong R[X]/(g)$ so the proof is complete.

Notice that we obtain an alternate proof of (4.5) since any finite local ring is complete.

REMARK. $GR(p^n,r)$ defined above can be characterized abstractly as the only rings without proper idempotents that are of prime power characteristic and are separable over the subring generated by the identity element. More generally the only rings that are finitely generated and separable over the subring generated by the identity are those of the form $A \oplus B$ where A is the direct sum of a finite number of copies of the integers, and B is a direct sum of rings $GR(p^n,r)$ for various choices of p,n,r. The proof of this statement requires the fact that the only strongly separable Z-algebras are direct sums of copies of Z. The equivalent statement to be found in [12, p. 215], is there are no unramified extensions of the rational field. Regarding the equivalence of these notions see [6, p. 21, Remark (d)].

5. **An application.** In this section we apply the preceding theory to show

the existence of a separable splitting ring for group algebras of finite groups. We shall use the following terminology.

DEFINITION 6. Let G be a finite group and R a commutative ring such that the group algebra RG is separable over R. We call R a splitting ring for G in case RG is the direct sum of central separable R-algebras each equivalent to R in the Brauer group of R.

If R is a field with RG a separable group algebra then it is always possible to find a strongly separable (field) extension of R which is a splitting ring for G. In fact a well-known theorem of R. Brauer states that such a splitting ring can be obtained from R by adjoining a primitive nth root of unity where n is the exponent of G. When R is not a field, it is not known if a strongly separable extension of R can be found to split a given group. We can prove the following special case however.

THEOREM 5.1. *Let G be a finite group of exponent n and R a Noetherian regular domain such that RG is a separable R-algebra. Then the splitting ring of $X^n - 1$ is a regular domain which is strongly separable over R and is a splitting ring for G.*

We recall first that a regular domain is an integral domain of finite global dimension. For properties of regular domains see [10] and [2] along with the references given there.

Proof. Since RG is separable over R, we know $n \cdot 1$ is invertible in R [9, Theorem 12]. Hence by (2.4) $X^n - 1$ is a separable polynomial. By (2.2), part (2), and (2.6) we know $X^n - 1$ has a splitting ring, S, which is a Galois extension of R (and hence is strongly separable over R) and has no proper idempotents. By (4.2) S is a domain and S must be a regular domain since it is separable over a regular domain. Let K denote the quotient field of S. The Brauer theorem mentioned above implies K is a splitting ring for G. That is KG is the direct sum of central separable K-algebras each equivalent to K in the Brauer group, $B(K)$, of K. Theorem 7.2 of [2] states that the map from $B(S)$ to $B(K)$ induced by the inclusion of S into K is a monomorphism. Thus SG is the direct sum of central separable S-algebras each equivalent to S in $B(S)$. That is S is a splitting ring for G.

REMARKS. (1) If G is an abelian group and R any commutative ring with no proper idempotents such that RG is a separable R-algebra then the remark (2) at the end of §1 shows the existence of a strongly separable R-algebra that is a splitting ring for G. Again one can show that the splitting ring of $X^n - 1$ will be a splitting ring for G, $n =$ exponent of G.

(2) If R is any commutative ring such that R is a splitting ring for G, an application of the Morita theorems [3] shows that the category of left RG-modules is isomorphic to the category

$$ {}_RM \times {}_RM \times \cdots \times {}_RM $$

(the category of left R-modules crossed with itself m times where $m =$ number of conjugate classes in G). The RG-modules are all of the form

$$ (P_1 \otimes X_1) \oplus \cdots \oplus (P_m \otimes X_m) $$

where the X_i are suitable R-modules and the P_i are fixed projective, finitely generated, RG-modules viewed also as right R-modules. The projective RG-modules P_i are determined uniquely up to change by an element in the class group of R. That is the only other choice for some P_i is a module of the form $P_i \otimes Y$ where Y is a rank one projective R-module.

BIBLIOGRAPHY

1. M. Auslander and D. Buchsbaum, *On ramification theory in Noetherian rings*, Amer. J. Math. **81** (1959), 749–765.

2. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

3. H. Bass, *The Morita theorems*, Mimeographed notes, University of Oregon, Eugene, 1962.

4. N. Bourbaki, *Algèbre commutative*, Hermann, Paris, 1961.

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

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

7. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

8. S. Eilenberg and N. Steenrod, *Foundations of algebraic topology*, Princeton Univ. Press, Princeton, N. J., 1952.

9. S. Eilenberg and T. Nakayama, *On the dimension of modules and algebras*. II, Nagoya Math. J. **9** (1955), 1–16.

10. D. G. Northcott, *Introduction to homological algebra*, Cambridge Univ. Press, London, 1960.

11. J.-P. Serre, *Corps locaux*, Actualités Sci. Ind. No. 1296, Hermann, Paris, 1962.

12. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

13. O. Zariski and P. Samuel, *Commutative algebra*. I, II, Van Nostrand, New York, 1960.

UNIVERSITY OF OREGON,
EUGENE, OREGON
THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, NEW JERSEY