

THE BRAUER GROUP OF A COMMUTATIVE RING

BY

MAURICE AUSLANDER AND OSCAR GOLDMAN⁽¹⁾

Introduction. This paper contains the foundations of a general theory of separable algebras over arbitrary commutative rings. Of the various equivalent conditions for separability in the classical theory of algebras over a field, there is one which is most suitable for generalization; we say that an algebra Λ over a commutative ring R is separable if Λ is a projective module over its enveloping algebra $\Lambda^e = \Lambda \otimes_R \Lambda^0$.

The basic properties of separable algebras are developed in the first three sections. The results obtained show that a considerable portion of the classical theory is preserved in our generalization. For example, it is proved that separability is maintained under tensor products as well as under the formation of factor rings. Furthermore, an R -algebra Λ is separable over R if, and only if, Λ is separable over its center C and C is separable over R . This fact shows that the study of separability can be split into two parts: commutative algebras and central algebras. The purely commutative situation has been studied to some extent by Auslander and Buchsbaum in [1]. The present investigation is largely concerned with central algebras. In the classical case, an algebra which is separable over a field K , and has K for its center, is simple. One cannot expect this if the center is not a field; however, if Λ is central separable over R , then the two-sided ideals of Λ are all generated by ideals of R .

In the fourth section we consider a different aspect of the subject, one which is more analogous to ramification theory. If Λ is an algebra over a ring R , the homological different $\mathfrak{S}(\Lambda/R)$ is an ideal in the center C of Λ which essentially describes the circumstances under which $\Lambda \otimes_R R_{\mathfrak{p}}$ is separable over $R_{\mathfrak{p}}$, when $\mathfrak{p}$ is a prime ideal of R . (Suitable finiteness conditions must be imposed in the statement of these theorems.) The general question of ramification in noncommutative algebras is only touched on in the present paper; various arithmetic applications will be treated in another publication.

In the classical theory of central simple algebras, the full matrix algebras have a special significance. The proper analogue of the full matrix algebra in the present context is the endomorphism ring $\text{Hom}_R(E, E)$ of a finitely generated projective R -module E . It is easy to show for such a module E that $\text{Hom}_R(E, E)$ is separable over R , and central if E is faithful. By analogy with the classical theory, we introduce an equivalence relation between central separable algebras over a ring R , under which the equivalence classes form

Received by the editors March 16, 1960.

⁽¹⁾ This work was carried out under a grant from the National Science Foundation.

an abelian group, the Brauer group $\mathfrak{B}(R)$ of R . Explicitly, the equivalence relation is the following: if Λ_1 and Λ_2 are central separable over R , then $\Lambda_1 \sim \Lambda_2$ if there exist finitely generated projective faithful R -modules E_1, E_2 so that $\Lambda_1 \otimes_R \text{Hom}_R(E_1, E_1) \cong \Lambda_2 \otimes_R \text{Hom}_R(E_2, E_2)$. The multiplication in $\mathfrak{B}(R)$ is induced by the tensor product of the algebras. The fact that $\mathfrak{B}(R)$ is a group depends on the following result proved in §2: if Λ is a central separable algebra over R , then Λ is a finitely generated projective R -module, and $\Lambda^e = \Lambda \otimes_R \Lambda^0$ is naturally isomorphic to the endomorphism ring, $\text{Hom}_R(\Lambda, \Lambda)$, of Λ over R .

It has been pointed out to the authors that Azumaya in [3] anticipated some of the results dealing with the formal properties of separable algebras and the Brauer Group of rings mentioned thus far. Since, in effect, Azumaya's definition of a maximally central algebra is a local version of what we call a central separable algebra, some of our results can be obtained from his by standard "localization" procedures. However, since our somewhat different point of view leads naturally to its own form of proof, we have presented these proofs even in those cases where the result can be deduced from Azumaya's results.

A ring homomorphism $f: R \rightarrow S$ induces a group homomorphism $f_*: \mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$. Some special cases of this homomorphism discussed in §§6 and 7 are the following: if R is a complete local ring with maximal ideal $\mathfrak{m}$, then the canonical homomorphism $R \rightarrow R/\mathfrak{m}$ induces an isomorphism $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R/\mathfrak{m})$; if R is a regular domain with quotient field K , then the imbedding $R \rightarrow K$ induces a monomorphism $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$. An example is given of an integral domain R with quotient field K for which the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is not a monomorphism. It would be interesting to know under what circumstances the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is in fact a monomorphism. To mention another special case, if k is a field, the map $\mathfrak{B}(k) \rightarrow \mathfrak{B}(k[x])$, arising from $k \rightarrow k[x]$, is an isomorphism if, and only if, k is perfect. (Rosenberg and Zelinsky have recently given another proof of this result by means of the Amitsur complex.)

A lengthy appendix contains a Galois theory of commutative rings as well as a theory of crossed-products relating $\mathfrak{B}(R)$ with the Galois cohomology of R . Under suitable restrictions, if S is a Galois extension of R relative to a group of automorphisms G , then the sequence $(1) \rightarrow H^2(G, U(S)) \rightarrow \mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$ is exact. ($U(S)$ is the group of units of S .) There are several applications of this theorem in the body of the paper.

Since this paper presents the foundations of the theory, we have not included any of its applications. There are a number of interesting applications, especially to algebraic number theory, which will be presented in other publications.

1. Formal properties of separable algebras. Throughout this paper we assume that all rings have units, that all modules are unitary, and that all ring homomorphisms carry the unit into the unit.

From now on R will denote generically a commutative ring. A ring Λ together with a (ring) homomorphism of R into the center of Λ will be called an R -algebra. We denote by Λ^0 the *opposite* ring of Λ (i.e. Λ^0 consists of a set in one-to-one correspondence with Λ , the correspondence being indicated by $x \rightarrow x^0$, with addition being defined by $x^0 + y^0 = (x + y)^0$ and multiplication by $x^0 y^0 = (yx)^0$). It is clear that Λ^0 is an R -algebra in a natural way. Now if M is a two-sided Λ -module, and we assume that the operations of R are the same on both sides, then this module structure can be described by means of the *enveloping* algebra $\Lambda^e = \Lambda \otimes_R \Lambda^0$ of Λ over R in the following way. We consider M a left Λ^e -module by means of $(x \otimes y^0)m = xmy$. It is easily seen that this establishes a natural one-to-one correspondence between the two-sided Λ -modules and the left Λ^e -modules which allows us to use these concepts interchangeably.

In particular, Λ is a two-sided Λ -module and thus a left Λ^e -module, the operation being given by $(x \otimes y^0)(z) = xzy$. We say that Λ is a *separable R -algebra* if and only if Λ is a projective Λ^e -module. The rest of this section is devoted to establishing some of the more formal properties of separable algebras.

In general there is a Λ^e -epimorphism $\phi: \Lambda^e \rightarrow \Lambda$ defined by $\phi(x \otimes y^0) = xy$. The kernel of ϕ , which we denote by J , is a left ideal in Λ^e which is generated as a left ideal by the elements of the form $x \otimes 1 - 1 \otimes x^0$. Now suppose M is a two-sided Λ -module and M^Δ the R -submodule of M consisting of all m in M such that $xm = mx$ for all x in Λ . Since $\phi: \Lambda^e \rightarrow \Lambda$ induces an isomorphism $\Lambda^e/J \cong \Lambda$, it is easily seen that the map of $\text{Hom}_{\Lambda^e}(\Lambda, M) \rightarrow M$ given by $f \rightarrow f(1)$ induces an isomorphism of $\text{Hom}_{\Lambda^e}(\Lambda, M)$ with M^Δ which we will consider an identification. For instance, we have that $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e)$ is the right annihilator of J in Λ^e which we denote by A and $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda)$ is the center of Λ which we denote by C .

Now Λ is Λ^e -projective if and only if the exact sequence $0 \rightarrow J \rightarrow \Lambda^e \xrightarrow{\phi} \Lambda \rightarrow 0$ splits. And this sequence splits if and only if there is a Λ^e -homomorphism $\Lambda \rightarrow \Lambda^e$ such that $\Lambda \rightarrow \Lambda^e \xrightarrow{\phi} \Lambda$ is the identity on Λ . From this it follows that Λ is Λ^e -projective if and only if $\phi: \Lambda^e \rightarrow \Lambda$ induces an epimorphism $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e) \rightarrow \text{Hom}_{\Lambda^e}(\Lambda, \Lambda) \rightarrow 0$. Thus identifying $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e)$ with A and $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda)$ with C , we have:

PROPOSITION 1.1. *A necessary and sufficient condition for Λ to be R -separable is that $\phi(A) = C$.*

It should be noted that A being the right annihilator of J is a right ideal in Λ^e and that $\phi(A)$ is an ideal in C .

Since the operation of Λ^e on Λ commutes with the operation of the center C on Λ we have a ring map $\eta: \Lambda^e \rightarrow \text{Hom}_C(\Lambda, \Lambda)$ given by $\eta(x \otimes y^0)(z) = xzy$. The homomorphisms ϕ and η are related through the following commutative diagram

$$\begin{array}{ccc}
 \Lambda^e & \xrightarrow{\eta} & \text{Hom}_C(\Lambda, \Lambda) \\
 \phi \searrow & & \swarrow \phi_0 \\
 & \Lambda &
 \end{array}$$

where ϕ_0 is defined by $\phi_0(\omega) = \omega(1)$ for all ω in $\text{Hom}_C(\Lambda, \Lambda)$. It is clear that J is the set of all y in Λ^e such that $\eta(y)$ as an element of $\text{Hom}_C(\Lambda, \Lambda)$ maps 1 on 0. It is also clear that if x is in A , then $\eta(x)$ is in the submodule $\text{Hom}_C(\Lambda, C)$ of $\text{Hom}_C(\Lambda, \Lambda)$.

PROPOSITION 1.2. *If Λ is separable over R then, considering Λ as a C -module, we have that C is a direct summand of Λ .*

Proof. Let $\alpha \in A$, with $\phi(\alpha) = 1$. Put $f = \eta(\alpha)$. Then, because $\alpha \in A$, we have $f \in \text{Hom}_C(\Lambda, C)$. Since $\phi(\alpha) = 1$, we have $f(1) = 1$. Thus, f maps Λ onto C and leaves fixed the elements of C . It follows that C is a C -direct summand of Λ .

COROLLARY 1.3. *If Λ is R -separable and a is an ideal in C , then $a\Lambda \cap C = a$.*

Proof. The result follows easily from the fact that C is a C -direct summand of Λ .

PROPOSITION 1.4. *Let Λ and Γ be R -algebras and $f: \Lambda \rightarrow \Gamma$ an R -algebra epimorphism. If Λ is separable over R , then Γ is also separable over R and the center of Γ is $f(C)$ where C is the center of Λ .*

Proof. We first observe that the epimorphism $f: \Lambda \rightarrow \Gamma$ induces an epimorphism of R -algebras $f^*: \Lambda^e \rightarrow \Gamma^e$ defined by $f^*(x \otimes y^0) = f(x) \otimes f(y)^0$. Now if M is a two-sided Γ -module, then it can also be considered a two-sided Λ -module. Since f is an epimorphism, we have that $M^\Lambda = M^\Gamma$.

If we define $\alpha: \text{Hom}_{\Gamma^e}(\Gamma, M) \rightarrow \text{Hom}_{\Lambda^e}(\Lambda, M)$ by $\alpha(h)(y) = h(f(y))$ for all h in $\text{Hom}_{\Gamma^e}(\Gamma, M)$ and y in Λ , we have a commutative diagram

$$\begin{array}{ccc}
 \text{Hom}_{\Gamma^e}(\Gamma, M) & \xrightarrow{\alpha} & \text{Hom}_{\Lambda^e}(\Lambda, M) \\
 \downarrow & & \downarrow \\
 M^\Gamma & = & M^\Lambda
 \end{array}$$

where the vertical isomorphisms are the standard identifications. Thus α is an isomorphism. Now the map $\Gamma^e \rightarrow \Gamma \rightarrow 0$ induces the commutative diagram

$$\begin{array}{ccc}
 \text{Hom}_{\Gamma^e}(\Gamma, \Gamma^e) & \rightarrow & \text{Hom}_{\Gamma^e}(\Gamma, \Gamma) \\
 \downarrow \alpha & & \downarrow \alpha \\
 \text{Hom}_{\Lambda^e}(\Lambda, \Gamma^e) & \rightarrow & \text{Hom}_{\Lambda^e}(\Lambda, \Gamma) \rightarrow 0
 \end{array}$$

with the bottom row exact since Λ is Λ^e -projective. Thus the top map is an epimorphism which means that Γ is R -separable.

Also since Λ is Λ^e -projective, we have that the epimorphism $f: \Lambda \rightarrow \Gamma$ induces the epimorphism $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda) \rightarrow \text{Hom}_{\Lambda^e}(\Lambda, \Gamma)$. But $\text{Hom}_{\Lambda^e}(\Lambda, \Gamma) = \text{Hom}_{\Gamma^e}(\Gamma, \Gamma)$ which is the center of Γ . Thus if C is the center of Λ , we have that $f(C)$ is the center of Γ .

PROPOSITION 1.5. *Suppose that R_1 and R_2 are commutative R -algebras. Λ_1 is a separable R_1 -algebra while Λ_2 is a separable R_2 -algebra. Then $\Lambda_1 \otimes_R \Lambda_2$ is either 0 or a separable $R_1 \otimes_R R_2$ -algebra. Furthermore the center of $\Lambda_1 \otimes_R \Lambda_2$ is equal to $C_1 \otimes_R C_2$ where C_i is the center of Λ_i .*

Proof. Set $\Gamma = \Lambda_1 \otimes_R \Lambda_2$. Then, it is immediate that $\Gamma^e = \Gamma \otimes_{R_1 \otimes_R R_2} \Gamma^0 = \Lambda_1^e \otimes_R \Lambda_2^e$ where $\Lambda_i^e = \Lambda_i \otimes_{R_i} \Lambda_i^0$. Because the maps $\phi_i: \Lambda_i^e \rightarrow \Lambda_i$ split, it is clear that the map $\phi: \Gamma^e \rightarrow \Gamma$ also splits, so that Γ is a separable $R_1 \otimes_R R_2$ -algebra. In particular, if g_i is an inverse to ϕ_i , then $g = g_1 \otimes_R g_2$ is an inverse to ϕ . But then we have $C_i = \phi_i(g_i(1)\Lambda_i^e)$, so that the center of Γ is $\phi(g(1)\Gamma^e) = C_1 \otimes_R C_2$.

As a special case, we have:

COROLLARY 1.6. *If Λ is a separable R -algebra and S is a commutative R -algebra then $\Lambda \otimes_R S$ is a separable S -algebra and the center of $\Lambda \otimes_R S$ is $C \otimes_R S$, C being the center of Λ .*

A theorem of a somewhat different nature about separable algebras is the following.

PROPOSITION 1.7. *Suppose that Λ and Γ are R -algebras such that $\Lambda \otimes_R \Gamma$ is separable over R . If Λ is a projective R -module having R as a direct summand (over R), then Γ is separable over R . (See Proposition 2(7) of [5].)*

Proof. Since Λ is a projective R -module, Λ^e is also a projective R -module, so that $(\Lambda \otimes_R \Gamma)^e \cong \Lambda^e \otimes_R \Gamma^e$ is a projective Γ^e -module. But $\Lambda \otimes_R \Gamma$ is a projective $(\Lambda \otimes_R \Gamma)^e$ -module, hence $\Lambda \otimes_R \Gamma$ is a projective Γ^e -module.

Because R is an R -direct summand of Λ , Γ is a Γ^e -direct summand of $\Lambda \otimes_R \Gamma$. Combining this with the previous observation, we find that Γ is a projective Γ^e -module, i.e., Γ is separable over R .

REMARK. Using an argument similar to that of Lemma 4.7 of [1], one can prove that if Λ is an R -algebra which contains R and is a finitely generated projective R -module, then R is an R -direct summand of Λ .

THEOREM 1.8. *Let Ω be a separable R -algebra which is projective as an R -module, and let Δ be an R -algebra. If E is an $\Omega \otimes_R \Delta$ -module, then $\text{pd}_{\Omega \otimes_R \Delta}(E) \leq \text{pd}_{\Delta}(E)$ and thus $\text{l.gl. dim}(\Omega \otimes_R \Delta) \leq \text{l.gl. dim}(\Delta)$.*

Proof. Let A and B be left $\Omega \otimes_R \Delta$ -modules. Then clearly $\text{Hom}_{\Omega \otimes_R \Delta}(A, B) \subset \text{Hom}_{\Delta}(A, B)$. We consider $\text{Hom}_{\Delta}(A, B)$ as an Ω^e -module as follows: if $\omega_1 \otimes \omega_2^0 \in \Omega^e$ and $f \in \text{Hom}_{\Delta}(A, B)$ we define $(\omega_1 \otimes \omega_2^0)f(a) = \omega_1 f(\omega_2 a)$. Obviously, a necessary and sufficient condition for an element $f \in \text{Hom}_{\Delta}(A, B)$ to be in $\text{Hom}_{\Omega \otimes_R \Delta}(A, B)$ is that $Jf = 0$, where J is the kernel of $\phi: \Omega^e \rightarrow \Omega$. Since an ele-

ment $g \in \text{Hom}_{R^e}(\Omega, \text{Hom}_\Delta(A, B))$ is completely determined by $g(1)$ and the set of values of $g(1)$ is exactly the annihilator of J in $\text{Hom}_\Delta(A, B)$, it follows that $\text{Hom}_{R^e}(\Omega, \text{Hom}_\Delta(A, B))$ is naturally isomorphic to $\text{Hom}_{\Omega \otimes \Delta}(A, B)$.

Let X be an $\Omega \otimes \Delta$ -projective resolution of E . We have the identity $\text{Hom}_{R^e}(\Omega, \text{Hom}_\Delta(X, B)) \cong \text{Hom}_{\Omega \otimes \Delta}(X, B)$, for any $\Omega \otimes \Delta$ -module B . Since Ω is Ω^e -projective, passing to homology, we have the isomorphism,

$$\text{Hom}_{R^e}(\Omega, H(\text{Hom}_\Delta(X, B))) \cong \text{Ext}_{\Omega \otimes \Delta}(E, B).$$

From the fact that Ω is R -projective we deduce that $\Omega \otimes \Delta$ is Δ -projective and hence that X is a Δ -projective resolution of B . Therefore,

$$\text{Hom}_{R^e}(\Omega, \text{Ext}_\Delta^i(E, B)) \cong \text{Ext}_{\Omega \otimes \Delta}^i(E, B),$$

which gives the desired result.

This theorem may also be deduced from a standard spectral sequence (see (5) on p. 346 of [4], or Proposition 2 of [5]).

2. Various criteria for separability. Except for the last theorem, this section is concerned with Λ as an algebra over its center C . It is understood that such objects as Λ^e and η , etc., are formed over C .

The primary purpose of this section is to establish:

THEOREM 2.1. *If Λ is considered as an algebra over its center C , then the following statements are equivalent:*

- (a) Λ is a separable C -algebra.
- (b) $\Lambda^e A = \Lambda^e$, where $A = \text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e) = (\Lambda^e)^\Lambda$.
- (c) The map $\eta: \Lambda^e \rightarrow \text{Hom}_C(\Lambda, \Lambda)$ is an isomorphism and Λ is a finitely generated projective C -module.
- (d) The map $\eta: \Lambda^e \rightarrow \text{Hom}_C(\Lambda, \Lambda)$ is an isomorphism and C is a direct summand of Λ when Λ is considered a C -module.

REMARK. It should be observed that statement (c) is the definition of a maximally central algebra given by Azumaya in [3], provided one assumes that Λ is C -free not just projective. Thus every maximally central algebra is separable over its center.

Proof. (a) $\Rightarrow$ (b). In order to prove that (a) $\Rightarrow$ (b) we shall first establish the following fact which is a special case of a more general theorem to be proved later (see Corollary 3.2): If Λ is separable over its center C and $\mathfrak{I}$ is a maximal two-sided ideal in Λ , then $\mathfrak{I} = \alpha\Lambda$ with α a proper ideal of C . For, let $\alpha = \mathfrak{I} \cap C$. Then $\mathfrak{I}_0 = \alpha\Lambda$ is contained in $\mathfrak{I}$ and $\mathfrak{I}_0 \cap C = \alpha$ by Corollary 1.3. Since Λ is C -separable, it follows that $\Lambda/\mathfrak{I}_0$ is C -separable with center C/α and is thus C/α -separable. In $\Lambda/\mathfrak{I}_0$ the ideal $\mathfrak{I}/\mathfrak{I}_0$ is a maximal two-sided ideal whose intersection with the center C/α is 0. Hence $\Lambda/\mathfrak{I} \cong \Lambda/\mathfrak{I}_0 / \mathfrak{I}/\mathfrak{I}_0$ is C/α -separable with C/α as its center. Since C/α is the center of the simple ring $\Lambda/\mathfrak{I}$, it follows that C/α is a field. But $\Lambda/\mathfrak{I}_0$ is a separable algebra over

its center $C/\mathfrak{a}$ which is a field. Thus we have that the Hochschild homological dimension of the $C/\mathfrak{a}$ -algebra $\Lambda/\mathfrak{Z}_0$ is zero. Because $C/\mathfrak{a}$ is a field, it follows that $\Lambda/\mathfrak{Z}_0$ is semi-simple with minimum condition. (See [4, Chapter IX, Proposition 7.6].) Since $\Lambda/\mathfrak{Z}_0$ is semi-simple with its center a field we have that $\Lambda/\mathfrak{Z}_0$ is simple, which shows that $\mathfrak{a}\Lambda = \mathfrak{Z}_0 = \mathfrak{Z}$.

Now suppose that $\Lambda^e A \neq \Lambda^e$. Since Λ is C -separable we have that Λ^e is C -separable and thus Λ^e is C -separable with center C . Therefore $\Lambda^e A$ being a proper ideal in Λ^e , we have that $\Lambda^e A \subset \mathfrak{a}\Lambda^e$ where $\mathfrak{a}$ is a proper ideal in C . But $\phi(\Lambda^e A) = \Lambda\phi(A) = \Lambda$, since Λ is C -separable, so that $\mathfrak{a}\Lambda = \Lambda$. This is impossible since $\mathfrak{a}\Lambda \cap C = \mathfrak{a}$ (see Corollary 1.3). Thus $\Lambda^e A = \Lambda^e$.

(b) $\Rightarrow$ (c). We prove this implication by applying Theorem A.2 of the Appendix to [2]. As observed previously C , the center of Λ , is $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda)$. Thus we have the following diagram:

$$\begin{array}{ccc} \text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e) \otimes_C \Lambda & \xrightarrow{\psi \otimes 1} & \text{Hom}_C(\Lambda, C) \otimes_C \Lambda \\ \downarrow \tau & & \downarrow \mu \\ \Lambda^e & \xrightarrow{\eta} & \text{Hom}_C(\Lambda, \Lambda), \end{array}$$

where $\tau(f \otimes x) = f(x)$ for all f in $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e)$ and x in Λ , where $\psi: \text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e) \rightarrow \text{Hom}_C(\Lambda, C)$ is defined by $\psi(f) = \eta(f(1))$, [note that $f(1)$ is in A , thus $\eta(f(1))$ is in $\text{Hom}_C(\Lambda, C)$], and μ is defined by $\mu(g \otimes x)(y) = g(y)x$ for all g in $\text{Hom}_C(\Lambda, C)$, x and y in Λ . Therefore we are in the position described in Theorem A.2 of [2] and we can conclude that η is an isomorphism and Λ is a finitely generated projective C -module if we show that $\text{Im } \tau = \mathfrak{T}_{\Lambda^e}(\Lambda) = \Lambda^e$. Since $\text{Hom}_{\Lambda^e}(\Lambda, \Lambda^e) = A$, it is easily seen that $\mathfrak{T}_{\Lambda^e}(\Lambda)$ is precisely the two-sided ideal generated by A in Λ^e [i.e., $\mathfrak{T}_{\Lambda^e}(\Lambda) = \Lambda^e A$] which is Λ^e by hypothesis. Therefore we have shown that (b) $\Rightarrow$ (c).

Before showing that (c) $\Rightarrow$ (d) $\Rightarrow$ (a), we prove the following proposition from which these implications will follow easily.

PROPOSITION 2.2. *Let Λ be a ring with center C and let J be the kernel of the epimorphism $\phi_0: \text{Hom}_C(\Lambda, \Lambda) \rightarrow \Lambda$ defined by $\phi_0(\omega) = \omega(1)$. Then the right annihilator of J in $\text{Hom}_C(\Lambda, \Lambda)$ is $\text{Hom}_C(\Lambda, C)$ and Λ is a projective $\text{Hom}_C(\Lambda, \Lambda)$ -module if, and only if, C is a C -direct summand of Λ .*

Proof. It is clear that J consists precisely of those ω in $\text{Hom}_C(\Lambda, \Lambda)$ such that $\omega(C) = 0$. Therefore it is also clear that $J \text{Hom}_C(\Lambda, C) = 0$. Suppose ω is in $\text{Hom}_C(\Lambda, \Lambda)$ and there is an x in $\omega(\Lambda)$ which is not in C . Since x is not in C , there is a y in Λ such that $yx - xy \neq 0$. Define g in $\text{Hom}_C(\Lambda, \Lambda)$ by $g(z) = yz - zy$. Then g is in J and $g\omega \neq 0$. Thus the right annihilator of J is precisely $\text{Hom}_C(\Lambda, C)$.

Now if Λ is $\text{Hom}_C(\Lambda, \Lambda)$ -projective, then J is a direct summand of $\text{Hom}_C(\Lambda, \Lambda)$. Thus there is an ω in J such that $\omega^2 = \omega$ and $J = \text{Hom}_C(\Lambda, \Lambda)\omega$.

Since $\text{Hom}_C(\Lambda, \Lambda)\omega(1-\omega)=0$, we have that $1-\omega$ is in $\text{Hom}_C(\Lambda, C)$ and $(1-\omega)(c)=c$ for all c in C . Thus C is a C -direct summand of Λ .

On the other hand, if C is a C -direct summand of Λ there is a map ω in $\text{Hom}_C(\Lambda, C)$ such that $\omega(c)=c$ for each c in C . Define the $\text{Hom}_C(\Lambda, \Lambda)$ -map $j: \Lambda \rightarrow \text{Hom}_C(\Lambda, \Lambda)$ by $j(x)(z)=x\omega(z)$ for all z in Λ . Then it is clear that $\phi_0 j$ is the identity on Λ . Thus Λ is a projective $\text{Hom}_C(\Lambda, \Lambda)$ -module.

Now we return to showing that (c) $\Rightarrow$ (d). By the hypothesis in (c) we know that Λ is a finitely generated projective C -module. Therefore we know by Proposition A.3 of [2] that Λ is a projective $\text{Hom}_C(\Lambda, \Lambda)$ -module. Thus by the above we know that C is a C -direct summand of Λ , which shows that (c) $\Rightarrow$ (d).

(d) $\Rightarrow$ (a). Since the diagram

$$\begin{array}{ccc} \Lambda^e & \xrightarrow{\eta} & \text{Hom}_C(\Lambda, \Lambda) \\ \phi \searrow & & \swarrow \phi_0 \\ & \Lambda & \end{array}$$

commutes and we are assuming that η is an isomorphism, in order to show that Λ is Λ^e -projective it suffices to show that Λ is $\text{Hom}_C(\Lambda, \Lambda)$ -projective. But this follows from Proposition 2.2 since we are also assuming that C is a C -direct summand of Λ . Thus the full circle of implications has been established, proving Theorem 2.1.

THEOREM 2.3. *If Λ is an R -algebra [R not necessarily the center of Λ], then Λ is separable over R if, and only if, Λ is separable over its center C and C is separable over R . (See Proposition 3 of [5].)*

Proof. Suppose first that Λ is separable over R . Since we always have an epimorphism $\Lambda \otimes_R \Lambda^0 \rightarrow \Lambda \otimes_C \Lambda^0$ whose kernel annihilates Λ , the fact that Λ is $\Lambda \otimes_R \Lambda^0$ -projective implies that Λ is $\Lambda \otimes_C \Lambda^0$ -projective. Thus Λ is a separable C -algebra.

By Theorem 2.1, Λ is projective over C , hence $\Lambda \otimes_R \Lambda^0$ is projective over $C \otimes_R C$. But C is a C -direct summand of Λ and thus also a $C \otimes_R C$ -direct summand of Λ^e . This shows that C is projective over $C \otimes_R C$ or that C is R -separable.

Suppose that C is separable over R and Λ is separable over C . Now the sequence $0 \rightarrow J_0 \rightarrow C \otimes_R C \rightarrow C \rightarrow 0$ splits over $C \otimes_R C$. If we tensor each term of the sequence with $\Lambda \otimes_R \Lambda^0$ over $C \otimes_R C$, the sequence which results will split over $\Lambda \otimes_R \Lambda^0$. We get then

$$0 \rightarrow J_1 \rightarrow \Lambda \otimes_R \Lambda^0 \rightarrow (\Lambda \otimes_R \Lambda^0) \otimes_{C \otimes_R C} C \rightarrow 0.$$

Now by Chapter IX, Proposition 2.1 of [4] we know that $(\Lambda \otimes_R \Lambda^0) \otimes_{C \otimes_R C} C$ is isomorphic to $\Lambda \otimes_C \Lambda^0$ as $\Lambda \otimes_C \Lambda^0$ -modules. Thus $\Lambda \otimes_C \Lambda^0$ is projective over $\Lambda \otimes_R \Lambda^0$. Combining this with the fact that Λ is projective over $\Lambda \otimes_C \Lambda^0$ it follows that Λ is projective over $\Lambda \otimes_R \Lambda^0$. Thus Λ is R -separable.

3. Two-sided modules over a separable algebra. Combining the results of the previous section with the information about modules over the ring of endomorphisms of a projective module contained in the appendix of [2], we obtain a description of the two-sided modules over an algebra which is central separable (i.e., separable over its center).

Suppose Λ is a ring with center C and M a two-sided Λ -module or equivalently a left Λ^e -module. We have already identified $\text{Hom}_{\Lambda^e}(\Lambda, M)$ with M^A , the set of m in M such that $xm = mx$ for all x in Λ . It should be observed that M^A is a C -submodule of M but not in general a Λ -submodule of M . We have a natural map $g: \Lambda \otimes_C M^A \rightarrow M$ defined by $g(x \otimes m) = xm$. Since we consider $\Lambda \otimes_C M^A$ a Λ^e -module by means of the operations of Λ^e on Λ , it is easily seen that g is a Λ^e -homomorphism.

THEOREM 3.1. *Let C be the center of Λ . Then the following statements are equivalent:*

- (a) Λ is separable over C .
- (b) The map $g: \Lambda \otimes_C (\Lambda^e)^A \rightarrow \Lambda^e$ is an epimorphism.
- (c) For every Λ^e -module M , the map $g: \Lambda \otimes_C M^A \rightarrow M$ is an isomorphism.

Proof. We first observe that the image of $g: \Lambda \otimes_C (\Lambda^e)^A \rightarrow \Lambda^e$ is $\Lambda^e A$. Since Λ is separable over C if and only if $\Lambda^e A = \Lambda^e$ (Theorem 2.1) it follows that (a) and (b) are equivalent. Since (c) obviously implies (b), we need only show that (a) implies (c).

If Λ is separable over C , then by Theorem 2.1 we know that Λ is a finitely generated projective C -module. It is clear that Λ is also a faithful C -module. Therefore Proposition A.6 of [2] can be applied to $\Omega = \text{Hom}_C(\Lambda, \Lambda)$. Thus we have that if M is a left Λ^e -module, then $h: \Lambda \otimes_C \text{Hom}_{\Lambda^e}(\Lambda, M) \rightarrow M$, defined by $h(x \otimes f) = f(x)$ for all x in Λ and f in $\text{Hom}_{\Lambda^e}(\Lambda, M)$, is an isomorphism. Since Λ is C -separable, we know that $\Lambda^e = \text{Hom}_C(\Lambda, \Lambda)$. (See Theorem 2.1.) Now $g: \Lambda \otimes_C \text{Hom}_{\Lambda^e}(\Lambda, M) \rightarrow M$ can be described by $g(x \otimes f) = f(x) = (x \otimes 1)f(1) = xf(1)$. Identifying $\text{Hom}_{\Lambda^e}(\Lambda, M)$ with M^A , we obtain the desired isomorphism, which shows that (a) implies (c).

COROLLARY 3.2. *If Λ is separable over its center C , then there is a one-to-one correspondence between ideals of C and the two-sided ideals of Λ . Every two-sided ideal of Λ has the form $\mathfrak{b}\Lambda$ with $\mathfrak{b}$ an ideal of C and $\mathfrak{b}\Lambda \cap C = \mathfrak{b}$.*

Proof. Let $\mathfrak{J}$ be a two-sided ideal of Λ . Then it is easily seen that $\mathfrak{J}^A = \mathfrak{J} \cap C$. If we denote this ideal by $\mathfrak{b}$, the theorem shows that $\mathfrak{J} = \mathfrak{b}\Lambda$. Since $\mathfrak{b}\Lambda \cap C = \mathfrak{b}$ for any ideal $\mathfrak{b}$ in C , we have the desired one-to-one correspondence and the corollary is proved.

Let Γ be a ring having center C and let Λ be a C -subalgebra of Γ . Then Γ may be considered a two-sided Λ -module. It is easily seen that Γ^A is a subring of Γ which is called the *commutant* of Λ in Γ .

THEOREM 3.3. *Let Γ be a ring with center C and Λ a subring of Γ having C for its center and separable over C . Then $g: \Lambda \otimes_C \Gamma^\Lambda \rightarrow \Gamma$ is an algebra isomorphism and Γ^Λ has center C . If in addition Γ is C -separable, then Γ^Λ is C -separable and the commutant of Γ^Λ in Γ is Λ .*

Proof. By Theorem 3.1 the map $g: \Lambda \otimes_C \Gamma^\Lambda \rightarrow \Gamma$ given by $g(x \otimes y) = xy$ (where x is in Λ and y is in Γ^Λ) is an isomorphism. It is clearly an algebra map. Since every element of the center of Γ^Λ commutes with Γ , we see that the center of Γ^Λ is C .

Assume now that Γ is C -separable. Since Λ is C -separable we know that Λ is a finitely generated projective C -module and C is a C -direct summand of Λ . Thus it follows from Proposition 1.7 that Γ^Λ is C -separable since $\Gamma \cong \Lambda \otimes_C \Gamma^\Lambda$. Let Λ' be the commutant of Γ^Λ in Γ . It is clear that $\Lambda \subset \Lambda'$. Applying to Γ^Λ what we have proven, we find that $\Lambda' \otimes_C \Gamma^\Lambda$ is isomorphic with Γ . Hence tensoring the exact sequence $0 \rightarrow \Lambda \rightarrow \Lambda' \rightarrow \Lambda'/\Lambda \rightarrow 0$ with Γ^Λ over C , we obtain $\Lambda'/\Lambda \otimes_C \Gamma^\Lambda = 0$. Since Γ^Λ is central separable over C , it follows that C is a direct summand of Γ^Λ , and therefore that Λ'/Λ is a direct summand of $\Lambda'/\Lambda \otimes_C \Gamma^\Lambda = 0$. Thus $\Lambda = \Lambda'$, which completes the proof of the theorem.

COROLLARY 3.4. *Let Λ be separable over its center C . Then every algebra endomorphism is an automorphism.*

Proof. Let $f: \Lambda \rightarrow \Lambda$ be an algebra endomorphism. Then the kernel of f is of the form $\mathfrak{f}\Lambda$ where $\mathfrak{f}$ is an ideal in C . Since f is the identity on C , we have $\mathfrak{f} = 0$ or f is a monomorphism. Let Γ be the image of f . Then Γ is a central separable C -subalgebra of Λ . Thus $\Gamma \otimes_C \Lambda^\Gamma = \Lambda$ where Λ^Γ is separable over C . Now Λ^Γ is separable over C and thus is a finitely generated projective C -module with C contained as a C -direct summand. Now if $\mathfrak{m}$ is a maximal ideal in C we have, passing to the local ring $C_\mathfrak{m}$, that $\Gamma \otimes_C C_\mathfrak{m} \otimes_{C_\mathfrak{m}} C_\mathfrak{m} \otimes_C \Lambda^\Gamma = \Lambda \otimes_C C_\mathfrak{m}$.⁽²⁾ Now over a ring with only one maximal ideal, all finitely generated projective modules are free. (This follows easily for instance from Chapter VIII, Theorems 5.4' and J.3 of [4].) Thus, counting ranks, we have that $C_\mathfrak{m} \otimes_C \Lambda^\Gamma = C_\mathfrak{m}$. Since this is true for all maximal ideals $\mathfrak{m}$ in C , we conclude that $\Lambda^\Gamma = C$ or $\Gamma = \Lambda$. Therefore f is an isomorphism.

THEOREM 3.5. *Suppose that Γ is separable over its center C . Let Λ and Ω be subalgebras of Γ such that $\Lambda \otimes_C \Omega$ is isomorphic to Γ , under the mapping $x \otimes y \rightarrow xy$. Then Λ and Ω are both separable over C and C is the center of each of them. Furthermore Λ is the commutant of Ω and Ω the commutant of Λ .*

Proof. Since the center C of Γ is a C -direct summand; there is a projection f of Γ on C . The restriction of f to Λ is a projection of Λ onto C so that C is a direct summand of Λ . Similarly, C is a direct summand of Ω . It follows from

⁽²⁾ If S is a multiplicatively closed subset of C with $0 \notin S$, we denote by C_S the ring of quotients of C with respect to S . If $\mathfrak{p}$ is a prime ideal of C , we write $C_\mathfrak{p}$ instead of $C_{C-\mathfrak{p}}$.

this, and from the fact that $\Gamma \cong \Lambda \otimes_C \Omega$, that Λ and Ω are C -direct summands of Γ . Since Γ is projective over C , the algebras Λ and Ω are also C -projective. Hence by Proposition 1.7 we conclude that Λ and Ω are separable over C .

Because the elements of Λ and Ω commute, it follows that C is the center of both Λ and Ω , and that Ω is contained in the commutant Γ^Λ of Λ in Γ . By Theorem 3.3 we have $\Lambda \otimes \Gamma^\Lambda \cong \Gamma$. Consequently $\Lambda \otimes \Gamma^\Lambda / \Omega = 0$, and therefore $\Omega = \Gamma^\Lambda$.

The similarity between the theorems of this section and certain results in the classical theory of simple algebras is apparent. In order to obtain further analogues, additional hypotheses must be imposed on the center of the algebra.

Let C be a commutative ring and M a finitely generated projective C -module. If $\mathfrak{m}$ is a maximal ideal in C , then $M_{\mathfrak{m}} = M \otimes C_{\mathfrak{m}}$ is a finitely generated projective $C_{\mathfrak{m}}$ -module. Since $C_{\mathfrak{m}}$ has a unique maximal ideal, it follows that each $M_{\mathfrak{m}}$ is a free $C_{\mathfrak{m}}$ -module. We shall say that M is of rank n if, for each maximal ideal $\mathfrak{m}$, the module $M_{\mathfrak{m}}$ is a free $C_{\mathfrak{m}}$ -module on precisely n generators.

THEOREM 3.6. *Suppose C is a commutative ring such that every finitely generated projective C -module of rank one is free. If C is the center of Λ and Λ is separable over C , then every algebra endomorphism of Λ is an inner automorphism.*

Proof. Let f be an algebra endomorphism of Λ . We make Λ into a Λ° -module in a new way by defining $(x \otimes y)(z) = f(x)zy$. We will denote this new module structure by $\bar{\Lambda}$. Then applying Theorem 3.1, we have that $g: \Lambda \otimes_C (\bar{\Lambda})^\Lambda \rightarrow \bar{\Lambda}$ given by $g(x \otimes y) = f(x)y$ is an isomorphism. Here $(\bar{\Lambda})^\Lambda$ consists of all y in Λ with the property $f(x)y = yx$ for all x in Λ . Since C is a C -direct summand of Λ and g is an isomorphism, we have that $(\bar{\Lambda})^\Lambda$ is a direct summand of $\bar{\Lambda}$. Thus $(\bar{\Lambda})^\Lambda$ is a finitely generated projective C -module which is clearly of rank one. Therefore $(\bar{\Lambda})^\Lambda$ is free on one generator so that $(\bar{\Lambda})^\Lambda = Cr$ for some r in $(\bar{\Lambda})^\Lambda$. Therefore the map from Λ to itself given by $x \rightarrow f(x)r$ is an isomorphism, so that r is a unit in Λ . Since $f(x)r = rx$ for all x in Λ , we have $f(x) = rxr^{-1}$ and hence f is an inner automorphism.

REMARK. The hypothesis on the ring C in Theorem 3.6 is satisfied for example by local and semi-local rings (not necessarily noetherian), as well as by noetherian unique factorization domains.

The fact that a finitely generated projective module of rank n over a semi-local ring is free of rank n is an immediate consequence of the general observation: Let R be a commutative ring and $\mathfrak{a}$ an ideal contained in the radical of R . If E is a finitely generated projective R -module such that $E/\mathfrak{a}E$ is a free $R/\mathfrak{a}$ -module of rank n , then E is a free R -module of rank n . This observation can be proven as follows: Let $x_1, \dots, x_n$ be elements of E which map onto free generators of $E/\mathfrak{a}E$. Nakayama's lemma implies that

$x_1, \dots, x_n$ generate E . Let $0 \rightarrow K \rightarrow F \rightarrow E \rightarrow 0$ be an exact sequence, with F a free R -module of rank n . Since E is projective, the sequence splits so that K is finitely generated. Since $x_1, \dots, x_n$ map onto free generators of E/aE , it follows from tensoring the exact sequence with R/a that $K \otimes R/a = 0$. Applying Nakayama's lemma again shows that $K = 0$.

4. The homological different. Let Λ be an R -algebra with center C . In §1 we associated to Λ the ideal $\phi(A)$ of C , where A is the right annihilator of J in Λ^* and J is the kernel of the map $\phi: \Lambda^* \rightarrow \Lambda$ defined by $\phi(xy^0) = xy$. Because $\phi(A)$ has properties similar to those of the classical different, we shall call $\phi(A)$ the *homological different* of Λ over R , and will denote it by $\mathfrak{S}(\Lambda/R)$. It is essential to keep in mind the fact that $\mathfrak{S}(\Lambda/R)$ is an ideal of the center C , not of R . By Proposition 1.1, we know that Λ is separable over R if, and only if, $\mathfrak{S}(\Lambda/R) = C$.

PROPOSITION 4.1. *If S is a commutative R -algebra which is such that the ideal generated by the image of $\mathfrak{S}(\Lambda/R)$ in $C \otimes_R S$ is the unit ideal, then $\Lambda \otimes_R S$ is separable over S .*

Proof. If we set $\Gamma = \Lambda \otimes_R S$, then it is clear that $\Gamma^* = \Lambda^* \otimes_R S$ and the map $\phi': \Gamma^* \rightarrow \Gamma$ coincides with $\phi \otimes 1$. The exactness of the sequence $0 \rightarrow J \rightarrow \Lambda^* \xrightarrow{\phi} \Lambda \rightarrow 0$ implies the exactness of $J \otimes S \rightarrow \Gamma^* \xrightarrow{\phi'} \Gamma \rightarrow 0$ from which it follows that the image of $A \otimes S$ in Γ^* is contained in the right annihilator A' of J' , the kernel of ϕ' . The hypothesis of the proposition asserts that ϕ' of the image of $A \otimes S$ contains the unit element of Γ , from which we obtain $1 \in \phi'(A')$. Thus, Γ is separable over S .

There are two special cases of Proposition 4.1 which merit some attention.

COROLLARY 4.2. *If a is an ideal of R which is such that $aC + \mathfrak{S}(\Lambda/R) = C$, then $\Lambda/a\Lambda$ is separable over R/a .*

COROLLARY 4.3. *If M is a multiplicatively closed system of R whose image in C does not contain 0 and has a nonempty intersection with $\mathfrak{S}(\Lambda/R)$, then $\Lambda \otimes_R R_M$ is separable over R_M .*

By imposing suitable finiteness conditions, the content of Proposition 4.1 can be strengthened so as to yield localization properties of $\mathfrak{S}(\Lambda/R)$.

PROPOSITION 4.4. *Let R be noetherian and Λ an R -algebra which is a finitely generated R -module. If S is a commutative R -algebra which is a flat R -module, then $\mathfrak{S}(\Lambda \otimes S/S) = \mathfrak{S}(\Lambda/R) \otimes_R S$.*

Proof. The hypotheses of the proposition imply the isomorphism $S \otimes_R \text{Hom}_{\Lambda^*}(\Lambda, \Lambda^*) \cong \text{Hom}_{S \otimes \Lambda^*}(S \otimes \Lambda, S \otimes \Lambda^*)$. (See for example Lemma 2.4 of [2].) Since we may identify A with $\text{Hom}_{\Lambda^*}(\Lambda, \Lambda^*)$, the result follows immediately.

COROLLARY 4.5. *Let R be noetherian and Λ an R -algebra which is a finitely*

generated R -module. Then, a necessary and sufficient condition that Λ be separable over R is that $\Lambda \otimes R_{\mathfrak{m}}$ be separable over $R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R .

Proof. The necessity of the condition has already been established in Corollary 1.6. If $\Lambda \otimes R_{\mathfrak{m}}$ is separable over $R_{\mathfrak{m}}$, then, using the fact that $R_{\mathfrak{m}}$ is a flat R -module, Proposition 4.4 shows that $C/\mathfrak{S}(\Lambda/R) \otimes R_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of R . It follows that $\mathfrak{S}(\Lambda/R) = C$, i.e., that Λ is separable over R .

One cannot in general replace "maximal" by "minimal" in Corollary 4.5^(*); it is possible to do so under suitably restricted conditions. We shall only consider the question of separability over the center.

PROPOSITION 4.6. *Let the center C of Λ be an integrally closed noetherian domain and let Λ be a finitely generated projective C -module. If, for every minimal prime ideal $\mathfrak{p}$ of C , we have $\Lambda \otimes C_{\mathfrak{p}}$ is separable over $C_{\mathfrak{p}}$, then Λ is separable over C .*

Proof. Let K be the field of quotients of C . It is clear that the center of $\Lambda \otimes K$ is K itself. Also, $\Lambda \otimes_c K$ is separable over K because $\Lambda \otimes_c K = (\Lambda \otimes_c C_{\mathfrak{p}}) \otimes_{C_{\mathfrak{p}}} K$, and $\Lambda \otimes_c C_{\mathfrak{p}}$ is separable over $C_{\mathfrak{p}}$. Therefore $\Lambda \otimes K$ is a central simple algebra over K . Consequently, $\Lambda^* \otimes K = (\Lambda \otimes K)^*$ is isomorphic to $\text{Hom}_K(\Lambda \otimes K, \Lambda \otimes K)$, so that the mapping $\eta: \Lambda^* \rightarrow \text{Hom}_C(\Lambda, \Lambda)$ is a monomorphism because Λ^* is a torsion-free C -module.

Since, for each prime ideal $\mathfrak{p}$ of C , we have $\eta \otimes 1: \Lambda^* \otimes C_{\mathfrak{p}} \rightarrow \text{Hom}_{C_{\mathfrak{p}}}(\Lambda \otimes C_{\mathfrak{p}}, \Lambda \otimes C_{\mathfrak{p}})$ is an isomorphism, it follows that the annihilator in C of $\text{Hom}_C(\Lambda, \Lambda)/\eta(\Lambda^*)$ is not of rank one. In view of the fact that Λ^* is isomorphic to its second dual with respect to C , it follows from this that the annihilator of $\text{Hom}_C(\Lambda, \Lambda)/\eta(\Lambda^*)$ is all of C , i.e., η is an epimorphism. (See Proposition 3.4 of [1].) It now follows from Theorem 2.1 that Λ is separable over C .

Having considered the consequences of the separability of $\Lambda \otimes R_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$, we turn to the question of $\Lambda/\mathfrak{m}\Lambda$ over $R/\mathfrak{m}$.

THEOREM 4.7. *Let R be noetherian, and Λ an R -algebra which is a finitely generated R -module. A necessary and sufficient condition that Λ be separable over R is that $\Lambda/\mathfrak{m}\Lambda$ be separable over $R/\mathfrak{m}$ for every maximal ideal of R .*

Proof. The necessity of the condition has already been established in Proposition 1.4. In view of Corollary 4.5, we need only prove the sufficiency of the condition under the assumption that R is a local ring. It is well known

(*) For example, let R be a regular local ring of dimension ≥ 3 . There exist nonprojective finitely generated modules E with $E = E^{**}$. Then $\Lambda = \text{Hom}_R(E, E)$ is a maximal order in a full matrix algebra (Proposition 4.2 of [2]). Since E is not projective, it follows from Theorem 4.3 of [2] that Λ is not projective and therefore not separable over R . If $\mathfrak{p}$ is any minimal prime ideal of R , then $R_{\mathfrak{p}}$ is a discrete rank one valuation ring and $\Lambda \otimes R_{\mathfrak{p}}$ is a maximal order over $R_{\mathfrak{p}}$ in a full matrix algebra and is therefore separable.

that Λ is Λ^e -projective if, and only if, every R -derivation from Λ to an arbitrary Λ^e -module is inner. (Proposition 3.2, Chapter IX of [4].) Because Λ^e is a finitely generated R -module, we may restrict ourselves to derivations into finitely generated Λ^e -modules. (See Chapter VI, Proposition 2.5 of [4].)

We shall consider first the case where R is a complete local ring. Let E be a finitely generated Λ^e -module and D an R -derivation of Λ into E . Then D induces a derivation of $\Lambda/m\Lambda$ into E/mE which is inner because $\Lambda/m\Lambda$ is separable over R/m . Hence there is an element $e_0 \in E$ such that $D_1(x) = D(x) - (xe_0 - e_0x) \in mE$, for every $x \in \Lambda$. But D_1 is an R -derivation of Λ into mE , so that there is an $e_1 \in mE$ with the property that $D_2(x) = D_1(x) - (xe_1 - e_1x) \in m^2E$. Continuing this process defines a sequence e_n of elements of E with the following properties: (a) $e_n \in m^nE$, (b) $D(x) - \sum_{j=0}^n (xe_j - e_jx) \in m^{n+1}E$. Since R is complete and E is a finitely generated R -module, E is also complete so that $e = \sum_{n=0}^{\infty} e_n$ is defined and is an element of E . But it is also clear that $D(x) - (xe - ex) \in m^nE$ for every n , so that $D(x) - (xe - ex) = 0$, or D is inner. Thus, Λ is separable over R .

Now suppose that R is a local ring and Λ an R -algebra which is a finitely generated R -module such that $\Lambda/m\Lambda$ is separable over R/m . Denote the completion of R by $\hat{R}$, and $\Lambda \otimes \hat{R}$ by $\hat{\Lambda}$. Then $(\hat{\Lambda})^e = \Lambda^e \otimes \hat{R}$.

Let E be any finitely generated Λ^e -module. Then we have, by Lemma 2.4 of [2], that $\hat{R} \otimes \text{Ext}_{\Lambda^e}^1(\Lambda, E) \cong \text{Ext}_{\hat{\Lambda}}^1(\hat{\Lambda}, \hat{R} \otimes E)$. But because $\hat{\Lambda}/\hat{m}\hat{\Lambda} = \Lambda/m\Lambda$, we know that $\hat{\Lambda}$ is separable over $\hat{R}$, so that $\text{Ext}_{\hat{\Lambda}}^1(\hat{\Lambda}, \hat{R} \otimes E) = 0$. However, $\text{Ext}_{\Lambda^e}^1(\Lambda, E)$ is a finitely generated R -module. Consequently the fact that $\hat{R} \otimes \text{Ext}_{\Lambda^e}^1(\Lambda, E) = 0$ yields the conclusion that $\text{Ext}_{\Lambda^e}^1(\Lambda, E) = 0$, i.e., that Λ is separable over R .

5. The Brauer group. The following proposition contains a number of properties of finitely generated projective modules which will be needed below. Since these statements are each readily verified, we shall omit their proofs.

PROPOSITION 5.1. *Let R be a commutative ring. If E is a finitely generated projective R -module with annihilator $\mathfrak{a}$ in R , then $\text{Hom}_R(E, E)$ is separable over R and its center is $R/\mathfrak{a}$. If E' is another finitely generated projective R -module, then $E \otimes_R E'$ is a finitely generated projective R -module and $\text{Hom}_R(E \otimes E', E \otimes E') \cong \text{Hom}_R(E, E) \otimes_R \text{Hom}_R(E', E')$. If both E and E' are faithful, then $E \otimes E'$ is also faithful.*

If R is a commutative ring, we denote by $\mathcal{Q}(R)$ the isomorphism classes of all algebras having R as center and separable over R , and by $\mathcal{Q}_0(R)$ the subset of $\mathcal{Q}(R)$ consisting of the algebras $\text{Hom}_R(E, E)$ where E is any finitely generated projective faithful R -module. By Proposition 1.5, $\mathcal{Q}(R)$ is closed under the operation of tensor product over R , and by Proposition 5.1 the same is the case for $\mathcal{Q}_0(R)$.

We introduce an equivalence relation in $\mathcal{Q}(R)$ as follows: If Λ_1 and Λ_2 are in $\mathcal{Q}(R)$, then Λ_1 is *equivalent* to Λ_2 , denoted by $\Lambda_1 \sim \Lambda_2$, if there are algebras

Ω_1 and Ω_2 in $\mathfrak{A}_0(R)$ such that $\Lambda_1 \otimes_R \Omega_1 \cong \Lambda_2 \otimes_R \Omega_2$. Proposition 5.1 shows that this is a proper equivalence relation. We denote by $\mathfrak{B}(R)$ the set of equivalence classes into which $\mathfrak{A}(R)$ is partitioned. Again, by Proposition 5.1, the operation of tensor product over R is compatible with the equivalence relation so that there is induced an associative and commutative multiplication in $\mathfrak{B}(R)$. The equivalence class which contains R itself is clearly an identity for this multiplication.

If $\Lambda \in \mathfrak{A}(R)$ then clearly Λ^0 is also in $\mathfrak{A}(R)$. By Theorem 2.1 we have that Λ is a finitely generated projective faithful R -module and that $\Lambda \otimes_R \Lambda^0 \cong \text{Hom}_R(\Lambda, \Lambda)$. Therefore it follows that $\Lambda \otimes_R \Lambda^0 \sim R$ so that the equivalence class of Λ^0 is an inverse to that of Λ in $\mathfrak{B}(R)$. Thus, we have proved:

THEOREM 5.2. $\mathfrak{B}(R)$ is an abelian group.

If K is a field, then $\mathfrak{B}(K)$ as defined here coincides with the group of algebra classes of K , i.e., $\mathfrak{B}(K)$ is the Brauer group of K . By analogy, we shall call the group $\mathfrak{B}(R)$, as defined above, the *Brauer group* of the ring R .

It is convenient to know precisely which algebras are equivalent to R . We have:

PROPOSITION 5.3. If $\Lambda \in \mathfrak{A}(R)$ then $\Lambda \sim R$ if, and only if, $\Lambda \in \mathfrak{A}_0(R)$.

Proof. If $\Lambda \in \mathfrak{A}_0(R)$ then certainly we have $\Lambda \sim R$. Suppose on the other hand that $\Lambda \sim R$. Then there are finitely generated projective faithful R -modules E_1 and E_2 such that $\Lambda \otimes_R \text{Hom}_R(E_1, E_1) \cong \text{Hom}_R(E_2, E_2)$. This isomorphism imbeds $\text{Hom}_R(E_1, E_1)$ into $\text{Hom}_R(E_2, E_2)$ and enables us to consider E_2 as a $\text{Hom}_R(E_1, E_1)$ -module. By Proposition A.6 of [2] there is a finitely generated projective (necessarily faithful) R -module E_3 such that $E_2 \cong E_1 \otimes_R E_3$. From this it follows that $\text{Hom}_R(E_2, E_2) \cong \text{Hom}_R(E_1, E_1) \otimes_R \text{Hom}_R(E_3, E_3)$ and in such a way that $\text{Hom}_R(E_1, E_1)$ is imbedded in $\text{Hom}_R(E_2, E_2)$ in the same way as it was under the isomorphism $\text{Hom}_R(E_2, E_2) \cong \Lambda \otimes_R \text{Hom}_R(E_1, E_1)$. It follows that both Λ and $\text{Hom}_R(E_3, E_3)$ are the commutants of $\text{Hom}_R(E_1, E_1)$ in $\text{Hom}_R(E_2, E_2)$ and consequently, $\Lambda = \text{Hom}_R(E_3, E_3)$.

COROLLARY 5.4. If Λ_1 and Λ_2 are in $\mathfrak{A}(R)$ then $\Lambda_1 \sim \Lambda_2$ if, and only if, $\Lambda_1 \otimes_R \Lambda_2^0 \in \mathfrak{A}_0(R)$.

Proof. The corollary follows immediately from the proposition and the fact that $\mathfrak{A}_0(R)$ is multiplicatively closed.

Suppose that S is a commutative R -algebra. Corollary 1.6 shows that the operation $\Lambda \rightarrow S \otimes_R \Lambda$ induces a map from $\mathfrak{A}(R)$ to $\mathfrak{A}(S)$. This mapping sends $\mathfrak{A}_0(R)$ into $\mathfrak{A}_0(S)$ because of the following fact:

PROPOSITION 5.5. If E is a finitely generated projective R -module and S is a commutative R -algebra, then $S \otimes_R E$ is a finitely generated projective S -module and $\text{Hom}_S(S \otimes_R E, S \otimes_R E) \cong S \otimes_R \text{Hom}_R(E, E)$. If, in addition, E is a faithful R -module, then $S \otimes_R E$ is a faithful S -module.

Proof. The proposition follows from the elementary properties of projective modules; the proof will be omitted.

It follows from the above remarks that the operation $\Lambda \rightarrow S \otimes_R \Lambda$ induces a homomorphism from $\mathfrak{B}(R)$ to $\mathfrak{B}(S)$ whenever S is an R -algebra. In particular, if $f: R \rightarrow S$ is a ring homomorphism, then there is induced a homomorphism $f_*: \mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$.

If Λ is a central separable algebra over R whose algebra class in $\mathfrak{B}(R)$ is in the kernel of f_* , we shall say that Λ is *split* by S , or that S is a *splitting ring* of Λ .

There are two facts about splitting rings of a general nature.

THEOREM 5.6. *Let Λ be a central separable algebra over R and S a maximal commutative subalgebra of Λ . If S is separable over R , then Λ is a finitely generated projective (left) S -module and $\text{Hom}_S(\Lambda, \Lambda) \cong S \otimes_R \Lambda^0$. Consequently Λ is split by S .*

Proof. Since Λ is a finitely generated R -module, Λ is certainly finitely generated over S . Set $\Omega = \text{Hom}_R(\Lambda, \Lambda)$, so that $\Omega \cong \Lambda \otimes_R \Lambda^0$. Considering $S \otimes_R \Lambda^0$ as a subalgebra of Ω , the fact that S is a maximal commutative subalgebra of Λ shows that the commutant of $S \otimes_R \Lambda^0$ in Ω is S itself, i.e., $\text{Hom}_{S \otimes_R \Lambda^0}(\Lambda, \Lambda) = S$. We form the trace ideal $\mathfrak{T}_{S \otimes_R \Lambda^0}(\Lambda)$ in $S \otimes_R \Lambda^0$ and we shall now prove that $\mathfrak{T}_{S \otimes_R \Lambda^0}(\Lambda) = S \otimes_R \Lambda^0$. For, we may then apply Theorem A.2 of [2], from which it will follow that Λ is S -projective and that $\text{Hom}_S(\Lambda, \Lambda) \cong S \otimes_R \Lambda^0$.

To prove the assertion about $\mathfrak{T}_{S \otimes_R \Lambda^0}(\Lambda)$ we consider the following diagram:

$$\begin{array}{ccccc}
 J_0 & \rightarrow & J_1 & \rightarrow & J \\
 \downarrow & & \downarrow & & \downarrow \\
 S \otimes S & \xrightarrow{f} & S \otimes \Lambda^0 & \rightarrow & \Lambda \otimes \Lambda^0 \\
 \downarrow \phi_0 & & \downarrow \phi_1 & & \downarrow \phi \\
 S & \rightarrow & \Lambda & \rightarrow & \Lambda
 \end{array}$$

in which ϕ_1 is the restriction of ϕ to $S \otimes \Lambda^0$ and J_i is the kernel of ϕ_i . If we denote by A_1 the right annihilator of J_1 in $S \otimes \Lambda^0$, then it is readily verified that $\mathfrak{T}_{S \otimes \Lambda^0}(\Lambda)$ is the two-sided ideal generated by A_1 , i.e., that $\mathfrak{T}_{S \otimes \Lambda^0}(\Lambda) = (S \otimes \Lambda^0)A_1$. One also readily verifies that J_1 is generated as a left ideal in $S \otimes \Lambda^0$ by $f(J_0)$. Consequently, if A_0 is the right annihilator of J_0 in $S \otimes S$, we have $f(A_0) \subset A_1$. But S is separable over R , so that $\phi_0(A_0) = S$. Therefore, we have $1 \in \phi_1(A_1)$. Now $\mathfrak{T}_{S \otimes \Lambda^0}(\Lambda)$ is a two-sided ideal in the algebra $S \otimes \Lambda^0$ which is central separable over S . There is therefore an ideal $\mathfrak{a}$ in S such that $\mathfrak{T}_{S \otimes \Lambda^0}(\Lambda) = \mathfrak{a}(S \otimes \Lambda^0)$ or that $(S \otimes \Lambda^0)A_1 = \mathfrak{a}(S \otimes \Lambda^0)$. Applying ϕ_1 to both sides, and using the fact that $1 \in \phi_1(A_1)$, we find that $\mathfrak{a}\Lambda = \Lambda$. Since Λ is a finitely generated faithful S -module, it follows that $\mathfrak{a} = S$ and therefore that $\mathfrak{T}_{S \otimes \Lambda^0}(\Lambda) = S \otimes \Lambda^0$, completing the proof of the theorem.

THEOREM 5.7. *Let Λ be a central separable algebra over R and S a splitting ring of Λ . If R is a subring of S and S is a finitely generated projective R -module, then there is an algebra equivalent to Λ which contains S as a maximal commutative subalgebra.*

Proof. Since S splits Λ it splits Λ^0 , so that there is a finitely generated projective faithful S -module E such that $S \otimes \Lambda^0 \cong \text{Hom}_S(E, E)$. Because S is a finitely generated projective R -module which contains R , it follows that E is a finitely generated projective faithful R -module. We have $S \otimes \Lambda^0 = \text{Hom}_S(E, E) \subset \text{Hom}_R(E, E)$. Let Γ be the commutant of Λ^0 in $\text{Hom}_R(E, E)$. Then by Theorem 3.3 we have $\Gamma \otimes \Lambda^0 = \text{Hom}_R(E, E)$ and therefore that $\Gamma \sim \Lambda$. Also it is clear from the definition of Γ that $S \subset \Gamma$. Finally, suppose that $x \in \Gamma$ commutes with the elements of S . Then, considering x as an element of $\text{Hom}_R(E, E)$, the fact that x commutes with S means that $x \in \text{Hom}_S(E, E) = S \otimes \Lambda^0$. The fact that x is in Γ means that x commutes with Λ^0 and therefore that x is in the center of $S \otimes \Lambda^0$. But the center of $S \otimes \Lambda^0$ is S , whence $x \in S$. Thus S is a maximal commutative subalgebra of Γ and the proof is complete.

The remainder of the paper is principally concerned with properties of the homomorphism $f_*: \mathcal{B}(R) \rightarrow \mathcal{B}(S)$ arising from various special ring homomorphisms $f: R \rightarrow S$.

6. Local rings⁽⁴⁾.

PROPOSITION 6.1. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and Λ a central separable algebra over R . If $\Lambda/\mathfrak{m}\Lambda \sim R/\mathfrak{m}$ (over $R/\mathfrak{m}$) and some primitive idempotent of $\Lambda/\mathfrak{m}\Lambda$ can be lifted to Λ , then $\Lambda \sim R$.*

Proof. Denote by $x \rightarrow \bar{x}$ the map from Λ to $\Lambda/\mathfrak{m}\Lambda$. Let e be an idempotent of Λ such that $\bar{e}$ is a primitive idempotent of $\Lambda/\mathfrak{m}\Lambda$. Then Λe is a direct summand of Λ so that Λe is a free R -module. The annihilator of Λe in Λ is a two-sided ideal and therefore by Corollary 3.2 has the form $\mathfrak{a}\Lambda$ with $\mathfrak{a}$ an ideal of R . But Λe is a free R -module so that its annihilator in R is 0. This shows that $\mathfrak{a} = 0$ and therefore Λe is a faithful Λ -module. In particular Λ is a subalgebra of $\text{Hom}_R(\Lambda e, \Lambda e)$ and the result will follow if we prove that Λ coincides with $\text{Hom}_R(\Lambda e, \Lambda e)$. Now, Λ and $\text{Hom}_R(\Lambda e, \Lambda e)$ are both central separable over R so that $\text{Hom}_R(\Lambda e, \Lambda e) \cong \Lambda \otimes_R \Gamma$ where Γ is the commutant of Λ in $\text{Hom}_R(\Lambda e, \Lambda e)$. It is clear that $\Gamma = \text{Hom}_\Lambda(\Lambda e, \Lambda e)$. We need to show therefore that $\Gamma = R$. Since $R \subset \Gamma$ and Γ is a free R -module, it is sufficient to prove that the rank of Γ over R is one.

Considering $R/\mathfrak{m}$ as an R -algebra, we apply Proposition 5.5 to obtain:

$$R/\mathfrak{m} \otimes_R \text{Hom}_R(\Lambda e, \Lambda e) \cong \text{Hom}_{R/\mathfrak{m}}(R/\mathfrak{m} \otimes \Lambda e, R/\mathfrak{m} \otimes \Lambda e).$$

Therefore we have:

⁽⁴⁾ For convenience of exposition we assume in this section that the local rings are noetherian, although this hypothesis is not always necessary for the proofs given.

$$\operatorname{Hom}_R(\Lambda e, \Lambda e)/\mathfrak{m} \operatorname{Hom}_R(\Lambda e, \Lambda e) \cong \operatorname{Hom}_{R/\mathfrak{m}}(\Lambda e/\mathfrak{m}\Lambda e, \Lambda e/\mathfrak{m}\Lambda e).$$

But it is clear that $\Lambda e/\mathfrak{m}\Lambda e \cong (\Lambda/\mathfrak{m}\Lambda)e = (\Lambda/\mathfrak{m}\Lambda)\bar{e}$, while $\operatorname{Hom}_{R/\mathfrak{m}}((\Lambda/\mathfrak{m}\Lambda)\bar{e}, (\Lambda/\mathfrak{m}\Lambda)\bar{e}) = \Lambda/\mathfrak{m}\Lambda$ because $\bar{e}$ is a primitive idempotent. Thus the rank over R of $\operatorname{Hom}_R(\Lambda e, \Lambda e)$ is the same as the rank of Λ over R , whence Γ has rank one.

COROLLARY 6.2. *If R is a complete local ring with maximal ideal $\mathfrak{m}$, then the homomorphism $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R/\mathfrak{m})$ induced by $R \rightarrow R/\mathfrak{m}$ is a monomorphism.*

Proof. In view of the above proposition we need only prove that an idempotent of $\Lambda/\mathfrak{m}\Lambda$ can be lifted to Λ . The usual procedure in the case of nilpotent radical works equally well in the case where R is complete. See p. 54 of [6].

THEOREM 6.3. *Let R be a local ring and Λ a central separable algebra over R . Then Λ has a splitting ring S which contains R as a subring, is a separable R -algebra and is a finitely generated free R -module. Furthermore, in case R is complete, S is also a local ring⁽⁶⁾.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R . Let L be a separable field extension of $R/\mathfrak{m}$ which splits the central simple algebra $\Lambda/\mathfrak{m}\Lambda$. Set $L = R/\mathfrak{m}(\theta)$, and let f be a monic irreducible polynomial with coefficients in $R/\mathfrak{m}$ having θ as a zero. Finally, let F be a monic polynomial with coefficients in R which maps onto f , modulo $\mathfrak{m}$. If $S_1 = R[x]/(F)$, then S_1 has the following properties: (a) S_1 contains R and is a finitely generated free R -module, (b) $S_1/\mathfrak{m}S_1 = L$, so that S_1 is a local ring with maximal ideal $\mathfrak{m}S_1$, (c) S_1 is a separable R -algebra (see Theorem 4.7), (d) the algebra class of $\Lambda \otimes S_1$ is in the kernel of the map $\mathfrak{B}(S_1) \rightarrow \mathfrak{B}(S_1/\mathfrak{m}S_1)$.

The existence of the ring S_1 disposes of the theorem in case R is complete. Namely, Corollary 6.2 combined with (d) above shows that S_1 is a splitting ring of Λ in that case. In general, the existence of S_1 shows that it is sufficient to prove the theorem under the additional hypothesis that $\Lambda/\mathfrak{m}\Lambda$ is a full matrix algebra over $R/\mathfrak{m}$. We shall now add this hypothesis, and suppose that $\Lambda/\mathfrak{m}\Lambda$ is the ring of $n \times n$ matrices over $R/\mathfrak{m}$.

Let W be a maximal commutative subring of $\Lambda/\mathfrak{m}\Lambda$ of dimension n over $R/\mathfrak{m}$, of the form $R/\mathfrak{m}[\alpha]$, and separable over $R/\mathfrak{m}$. The existence of such a W can be seen in the following way: if $R/\mathfrak{m}$ is a finite field, then $R/\mathfrak{m}$ has an extension of degree n (necessarily separable) which can be imbedded in the algebra of $n \times n$ matrices as a maximal commutative subring. If no such subfield of $\Lambda/\mathfrak{m}\Lambda$ exists, then the subalgebra of all diagonal matrices may be taken as W , and α may be chosen as a diagonal matrix with distinct elements.

With W and its generator α chosen as above, let β be an element of Λ which maps onto α under the map $\Lambda \rightarrow \Lambda/\mathfrak{m}\Lambda$. Let S be the R -submodule of Λ generated by $1, \beta, \dots, \beta^{n-1}$. Because R is a local ring, and because $1, \alpha, \dots, \alpha^{n-1}$ are linearly independent over $R/\mathfrak{m}$, it follows that

⁽⁶⁾ This proof is based on a suggestion of J.-P. Serre.

$1, \beta, \dots, \beta^{n-1}$ can be extended to a set of free generators of Λ over R . Therefore we find that S is a free R -module of rank n having $1, \beta, \dots, \beta^{n-1}$ as free generators and also that S is a direct summand over R of Λ .

We assert that S is a subring of Λ . To prove this, it is sufficient to show that $\beta^n \in S$. Let $\hat{R}$ be the completion of R and $\hat{\Lambda} = \hat{R} \otimes \Lambda$. Since $\hat{\Lambda}/\mathfrak{m}\hat{\Lambda} = \Lambda/\mathfrak{m}\Lambda$, it follows from Corollary 6.2 that $\hat{\Lambda} \sim \hat{R}$ so that $\hat{\Lambda} = \text{Hom}_{\hat{R}}(F, F)$ with F a free $\hat{R}$ -module of rank n . Considering β as an endomorphism of F , its characteristic polynomial ϕ is a monic polynomial of degree n with coefficients in $\hat{R}$ and we have $\phi(\beta) = 0$. (The usual proof of the Cayley-Hamilton Theorem applies equally well to the endomorphisms of a free module over any commutative ring.) Thus, we have $\beta^n \in \hat{R} \otimes S$. Since S is a direct summand of Λ , it follows therefore that $\beta^n \in S$ and that S is a subring of Λ .

Since S is a direct summand of Λ , we have $S \cap \mathfrak{m}\Lambda = \mathfrak{m}S$, so that $S/\mathfrak{m}S = W$. Therefore, by Theorem 4.7, S is separable over R .

All that remains is to show that S splits Λ . Let S' be the commutant of S in Λ . In view of the fact that W is a maximal commutative subalgebra of $\Lambda/\mathfrak{m}\Lambda$, we have $S' = S + S' \cap (\mathfrak{m}\Lambda)$. We may describe S' in another way. Consider Λ as a left S -module. Since Λ is R -free, and S is both R -free and R -separable, it follows from Theorem 1.8 that Λ is a projective S -module, and therefore that $\Omega = \text{Hom}_S(\Lambda, \Lambda)$ is a central separable S -algebra. We have $\Lambda \otimes_R \Lambda^0 = \text{Hom}_R(\Lambda, \Lambda) \supset \Omega$, and the subalgebra $S \otimes_R \Lambda^0$ of $\Lambda \otimes_R \Lambda^0$ is clearly contained in Ω . Now, $S \otimes_R \Lambda^0$ is a central separable algebra over S . It is obvious that the commutant of $S \otimes_R \Lambda^0$ in Ω is S' . It follows from Theorem 3.3 that S' has S for its center and is separable over S . In addition, Theorem 3.3 shows that $(S \otimes_R \Lambda^0) \otimes_S S' = \Omega$.

Now, $S' \cap (\mathfrak{m}\Lambda)$ is a two-sided ideal in S' , so that there is an ideal $\mathfrak{b}$ in S with $\mathfrak{b}S' = (S' \cap \mathfrak{m}\Lambda)$. But $\mathfrak{b}S' \cap S = \mathfrak{b}$, while $S' \cap \mathfrak{m}\Lambda \cap S = \mathfrak{m}S$ so that $\mathfrak{b} = \mathfrak{m}S$, and therefore $S' = S + \mathfrak{m}S'$. It follows immediately that $S' = S$. In view of the relation $(S \otimes_R \Lambda^0) \otimes_S S' = \Omega$, we find that $S \otimes_R \Lambda^0 = \Omega = \text{Hom}_S(\Lambda, \Lambda)$ and therefore we conclude that S splits Λ . This completes the proof of the theorem.

COROLLARY 6.4. *If R is a local ring and Λ a central separable algebra over R , then Λ is split by a Galois extension of R . In case R is complete, Λ has such a splitting ring which is also a local ring.*

Proof. If S is the splitting ring whose existence is proved in Theorem 6.3, then S may be imbedded in a Galois extension of R (see Theorem A.7). If R is complete, we may proceed differently. If $\mathfrak{m}$ is the maximal ideal of R , then $\Lambda/\mathfrak{m}\Lambda$ is a central simple algebra over $R/\mathfrak{m}$. Let L be a Galois field extension of $R/\mathfrak{m}$ which splits $\Lambda/\mathfrak{m}\Lambda$ and let $L = R/\mathfrak{m}(\theta)$. If f is a monic irreducible polynomial with coefficients in $R/\mathfrak{m}$ such that $f(\theta) = 0$, let F be a monic polynomial with coefficients in R which maps onto f through the homomorphism $R \rightarrow R/\mathfrak{m}$. Set $S = R[x]/(F)$. Then, because R is complete, Corollary 6.2 shows that S splits Λ . In addition, S is a Galois extension of R with respect to the

group of all automorphisms of S over R . This follows easily from the fact that R is complete and that L is a Galois extension of $R/\mathfrak{m}$.

Let G be the Galois group of L over $R/\mathfrak{m}$ and let G' be the group of all automorphisms of S leaving the elements of R fixed. Since $\mathfrak{m}S$ is the maximal ideal of S , there is a natural homomorphism $j: G' \rightarrow G$ such that $\pi\sigma(w) = j(\sigma)\pi(w)$, where $\pi: S \rightarrow L$ is the canonical homomorphism. It follows from Hensel's lemma that F splits into linear factors in S and also that $\pi(\alpha_1), \dots, \pi(\alpha_n)$ are the zeros of f where $\alpha_1, \dots, \alpha_n$ are the zeros of F . It follows immediately that j is a monomorphism. A further application of Hensel's lemma shows that j is also an epimorphism. We may now identify G' with G , considering j as the identity map.

Let Δ be the trivial crossed product formed from S and G , (see appendix), and Δ^* the one formed from L and G . Then we have the following commutative diagram:

$$\begin{array}{ccc} \Delta & \xrightarrow{\delta} & \text{Hom}_R(S, S) \\ \downarrow & & \downarrow u \\ \Delta^* & \xrightarrow{\delta^*} & \text{Hom}_{R/\mathfrak{m}}(L, L) \\ \downarrow & & \\ 0 & & \end{array}$$

In the diagram, the vertical maps arise from the canonical map $\pi: S \rightarrow L$. Also, δ^* is an isomorphism because L is a Galois extension of $R/\mathfrak{m}$ relative to G . It follows from Proposition 5.5 that the kernel of u is $\mathfrak{m} \text{Hom}_R(S, S)$. Since δ^* is an epimorphism, we find $\delta(\Delta) + \mathfrak{m} \text{Hom}_R(S, S) = \text{Hom}_R(S, S)$, and hence by Nakayama's lemma, we have $\delta(\Delta) = \text{Hom}_R(S, S)$. Thus δ is an epimorphism. Finally, if the rank of S over R is n , then both Δ and $\text{Hom}_R(S, S)$ are free R -modules of rank n^2 so that δ is also a monomorphism. The fact that δ is an isomorphism shows therefore that S is a Galois extension of R relative to G .

If S is a Galois extension of the local ring R with group G , then, because S is semi-local, Theorem A.15 of the appendix shows that $(1) \rightarrow H^2(G, U(S)) \rightarrow \mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$ is exact. Furthermore, Corollary 6.4 shows that $\mathfrak{B}(R)$ is the union of the groups $H^2(G, U(S))$ as S ranges over the Galois extensions of R .

The final result of this section has already been proved by Azumaya (Theorem 31 of [3]).

THEOREM 6.5. *If R is a complete local ring, then the homomorphism $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R/\mathfrak{m})$ is an isomorphism.*

Proof. Corollary 6.2 shows that the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R/\mathfrak{m})$ is a monomorphism, hence we need only show that it is an epimorphism. If L is a Galois extension of $R/\mathfrak{m}$, we have already seen several times that there is a local

Galois extension S of R such that $S/mS = L$. Furthermore, if G is the Galois group of L over R/m , then the group of automorphisms of S over R is isomorphic to G . Thus the result will follow if we can prove that $H^2(G, U(S)) \rightarrow H^2(G, U(L))$ is an epimorphism. That this is in fact the case follows easily from the completeness of R .

We observe first that $m^n S/m^{n+1}S$ and $m^n/m^{n+1} \otimes_{R/m} S/mS$ are isomorphic G -modules. Therefore, for $q \geq 1$, we have $H^q(G, m^n S/m^{n+1}S) \cong H^q(G, S/mS) = 0$.

Set $S_n = 1 + m^n S \subset U(S)$. Then $(1) \rightarrow S_1 \rightarrow U(S) \rightarrow U(L) \rightarrow (1)$ is an exact sequence. Now the multiplicative group S_n/S_{n+1} is G -isomorphic to the additive group $m^n S/m^{n+1}S$ (for $n \geq 1$) and hence, for $q \geq 1$, $H^q(G, S_n/S_{n+1}) = (1)$. From this we shall deduce $H^q(G, S_1) = (1)$, for $q \geq 1$. Namely, suppose $f \in Z^q(G, S_1)$. Then there is a $g_1 \in C^{q-1}(G, S_1)$ such that $f\delta g_1 \in Z^q(G, S_2)$. Continuing this process leads to a sequence $g_1, g_2, \dots, g_n, \dots$ such that $g_n \in C^{q-1}(G, S_n)$ and $f\delta(g_1 g_2 \dots g_n) \in Z^q(G, S_{n+1})$.

Now, $g_1, g_1 g_2, \dots, \prod_{i=1}^n g_i, \dots$ forms a Cauchy sequence in $C^{q-1}(G, S_1)$ so that, because S is complete, there is a $g \in C^{q-1}(G, S_1)$ with $g = \lim \prod_{i=1}^n g_i$. We have $g(g_1 g_2 \dots g_n)^{-1} \in C^{q-1}(G, S_{n+1})$.

Set $h = f\delta g$. Then $h = f\delta(g_1 \dots g_n) \delta(g g_1^{-1} \dots g_n^{-1})$, while $f\delta(g_1 \dots g_n) \in Z^q(G, S_n)$ and $\delta(g g_1^{-1} \dots g_n^{-1}) \in Z^q(G, S_{n+1})$. Consequently, $h \in Z^q(G, S_n)$ for every $n \geq 1$ and therefore $h = 1$. It follows that $H^q(G, S_1) = (1)$.

From the exact sequence $(1) \rightarrow S_1 \rightarrow U(S) \rightarrow U(L) \rightarrow (1)$, we have

$$\rightarrow H^q(G, S_1) \rightarrow H^q(G, U(S)) \rightarrow H^q(G, U(L)) \rightarrow H^{q+1}(G, S_1) \rightarrow$$

and therefore, for $q \geq 1$, we have $H^q(G, U(S)) \cong H^q(G, U(L))$, which completes the proof of the theorem.

7. Separable orders. Let R be an integral domain with quotient field K and Λ an algebra having R as center and separable over R . Then $\Lambda \otimes_R K$ is separable over K and has K for its center, so that $\Lambda \otimes K$ is a central simple algebra over K . Since Λ is a finitely generated R -module, it follows that Λ is an order in $\Lambda \otimes K$. (See [2] for the definition and basic properties of orders.)

PROPOSITION 7.1. *Let R be an integrally closed noetherian domain with quotient field K and Λ an R -algebra having R for its center and separable over R . Then Λ is a maximal order in $\Lambda \otimes K$.*

Proof. Let Γ be an order in $\Lambda \otimes K$ containing Λ . Denoting by Γ^Λ the commutant of Λ in Γ , we have by Theorem 3.3 that $\Gamma = \Lambda \otimes_R \Gamma^\Lambda$. Now if an element of $\Lambda \otimes K$ commutes with every element of Λ , it must be in the center K of $\Lambda \otimes K$. Consequently, Γ^Λ is a subring of K and is a finitely generated R -module. Since R is integrally closed, it follows that $\Gamma^\Lambda = R$ and hence that $\Gamma = \Lambda$. Thus Λ is a maximal order.

A ring R is called a *regular domain* if R is a noetherian domain such that, for every prime ideal $\mathfrak{p}$ of R , the ring of quotients $R_{\mathfrak{p}}$ is a regular local ring.

THEOREM 7.2. *If R is a regular domain with quotient field K , then the homomorphism $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ induced by the inclusion map $R \rightarrow K$ is a monomorphism.*

Proof. Suppose that Λ is a central separable algebra over R such that the algebra class of Λ is in the kernel of the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$. Then $\Lambda \otimes K$ is a full matrix algebra over K and Λ is a maximal order in this algebra. By Theorem 2.1, we know that Λ is projective over R . We now apply to this situation Theorem 4.3 of [2] which asserts that under the present circumstances, $\Lambda = \text{Hom}_R(E, E)$ with E a finitely generated projective R -module. Thus $\Lambda \sim R$ and hence the kernel of the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ consists of the identity element alone. The mapping $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is therefore a monomorphism.

REMARK. If R is an integral domain with quotient field K , the mapping $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ need not be a monomorphism. We shall show that this is so by an example.

Let k be the field of real numbers, and $R = k[x, y]$ with $x^2 + y^2 = 0$. Then R is an integral domain. Let Δ be the algebra of quaternions over the reals k , and $\Lambda = \Delta \otimes_k R$. Then Λ is a central separable algebra over R . If $\mathfrak{m}$ is the ideal of R generated by x and y , then $\Lambda/\mathfrak{m}\Lambda \cong \Delta$, so that $\Lambda \sim R$. Now, -1 is a square in the quotient field K of R , i.e., $-1 = (x/y)^2$, and consequently K is a splitting field for the quaternions Δ . It follows that K is a splitting ring for Λ also. Thus in this case the mapping $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ has a nontrivial kernel. In general, it is an open question under what circumstances the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is a monomorphism.

PROPOSITION 7.3. *Let R be an integrally closed noetherian domain with quotient field K and Σ a central simple algebra over K . If Σ contains an order which is separable over R , then every maximal order of Σ which is projective as an R -module is separable over R .*

Proof. Let Λ be an order in Σ which is separable over R , and Γ a maximal order which is a projective R -module. By Proposition 7.1, Λ is also a maximal order. Let $\mathfrak{p}$ be a minimal prime ideal of R and form $\Lambda \otimes R_{\mathfrak{p}}$ and $\Gamma \otimes R_{\mathfrak{p}}$. These are orders in Σ over $R_{\mathfrak{p}}$. The maximality of Λ and Γ assure the maximality of $\Lambda \otimes R_{\mathfrak{p}}$ and $\Gamma \otimes R_{\mathfrak{p}}$ (Proposition 1.2 of [2]). Furthermore, $R_{\mathfrak{p}}$ is a discrete rank one valuation ring, so that $\Lambda \otimes R_{\mathfrak{p}}$ and $\Gamma \otimes R_{\mathfrak{p}}$ are isomorphic (Proposition 3.5 of [2]). Since Λ is separable over R , it follows that $\Lambda \otimes R_{\mathfrak{p}}$ is separable over $R_{\mathfrak{p}}$ so that $\Gamma \otimes R_{\mathfrak{p}}$ is also separable over $R_{\mathfrak{p}}$. Therefore, by Proposition 4.6, we conclude that Γ is separable over R .

It should be remarked that the condition that Γ be a projective R -module is essential for the validity of the result. (See footnote 3.)

Let R be a regular domain with quotient field K , and let $\mathfrak{p}$ be a minimal prime ideal of R . Then, by Theorem 7.2, the homomorphisms $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R_{\mathfrak{p}}) \rightarrow \mathfrak{B}(K)$ are monomorphisms. It will be convenient to treat these maps as identifications, so that we shall write $\mathfrak{B}(R) \subset \mathfrak{B}(R_{\mathfrak{p}}) \subset \mathfrak{B}(K)$.

PROPOSITION 7.4. *Let R be a regular domain with $\dim R \leq 2^{(*)}$. Then, as $\mathfrak{p}$ ranges over the minimal prime ideals of R , we have $\mathfrak{B}(R) = \bigcap \mathfrak{B}(R_{\mathfrak{p}})$.*

Proof. Since $\mathfrak{B}(R) \subset \mathfrak{B}(R_{\mathfrak{p}})$ we have of course $\mathfrak{B}(R) \subset \bigcap \mathfrak{B}(R_{\mathfrak{p}})$. In order to prove the inclusion in the other direction, let Δ be a central division algebra over K whose algebra class in $\mathfrak{B}(K)$ is in $\mathfrak{B}(R_{\mathfrak{p}})$, for every minimal prime ideal $\mathfrak{p}$ of R . Let Λ be a maximal order over R in Δ . The maximality of Λ implies the equality $\Lambda = \Lambda^{**}$ (Proposition 1.3 of [2]). Because R is a regular domain of dimension ≤ 2 , it follows that Λ is R -projective (Corollary to Proposition 4.7 of [2]).

Let $\mathfrak{p}$ be a minimal prime ideal of R . There is a central separable algebra $\Gamma_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ such that $\Gamma_{\mathfrak{p}} \otimes K \sim \Delta$. Since Δ is a division algebra, it follows that $\Gamma_{\mathfrak{p}} \otimes K$ is the algebra of $n \times n$ matrices over Δ , for some n . Because $\Lambda \otimes R_{\mathfrak{p}}$ is a maximal order over $R_{\mathfrak{p}}$ in Δ , it follows from Theorem 3.8 of [2] that the algebra of $n \times n$ matrices over $\Lambda \otimes R_{\mathfrak{p}}$ is a maximal order in $\Gamma_{\mathfrak{p}} \otimes K$. By Proposition 3.5 of [2], any two maximal orders in $\Gamma_{\mathfrak{p}} \otimes K$ are isomorphic. Hence $\Gamma_{\mathfrak{p}}$ is isomorphic to the algebra of $n \times n$ matrixes over $\Lambda \otimes R_{\mathfrak{p}}$, that is, $\Gamma_{\mathfrak{p}} \cong \Lambda \otimes R_{\mathfrak{p}} \otimes \text{Hom}_{R_{\mathfrak{p}}}(F, F)$ with F a free $R_{\mathfrak{p}}$ -module of rank n . It follows from Theorem 3.5 that $\Lambda \otimes R_{\mathfrak{p}}$ is separable over $R_{\mathfrak{p}}$. This being the case for every minimal prime, it now follows from Proposition 4.6 that Λ is separable over R . Since $\Delta = \Lambda \otimes K$, we find that the algebra class of Δ is indeed in $\mathfrak{B}(R)$, which completes the proof of the equality $\mathfrak{B}(R) = \bigcap \mathfrak{B}(R_{\mathfrak{p}})$.

It should be remarked that the condition on the dimension of R was used in the proof only to insure that Δ contains a maximal order which is R -projective. It is not known at the present time whether the restriction on the dimension of R is actually necessary.

We turn now to a different situation involving homomorphisms between Brauer groups. Let K be a field and $R = K[x]$, with x an indeterminate over K . From the homomorphisms $K \rightarrow R \rightarrow K$, we deduce homomorphisms $\mathfrak{B}(K) \rightarrow \mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$. Since $K \rightarrow R \rightarrow K$ is the identity on K , we have: $\mathfrak{B}(K) \rightarrow \mathfrak{B}(R)$ is a monomorphism, $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is an epimorphism and the sequence splits, so that $\mathfrak{B}(R)$ is the direct product of $\mathfrak{B}(K)$ and the kernel $\mathfrak{B}'(R)$ of $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$.

THEOREM 7.5. *If Λ is a central separable algebra over $K[x]$, then the algebra class of Λ is in the image of $\mathfrak{B}(K)$ if, and only if, there exists a separable extension L of K of finite degree such that Λ is split by $L[x]$. The mapping $\mathfrak{B}(K) \rightarrow \mathfrak{B}(K[x])$ is an isomorphism if, and only if, K is a perfect field.*

Proof. Suppose first that the class of Λ is in the image of $\mathfrak{B}(K) \rightarrow \mathfrak{B}(K[x])$. Then there is a central simple algebra Σ over K such that $\Sigma \otimes_K K[x] \sim \Lambda$. There is a separable extension field L of finite degree over K which splits Σ . Clearly then $L[x]$ splits Λ .

(*) $\dim R = \max \dim R_{\mathfrak{p}}$, as $\mathfrak{p}$ ranges over the prime ideals of R .

Assume now that Λ is split by $L[x]$ with L separable over K . Then, by extending L if necessary, we may suppose that L is a Galois extension of K , with Galois group G . Referring to Theorem A.8 of the appendix, we see that $L[x]$ is a Galois extension of $K[x]$ with group G , for we have $L[x] = L \otimes_K K[x]$ and L is a Galois extension of K with the group G . Since $L[x]$ is a principal ideal ring, we may apply Theorem A.15 of the appendix, and conclude that Λ is equivalent to a crossed product Γ formed from the Galois extension $L[x]$ of $K[x]$ and a cocycle $f \in H^2(G, U(L[x]))$. But the units of $L[x]$ are the nonzero elements of L , so that $f \in H^2(G, U(L))$, and therefore $\Gamma = \Gamma_0 \otimes_K K[x]$, where Γ_0 is the crossed-product formed from L over K and f . Thus $\Lambda \sim \Gamma_0 \otimes_K K[x]$, and the algebra class of Λ is in the image of $\mathfrak{B}(K)$ in $\mathfrak{B}(K[x])$.

Now suppose that K is a perfect field. If $\bar{K}$ is the algebraic closure of K , then by Tsen's theorem [9], we know that $\mathfrak{B}(\bar{K}(x)) = (1)$. Since $\bar{K}[x]$ is a regular domain, it follows from Theorem 7.2 that $\mathfrak{B}(\bar{K}[x]) = (1)$ and therefore every central separable algebra over $K[x]$ is split by $\bar{K}[x]$. But, if Λ is such an algebra, the fact that $\bar{K}[x]$ splits Λ shows that Λ is already split by $L[x]$ with L an extension of finite degree over K . Since K is perfect, L is a separable extension of K . Thus if K is perfect, we find that the mapping $\mathfrak{B}(K) \rightarrow \mathfrak{B}(K[x])$ is an epimorphism and hence an isomorphism.

If K is not perfect, we shall show that the kernel $\mathfrak{B}'$ of $\mathfrak{B}(K[x]) \rightarrow \mathfrak{B}(K)$ is not trivial by explicitly constructing a nontrivial element of the kernel.

Let y be a root of $y^p - y - x = 0$, and $\Omega = K(x)(y)$ where p is the characteristic of K . It is well known that Ω is a cyclic extension of $K(x)$ of degree p , and it is easily verified that the integral closure of $K[x]$ in Ω is $K[x][y] = K[y]$. Since the discriminant of the polynomial defining the extension is -1 , it follows that $K[y]$ is unramified over $K[x]$, so that $K[y]$ is a Galois extension of $K[x]$ with the same cyclic Galois group (see Proposition A.6).

Assuming that K is not perfect, let $c \in K$ with $c \notin K^p$. Then a simple calculation shows that c as an element of $K(x)$ is not a norm from Ω . Thus, c determines a crossed-product Σ over $K(x)$ which is not trivial. Using the fact that $K[y]$ is a Galois extension of $K[x]$, the non-norm c determines a crossed-product Λ over $K[x]$. Since $\Lambda \otimes K(x) = \Sigma$ and Σ is not the trivial algebra, it follows that Λ is not a trivial algebra over $K[x]$. Now Λ is generated over $K[x]$ by elements α and β with the relations: $\alpha^p - \alpha = x$, $\beta^p = c$, $\beta\alpha = (\alpha+1)\beta$. The image $\bar{\Lambda}$ of Λ under the map $K[x] \rightarrow K$ is generated over K by elements $\bar{\alpha}$ and $\bar{\beta}$ with the relations $\bar{\alpha}^p - \bar{\alpha} = 0$, $\bar{\beta}^p = c$ and $\bar{\beta}\bar{\alpha} = (\bar{\alpha}+1)\bar{\beta}$. We shall show that $\bar{\Lambda}$ is a full matrix algebra over K . Let $L = K(t)$ with $t^p = c$ and let $\alpha', \beta' \in \text{Hom}_K(L, L)$ be defined as follows: α' is the derivation of L over K given by $\alpha'(t^n) = -nt^{n-1}$ and β' is multiplication by t . Then one verifies directly that α' and β' satisfy the same relations over K as do $\bar{\alpha}$ and $\bar{\beta}$, so that there is a homomorphism from $\bar{\Lambda}$ to $\text{Hom}_K(L, L)$ under which $\bar{\alpha} \rightarrow \alpha'$ and $\bar{\beta} \rightarrow \beta'$. Since $\bar{\Lambda}$ is a central simple algebra over K of dimension p^2 and $\text{Hom}_K(L, L)$ also has dimension p^2 over K , it follows that $\bar{\Lambda} \cong \text{Hom}_K(L, L)$. Thus, the class of

Λ is a nontrivial element of $\mathfrak{B}'(K[x])$. This completes the proof of the theorem.

Some further facts can be proved about $\mathfrak{B}'(K[x])$.

PROPOSITION 7.6. *If L is a separable extension of K , then the restriction of the map $\mathfrak{B}(K[x]) \rightarrow \mathfrak{B}(L[x])$ to $\mathfrak{B}'(K[x])$ is a monomorphism, and maps $\mathfrak{B}'(K[x])$ into $\mathfrak{B}'(L[x])$. If p is the characteristic of K , then every element of $\mathfrak{B}'(K[x])$ has order a power of p .*

Proof. Since $\mathfrak{B}(K)$ and $\mathfrak{B}'(K[x])$ have only the identity element in common, the first part of Theorem 7.5 shows that $L[x]$ cannot split any nontrivial element of $\mathfrak{B}'(K[x])$ if L is separable over K . That $\mathfrak{B}'(K[x])$ maps into $\mathfrak{B}'(L[x])$ is immediate.

Let c be a nontrivial element of $\mathfrak{B}'(K[x])$. If $\bar{K}$ is the algebraic closure of K , then c is split by $\bar{K}[x]$, so that there is an extension L of finite degree over K such that c is split by $L[x]$. Let L_0 be the maximal separable extension of K in L . Then the mapping $\mathfrak{B}(K[x]) \rightarrow \mathfrak{B}(L_0[x])$ is a monomorphism on the subgroup $\mathfrak{B}'(K[x])$, so that the image d of c in $\mathfrak{B}'(L_0[x])$ has the same order as c . Now, d is split by $L[x]$ so that the image d' of d in $\mathfrak{B}(L_0(x))$ is split by $L(x)$. Since the mapping $\mathfrak{B}(L_0[x]) \rightarrow \mathfrak{B}(L_0(x))$ is a monomorphism, the order of d' is equal to the order of d , hence to that of c . But L is a purely inseparable extension of L_0 so that $[L: L_0] = p^h$ and therefore $[L(x): L_0(x)] = p^h$. Because $L(x)$ is a splitting field of d' , it follows that the order of d' divides p^h . Thus the order of c is a power of p . This completes the proof.

PROPOSITION 7.7. *If R is a regular domain of characteristic zero, then $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R[x])$ is an isomorphism.*

Proof. From the sequence $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R[x]) \rightarrow \mathfrak{B}(R)$ it follows that the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(R[x])$ is a monomorphism, so that we need only show that the map $\mathfrak{B}(R[x]) \rightarrow \mathfrak{B}(R)$ is a monomorphism. Let K be the quotient field of R . Then we have the commutative diagram:

$$\begin{array}{ccc} \mathfrak{B}(R[x]) & \rightarrow & \mathfrak{B}(R) \\ \downarrow & & \downarrow \\ \mathfrak{B}(K[x]) & \rightarrow & \mathfrak{B}(K) \end{array}$$

in which both vertical maps are monomorphisms because R and $R[x]$ are regular domains⁽⁷⁾, while the lower horizontal map is an isomorphism. It follows that the upper horizontal map is a monomorphism.

REMARK. The proof of the above Proposition 7.7 makes use of the hypothesis that $\mathfrak{B}(K[x]) \rightarrow \mathfrak{B}(K)$ is a monomorphism. Consequently by Theorem 7.5

⁽⁷⁾ The fact that regularity of R implies regularity of $R[x]$ is well known and can be deduced easily from the theorem that a ring of quotients of a regular domain is regular. See, for example, D. G. Northcott, J. London Math. Soc. vol. 33 (1958) pp. 36-39.

we must suppose that K is a perfect field. This explains the hypothesis that R be of characteristic 0. Namely, an integrally closed noetherian domain R whose quotient field is perfect and of nonzero characteristic is a field. For if R is not a field, localizing R with respect to a minimal prime ideal would give a discrete rank one valuation ring whose maximal ideal is principal, generated by some element x . It is clear that $x^{1/p}$ cannot be in the field of quotients of R .

8. Valuation rings. In this section, R will denote a discrete rank one valuation ring with maximal ideal $\mathfrak{m}$. We shall denote $R/\mathfrak{m}$ by k and the quotient field of R by K .

PROPOSITION 8.1. *Suppose that k is a perfect field and Λ is a central separable R -algebra such that $\Lambda/\mathfrak{m}\Lambda$ is a division algebra. Then $\Delta = K \otimes \Lambda$ is a division algebra and Λ is the only maximal order in Δ . If L is any subfield of Δ (containing K) and S is the integral closure of R in L , then S is a discrete rank one valuation ring and is separable over R , and L is separable over K .*

Proof. The fact that Δ is a division algebra and that Λ is the only maximal order in Δ both follow directly from the hypothesis that $\Lambda/\mathfrak{m}\Lambda$ is a division algebra (see Theorem 3.11 of [2]).

Let L be a subfield of Δ containing K , and S the integral closure of R in L . If a is an element of S , then the ring $R[a]$ is a finitely generated R -module and is therefore contained in some maximal order of Δ . Since Λ is the only maximal order, it follows that $a \in \Lambda$, so that we have $S \subset \Lambda$. It follows from this, and from the fact that S is integrally closed, that $L \cap \Lambda = S$. Therefore Λ/S is a torsion-free R -module and hence a free R -module. Therefore S is a direct summand of Λ as an R -module, so that $(\mathfrak{m}\Lambda) \cap S = \mathfrak{m}S$. Thus, $S/\mathfrak{m}S$ is a subring of $\Lambda/\mathfrak{m}\Lambda$. Since $\Lambda/\mathfrak{m}\Lambda$ is a division algebra, it follows that $S/\mathfrak{m}S$ is a field extension of the perfect field $R/\mathfrak{m}$ and hence, by Theorem 4.7, S is separable over R . Also, because $S/\mathfrak{m}S$ is a field, we have that $\mathfrak{m}S$ is a maximal ideal in S , so that S is a discrete rank one valuation ring. It follows immediately that L is separable over K , completing the proof of the proposition.

Denote by $\hat{R}$ the completion of R . Then $\hat{R}$ is again a discrete rank one valuation ring with maximal ideal $\hat{\mathfrak{m}} = \mathfrak{m}\hat{R}$. Also, $\hat{K} = K \otimes \hat{R}$ is the quotient field of $\hat{R}$. Since both R and $\hat{R}$ are regular domains, we have by Theorem 7.2 (1) $\rightarrow \mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ and (1) $\rightarrow \mathfrak{B}(\hat{R}) \rightarrow \mathfrak{B}(\hat{K})$ are exact. We also have the following diagram which is obviously commutative:

$$\begin{array}{ccccc} (1) & \rightarrow & \mathfrak{B}(R) & \rightarrow & \mathfrak{B}(K) \\ & & \downarrow & & \downarrow \\ (1) & \rightarrow & \mathfrak{B}(\hat{R}) & \rightarrow & \mathfrak{B}(\hat{K}). \end{array}$$

PROPOSITION 8.2. *The kernel of the map $\mathfrak{B}(K) \rightarrow \mathfrak{B}(\hat{K})$ coincides with the kernel of $\mathfrak{B}(R) \rightarrow \mathfrak{B}(\hat{R})$.*

Proof. It is clear that $\ker(\mathfrak{B}(R) \rightarrow \mathfrak{B}(\hat{R})) \subset \ker(\mathfrak{B}(K) \rightarrow \mathfrak{B}(\hat{K}))$. Suppose that Σ is a central simple algebra over K such that $\Sigma \otimes \hat{K}$ is a full matrix algebra over $\hat{K}$. Let Λ be a maximal order in Σ over R . Then, $\hat{\Lambda} = \Lambda \otimes \hat{R}$ is a maximal order over $\hat{R}$ (see Proposition 2.5 of [2]). By Proposition 7.3, it follows that $\hat{\Lambda}$ is separable over $\hat{R}$. But $\hat{\Lambda}/\hat{m}\hat{\Lambda} \cong \Lambda/m\Lambda$, so that $\Lambda/m\Lambda$ is separable over R/m and hence, by Theorem 4.7, Λ is separable over R . Thus the algebra class of Σ is in $\mathfrak{B}(R)$, and therefore $\ker(\mathfrak{B}(K) \rightarrow \mathfrak{B}(\hat{K})) \subset \ker(\mathfrak{B}(R) \rightarrow \mathfrak{B}(\hat{R}))$. This establishes the equality of the two kernels, and completes the proof of the proposition.

The following result, which is stated without proof, is classical in the theory of algebras. See Theorem 8 of Chapter 5 of [7] and Theorem 2.5 of [1].

THEOREM 8.3. *Let R be a complete discrete rank one valuation ring whose residue class field R/m is perfect, and let Σ be a central simple algebra over the quotient field K of R . Then Σ has a splitting field L of finite degree over K , such that the integral closure S of R in L is separable over R . The ring S is necessarily again a discrete rank one valuation ring.*

Using the above theorem, we have the following result.

PROPOSITION 8.4. *Let R be a discrete rank one valuation ring such that $k = R/m$ is perfect, and let Λ be a maximal order in a central simple algebra over K . If $\mathfrak{N}$ is the radical of Λ , then Λ is separable over R if, and only if, R/m is the center of $\Lambda/\mathfrak{N}$.*

Proof. If Λ is separable over R , then $\mathfrak{N} = m\Lambda$ and we know in this case that R/m is the center of $\Lambda/m\Lambda$. Assume now that R/m is the center of $\Lambda/\mathfrak{N}$. If $\hat{R}$ is the completion of R , then $\hat{\Lambda}/\hat{m}\hat{\Lambda} = \Lambda/m\Lambda$ so that Λ is separable over R if, and only if, $\hat{\Lambda}$ is separable over $\hat{R}$. Furthermore the radical $\hat{\mathfrak{N}}$ of $\hat{\Lambda}$ is equal to $\mathfrak{N} \otimes \hat{R}$, so that $\hat{\Lambda}/\hat{\mathfrak{N}} = \Lambda/\mathfrak{N}$. Thus we may assume that R itself is complete.

Set $\Sigma = K \otimes \Lambda$ and let L be a splitting field of Σ of the type described in the previous theorem, i.e., the integral closure S of R in L is separable over R . Then mS is the maximal ideal of S and S/mS is a separable field extension of R/m .

Now $\Lambda/\mathfrak{N}$ is central simple over R/m , so that $S/mS \otimes_k \Lambda/\mathfrak{N}$ is again a simple algebra. Denote by $\mathfrak{M}$ the kernel of the mapping $S \otimes_R \Lambda \rightarrow S/mS \otimes \Lambda/\mathfrak{N}$, so that $\mathfrak{M}$ is a maximal two-sided ideal in $S \otimes_R \Lambda$. Since $S/mS \otimes_k \Lambda/\mathfrak{N} = S \otimes_R \Lambda/\mathfrak{M}$, we have the exact sequence:

$$0 \rightarrow S \otimes_R \mathfrak{N} \rightarrow S \otimes_R \Lambda \rightarrow S \otimes_R \Lambda/\mathfrak{M} \rightarrow 0$$

and therefore $\mathfrak{M} = S \otimes_R \mathfrak{N}$. But $S \otimes_R \mathfrak{N}$ is contained in the radical of $S \otimes \Lambda$,^(*) while $\mathfrak{M}$, being a maximal two-sided ideal, contains the radical of $S \otimes \Lambda$. It

^(*) This assertion follows easily from the observation that if Δ is a subring of Ω such that Ω is a finitely generated left Δ -module, then the extension to Ω of the radical of Δ is contained in the radical of Ω .

follows therefore that $\mathfrak{M}$ is equal to the radical of $S \otimes \Lambda$ and hence that the radical of $S \otimes \Lambda$ is a maximal two-sided ideal.

Applying Theorem 2.3 of [2], we have the following situation: since Λ is a maximal order, it is hereditary, and since S is separable over R , it follows from Theorem 1.8 that the algebra $S \otimes_R \Lambda$ is still hereditary. Since the radical of $S \otimes \Lambda$ is a maximal two-sided ideal, a second application of Theorem 2.3 of [2] enables us to conclude that $S \otimes \Lambda$ is a maximal order over S in $L \otimes_K \Sigma$. But L is a splitting field of Σ . Therefore, every maximal order in $L \otimes \Sigma$ is separable over S . (See Theorem 4.3 of [2].) Thus knowing that $S \otimes \Lambda$ is separable over S and S is separable over R , we find that Λ is separable over R . This completes the proof of the proposition.

COROLLARY 8.5. *If R is a discrete rank one valuation ring such that $R/\mathfrak{m}$ is algebraically closed, then $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is an epimorphism, hence an isomorphism.*

Proof. Let Σ be a central simple algebra over K and Λ a maximal order in Σ . If $\mathfrak{N}$ is the radical of Λ , then $\Lambda/\mathfrak{N}$ is a simple algebra so that the center of $\Lambda/\mathfrak{N}$ is a field extension of finite degree over $R/\mathfrak{m}$. Because $R/\mathfrak{m}$ is algebraically closed, it follows that the center of $\Lambda/\mathfrak{N}$ is $R/\mathfrak{m}$ and therefore, by the above proposition, it follows that Λ is separable over R . Thus we have $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is an epimorphism. Since we know already that the map is a monomorphism, we conclude that $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is an isomorphism.

REMARK. If in addition to the hypotheses in the corollary we also assume that R is complete, then it follows from Corollary 6.2 that $\mathfrak{B}(R) = (1)$. But if R is not complete, it may well happen that $\mathfrak{B}(R) \neq (1)$. For example, let k be the field of real numbers, $K = k(x)$ and R the valuation ring defined by $x^2 + 1$. Then the residue class field of R is the field of complex numbers, while $\mathfrak{B}(R) \neq (1)$ since $(1) \neq \mathfrak{B}(k) \subset \mathfrak{B}(k[x]) \subset \mathfrak{B}(R)$.

We bring this section to an end with a description of some new algebra invariants of a discrete rank one valuation ring which may merit further study. In [2] it was proved (Theorem 2.3) that every maximal order over R in a central simple algebra is hereditary. An example was provided to show that the converse is not true.

For R a discrete rank one valuation ring, denote by $\mathcal{H}'(R)$ the set of all hereditary orders over R , and by $\mathfrak{M}'(R) \subset \mathcal{H}'(R)$ the maximal orders. In exactly the same way as for separable algebras, one can define an equivalence relation in $\mathcal{H}'(R)$ as follows: if $\Lambda, \Lambda' \in \mathcal{H}'(R)$, then $\Lambda \sim \Lambda'$ if there exist finitely generated free R -modules, E and E' , such that $\Lambda \otimes \text{Hom}_R(E, E) \cong \Lambda' \otimes \text{Hom}_R(E', E')$. That this is in fact an equivalence relation is immediate. We denote by $\mathcal{H}(R)$ the set of equivalence classes of $\mathcal{H}'(R)$, and by $\mathfrak{M}(R)$ the subset of $\mathcal{H}(R)$ of those classes which contain elements of $\mathfrak{M}'(R)$. It will turn out as a result of the proposition to be proved in a moment, that each equivalence class in $\mathfrak{M}(R)$ consists exclusively of maximal orders.

PROPOSITION 8.6. *Let Λ be a central separable R -algebra and Γ an order over R in a central simple algebra. Then $\Lambda \otimes \Gamma$ is hereditary if, and only if, Γ is hereditary. $\Lambda \otimes \Gamma$ is maximal if, and only if, Γ is maximal.*

Proof. We shall only prove the second statement, the first being a consequence of Theorem 1.8. In view of Theorem 2.3 of [2], the second statement is equivalent to the following: the radical $\mathfrak{N}$ of Γ is a maximal two-sided ideal if, and only if, the radical $\mathfrak{M}$ of $\Lambda \otimes \Gamma$ is a maximal two-sided ideal. From the exact sequence $0 \rightarrow \mathfrak{N} \rightarrow \Gamma \rightarrow \Gamma/\mathfrak{N} \rightarrow 0$ we deduce the exact sequence $0 \rightarrow \Lambda \otimes_R \mathfrak{N} \rightarrow \Lambda \otimes_R \Gamma \rightarrow \Lambda \otimes_R \Gamma/\mathfrak{N} \rightarrow 0$. Now, $\Gamma/\mathfrak{N}$ is a semi-simple algebra over $R/\mathfrak{m}$, and $\Lambda \otimes_R \Gamma/\mathfrak{N} = \Lambda/\mathfrak{m}\Lambda \otimes_{R/\mathfrak{m}} \Gamma/\mathfrak{N}$. Since $\Lambda/\mathfrak{m}\Lambda$ is a central simple algebra over $R/\mathfrak{m}$, it follows that $\Lambda/\mathfrak{m}\Lambda \otimes_{R/\mathfrak{m}} \Gamma/\mathfrak{N}$ is still semi-simple so that we have $\Lambda \otimes \mathfrak{N} \supset \mathfrak{M}$. However, it is clear that $\Lambda \otimes \mathfrak{N} \subset \mathfrak{M}$ (see footnote 8), whence $\mathfrak{M} = \Lambda \otimes_R \mathfrak{N}$. Thus we have $\Lambda \otimes \Gamma/\mathfrak{M} = \Lambda/\mathfrak{m}\Lambda \otimes_{R/\mathfrak{m}} \Gamma/\mathfrak{N}$. Because $\Lambda/\mathfrak{m}\Lambda$ is a central simple algebra over $R/\mathfrak{m}$ it is clear that $\Lambda \otimes \Gamma/\mathfrak{M}$ is a simple algebra if, and only if, $\Gamma/\mathfrak{N}$ is a simple algebra. This proves the assertion.

COROLLARY 8.7. *If the hereditary order Γ is equivalent to a maximal order Γ' , then Γ is also maximal.*

Proof. We have finitely generated free R -modules E and E' such that $\Gamma \otimes \text{Hom}_R(E, E) \cong \Gamma' \otimes \text{Hom}_R(E', E')$. Using the above proposition we may conclude that $\Gamma' \otimes \text{Hom}(E', E')$ is a maximal order and therefore, using the proposition again, it follows that Γ is maximal.

Since any two maximal orders in the same simple algebra are isomorphic (Proposition 3.5 of [2]), it is clear that $\mathfrak{M}(R)$ is in a natural one-to-one correspondence with $\mathfrak{B}(K)$. Using Proposition 8.6, the pairing $\Lambda, \Gamma \rightarrow \Lambda \otimes \Gamma$ with Λ separable and $\Gamma \in \mathcal{K}'(R)$, induces a representation of $\mathfrak{B}(R)$ by permutations of $\mathcal{K}(R)$. In this representation, the operation of $\mathfrak{B}(R)$ on $\mathfrak{M}(R)$ is the one arising from the fact that $\mathfrak{B}(R)$ is a subgroup of $\mathfrak{B}(K)$. By Proposition 8.6, an orbit under $\mathfrak{B}(R)$ of $\mathcal{K}(R)$ meets $\mathfrak{M}(R)$ only if that orbit is entirely contained in $\mathfrak{M}(R)$.

PROPOSITION 8.8. *The operation of $\mathfrak{B}(R)$ on $\mathcal{K}(R)$ is without fixed points.*

Proof. Suppose that Λ is a separable order, Γ a hereditary order such that $\Lambda \otimes \Gamma \sim \Gamma$. By tensoring with K , we find $(\Lambda \otimes K) \otimes (\Gamma \otimes K) \sim \Gamma \otimes K$ so that $\Lambda \otimes K \sim K$. But the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(K)$ is a monomorphism. It follows therefore that the algebra class of Λ in $\mathfrak{B}(R)$ is the identity element.

Appendix. Galois theory. Let S be a commutative ring and G a finite group. Given a representation of G by ring automorphisms of S , there is associated a "twisted" group ring or a trivial crossed-product $\Delta(S; G)$ defined as follows: $\Delta(S; G)$ is a free (left) S -module with free generators $\{u_\sigma\}$ indexed by G and with multiplication defined by $(au_\rho)(bu_\sigma) = a\rho(b)u_{\rho\sigma}$. The ring Δ has u_1 for its identity element and the map $x \rightarrow xu_1$ imbeds S as a subring of Δ .

S has a natural structure as a left Δ -module by means of the operation $(au_\sigma)x = a\sigma(x)$. In this, the operation of S as a subring of Δ , on S as a Δ -module coincides with the multiplication in S . Because of this fact, it is simple to verify that $\text{Hom}_\Delta(S, S)$ may be identified with the subring of S consisting of the elements left fixed by G . If R is any subring of S consisting of elements left fixed by G , then $R \subset \text{Hom}_\Delta(S, S)$ so that the structure of S as a Δ -module defines a homomorphism $\delta: \Delta \rightarrow \text{Hom}_R(S, S)$. Explicitly, we have $\delta(au_\sigma)(x) = a\sigma(x)$.

If R is a subring of the commutative ring S , and G is a finite group represented by automorphisms of S leaving R elementwise fixed, then we shall say that S is a *Galois extension of R relative to G* if S is a finitely generated projective R -module and δ is an isomorphism of $\Delta(S; G)$ with $\text{Hom}_R(S, S)$.

It is a consequence of the Galois theory of fields that the present definition agrees with the usual one in the case of fields⁽⁹⁾. It should also be remarked that when S is a Galois extension of R relative to G , then the representation of G by automorphisms of S is certainly faithful.

PROPOSITION A.1. *S is a Galois extension of R relative to G if, and only if, $\mathfrak{T}_\Delta(S) = \Delta$ and R is the fixed subring of S under G .*

Proof. Assume first that S is a Galois extension of R relative to G . Since S is a finitely generated projective and faithful R -module, it follows from Proposition 5.1 that the center of $\text{Hom}_R(S, S)$ is R itself. Because δ is an isomorphism, it follows that the center of $\Delta(S; G)$ is R . On the other hand, it is clear that the center of $\Delta(S; G)$ is the fixed subring of S under G . Also, the fact that S is a finitely generated projective R -module implies that the trace ideal of S in $\text{Hom}_R(S, S)$ is $\text{Hom}_R(S, S)$ itself (Proposition A.3 of [2]), so that $\mathfrak{T}_\Delta(S) = \Delta$.

Assuming that R is the fixed ring under G and that $\mathfrak{T}_\Delta(S) = \Delta$, it follows from Theorem A.2 of [2] that S is a finitely generated projective R -module, and that $\Delta = \text{Hom}_R(S, S)$. Thus, S is a Galois extension of R relative to G .

Set $s = \sum u_\sigma \in \Delta(S; G)$. It is clear that $u_\sigma s = s$, for every $\sigma \in G$, so that s maps S into the fixed ring of G .

PROPOSITION A.2. *Let $R = \text{Hom}_\Delta(S, S)$, and suppose that $\delta: \Delta(S; G) \rightarrow \text{Hom}_R(S, S)$ is an isomorphism. Then, $\delta^{-1}\text{Hom}_R(S, R) = sS$.*

Proof. If $a \in S$, then for $x \in S$ we have $\delta(sa)(x) = \sum \sigma(ax) \in R$, so that $\delta(sa) \in \text{Hom}_R(S, R)$. Suppose $f = \delta(y) \in \text{Hom}_R(S, R)$. If $y = \sum a_\sigma u_\sigma$, then for every $x \in S$, we have $\sum a_\sigma \sigma(x) \in R$, so that $\rho(\sum a_\sigma \sigma(x)) = \sum a_\sigma \sigma(x)$. This shows that $\sum_\tau \rho(a_{\sigma^{-1}\tau})\tau(x) = \sum_\tau a_\tau \tau(x)$. But δ is an isomorphism; therefore $\rho(a_{\sigma^{-1}\tau}) = a_\tau$, or $a_\sigma = \sigma(a_1)$. Thus, $y = \sum \sigma(a_1)u_\sigma = sa_1$.

⁽⁹⁾ In case R is a field, our definition of Galois extension is equivalent to that of Normal-ring studied by Teichmüller in [8].

Suppose that S is a finitely generated projective R -module with R a subring of S . Then, by Proposition A.1 of [2], $\mu: S \otimes_R \text{Hom}_R(S, R) \rightarrow \text{Hom}_R(S, S)$ defined by $\mu(a \otimes f)(x) = f(x)a$ is an isomorphism. At the same time, we also have the map $\tau: S \otimes_R \text{Hom}_R(S, R) \rightarrow R$ defined by $\tau(a \otimes f) = f(a)$. If $x \in S$, we define the *trace* of x to be $\tau\mu^{-1}(x)$ and denote it by $t(x)$. As defined, t is an element of $\text{Hom}_R(S, R)$. The fact that S is a finitely generated projective R -module implies the existence of elements $x_1, \dots, x_n \in S$ and $f_1, \dots, f_n \in \text{Hom}_R(S, R)$ such that $\sum f_i(x)x_i = x$ for all x in S . Then, it is readily verified that $t(x) = \sum f_i(xx_i)$.

PROPOSITION A.3. *If S is a Galois extension of R relative to G , then $t = \delta(s)$. Furthermore, t maps S onto R and therefore R is a direct summand of S as an R -module.*

Proof. As above, we have elements $x_i \in S$ and $f_i \in \text{Hom}_R(S, R)$ such that $x = \sum f_i(x)x_i$ for $x \in S$. By Proposition A.2, there are elements $y_i \in S$ such that $f_i = \delta(sy_i)$. Therefore, $x = \sum_i \delta(sy_i)(x)x_i = \sum_{i,\sigma} \sigma(y_i)x_i\sigma(x)$. Because δ is an isomorphism, it follows that $\sum_{i,\sigma} \sigma(y_i)x_i u_\sigma = 1$. In particular, we have $\sum_i x_i y_i = 1$. But $t(x) = \sum f_i(xx_i)$, so that $t(x) = \sum_{i,\sigma} \sigma(xx_i y_i) = \sum \sigma(x)$. Thus, $t = \delta(s)$.

Because S is a finitely generated projective faithful R -module, we have $\mathfrak{T}_R(S) = R$ (Proposition A.3 of [2]). Therefore there are elements $z_i \in S$ and $g_i \in \text{Hom}_R(S, R)$ with $\sum g_i(z_i) = 1$. If $g_i = \delta(sw_i)$, we have $1 = \sum_{i,\sigma} \sigma(w_i z_i)$ or $t(\sum_i w_i z_i) = 1$. Thus t maps S onto R .

Assuming once more that R is a subring of S and that S is a finitely generated R -module, we have $\text{Hom}_R(S, R) \subset \text{Hom}_R(S, S)$ with $\text{Hom}_R(S, R)$ a right S -submodule of $\text{Hom}_R(S, S)$. Since $t \in \text{Hom}_R(S, R)$, we have $tS \subset \text{Hom}_R(S, R)$.

PROPOSITION A.4. *Let R be a subring of S and suppose that S is a finitely generated projective R -module. Then, S is separable over R if, and only if, $\text{Hom}_R(S, R)$ is a free right S -module having t as free generator.*

Proof. Because S is a finitely generated projective R -module, there are elements $x_1, \dots, x_n \in S$ and $f_1, \dots, f_n \in \text{Hom}_R(S, R)$ such that $\sum f_i(x)x_i = x$, for all $x \in S$. In terms of these elements, we have $t(x) = \sum f_i(xx_i)$.

Consider the following diagram:

$$\begin{array}{ccc} S \otimes_R S & \xrightarrow{\beta} & \text{Hom}_R(\text{Hom}_R(S, R), S) \\ \phi \searrow & & \swarrow \alpha \\ & S & \end{array}$$

where, as usual, $\phi(x \otimes y) = xy$ and $\beta(x \otimes y)(f) = f(y)x$ and $\alpha(h) = \sum_i h(f_i)x_i$. Furthermore, the fact that S is a finitely generated projective R -module implies that β is an isomorphism. In addition, $\text{Hom}_R(\text{Hom}_R(S, R), S)$ is an S^e -module through the operations: $(x \otimes y)h(f) = xh(f \circ y)$. In this structure,

β is an S^e -map. Therefore the image of A under β coincides with the annihilator of J in $\text{Hom}_R(\text{Hom}_R(S, R), S)$, while the annihilator of J is just $\text{Hom}_S(\text{Hom}_R(S, R), S)$. It is to be noted that in the latter expression we are considering $\text{Hom}_R(S, R)$ as a right S -module. Thus S is separable over R if, and only if, the image of $\text{Hom}_S(\text{Hom}_R(S, R), S)$ under α is S itself. Also, when S is separable, the restriction of ϕ to A is an isomorphism. Thus if α_0 is the restriction of α to $\text{Hom}_S(\text{Hom}_R(S, R), S)$, then S is separable over R if, and only if, $\alpha_0: \text{Hom}_S(\text{Hom}_R(S, R), S) \rightarrow S$ is an isomorphism. Taking into account the fact that $t(x) = \sum f_i(xx_i)$, we have $\alpha_0(h) = h(t)$.

Define $q: S \rightarrow \text{Hom}_R(S, R)$ by $q(x) = t \circ x$. Clearly q is a right S -map, and its dual

$$q': \text{Hom}_S(\text{Hom}_R(S, R), S) \rightarrow \text{Hom}_S(S, S) = S$$

is given by $q'(h) = h(q(1)) = h(t)$. Thus, $q' = \alpha_0$. Therefore if q is an isomorphism, then $\alpha_0 = q'$ is also an isomorphism and S is separable over R .

Now suppose that S is separable over R so that $q' = \alpha_0$ is an isomorphism. Because α_0 is an isomorphism, its dual

$$\alpha'_0: \text{Hom}_S(S, S) \rightarrow \text{Hom}_S(\text{Hom}_S(\text{Hom}_R(S, R), S), S)$$

is also an isomorphism. The following diagram is commutative:

$$\begin{array}{ccc} S = \text{Hom}_S(S, S) & \xrightarrow{\alpha'_0} & \text{Hom}_S(\text{Hom}_S(\text{Hom}_R(S, R), S), S) \\ \downarrow q & \nearrow \gamma & \\ & \text{Hom}_R(S, R) & \end{array}$$

where γ is the natural imbedding of a module into its second dual. Now, $\text{Hom}_R(S, R)$ is R -projective because S is R -projective. It follows from Theorem 1.8 that $\text{Hom}_R(S, R)$ is S -projective. Therefore γ is an isomorphism, and since α'_0 is an isomorphism, it follows that q is an isomorphism. This completes the proof of the proposition.

COROLLARY A.5. *If S is a Galois extension of R relative to a group G , then S is separable over R .*

Proof. Combining Propositions A.2 and A.3 shows that the map $x \rightarrow t \circ x$ is an isomorphism of S on $\text{Hom}_R(S, R)$. Therefore it follows from Proposition A.4 that S is separable over R .

PROPOSITION A.6. *Let S be a commutative ring and G a finite group represented by automorphisms of S . Let R be a subring of S whose elements are left fixed by the elements of G , and such that S is a finitely generated projective R -module as well as a separable algebra over R . If $t = \delta(s)$, then $\delta: \Delta(S; G) \rightarrow \text{Hom}_R(S, S)$ is an epimorphism. If in addition δ is a monomorphism, then S is a Galois extension of R relative to G .*

Proof. The fact that S is a finitely generated projective R -module implies that the map $\mu: S \otimes_R \text{Hom}_R(S, R) \rightarrow \text{Hom}_R(S, S)$ given by $\mu(x \otimes f)(y) = f(y)x$ is an isomorphism (Proposition A.1 of [2]). Now if $f \in \text{Hom}_R(S, R)$, it follows from Proposition A.4 that $f = t \circ y$, for some $y \in S$. In view of the fact that $t = \delta(s)$, we have $f = \delta(sy)$, and therefore that $\mu(x \otimes f) = \delta(\sum x \sigma(y) u_\sigma)$. Thus, δ is an epimorphism. If δ is also a monomorphism, then it follows from the definition that S is a Galois extension of R .

THEOREM A.7. *Let S be a commutative ring, R a subring of S such that S is separable over R and such that S is a free R -module of finite rank n . Then, S can be imbedded in a Galois extension of R relative to a group which is isomorphic to the symmetric group of degree n .*

Proof. Set $\Gamma = S \otimes_R \cdots \otimes_R S$ (n factors) which we shall consider as an R -algebra. Denote by G the symmetric group of degree n ; G has a natural representation by automorphisms of Γ in which the elements of G permute the factors. The required Galois extension of R will be constructed as a factor ring of Γ .

We temporarily suppress the multiplication in S and Γ , considering them only as R -modules. Let E be the homogeneous component of degree n of the exterior algebra of S over R . Since S is free of rank n over R , we have that E is a free R -module of rank one. Furthermore, there is a canonical R -epimorphism $\pi: \Gamma \rightarrow E$ with the property $\pi\sigma(\xi) = \epsilon(\sigma)\pi(\xi)$ for $\xi \in \Gamma$ and $\sigma \in G$. The symbol $\epsilon(\sigma)$ is the signature of the permutation σ , having the value 1 for even permutations and -1 for odd ones.

Let H be the kernel of π . Then H is an R -submodule of Γ which is mapped into itself by the elements of G . Denote by $\mathfrak{J}$ the set of elements $\xi \in \Gamma$ having the property that $\xi\Gamma \subset H$. It is clear that $\mathfrak{J}$ is an ideal in Γ which is mapped into itself by the elements of G . If $\Omega = \Gamma/\mathfrak{J}$, then G is represented by automorphisms of Ω . We shall prove that Ω is the required Galois extension of R relative to this particular representation of G by automorphisms of Ω .

Since E is a free R -module and $E = \Gamma/H$, it follows that $R \cap \mathfrak{J} = 0$. Thus the map $\Gamma \rightarrow \Omega$ induces a monomorphism on R which we consider an identification so that R is a subring of Ω .

If $\omega \in \text{Hom}_R(S, S)$, we define an endomorphism ω' of Γ by:

$$\begin{aligned} \omega'(x_1 \otimes \cdots \otimes x_n) &= \omega(x_1) \otimes x_2 \otimes \cdots \otimes x_n + x_1 \otimes \omega(x_2) \otimes \cdots \\ &\quad \otimes x_n + \cdots + x_1 \otimes x_2 \otimes \cdots \otimes \omega(x_n). \end{aligned}$$

Then it follows from the elementary properties of the exterior algebra that $\pi\omega'(\xi) = \tau(\omega)\pi(\xi)$, where $\tau(\omega)$ is the trace of the endomorphism ω . Therefore we find that the endomorphism $\omega' - \tau(\omega)$ of Γ maps Γ into H .

For $i = 1, 2, \dots, n$ define $p_i: S \rightarrow \Gamma$ by $p_i(x) = 1 \otimes \cdots \otimes x \otimes \cdots \otimes 1$ (the x occurring in the i th place). The map p_i is an R -algebra monomorphism of S into Γ . Furthermore, if $\sigma \in G$, then $\sigma p_i = p_{\sigma(i)}$.

If $x \in S$ let ω be the element of $\text{Hom}_R(S, S)$ defined by multiplication by x , so that $\tau(\omega) = t(x)$. Defining ω' as in the previous paragraph, it is clear that we have $\omega'(\xi) = \sum_i p_i(x)\xi$, for $\xi \in \Gamma$. Therefore multiplication by $\sum p_i(x) - t(x)$ maps Γ into H , or

$$(1) \quad \sum_i p_i(x) - t(x) \in \mathfrak{J}.$$

As an immediate consequence of (1) we have that $p_i(S) \cap \mathfrak{J} = 0$. Namely, suppose that for some i and some $x \in S$ we have $p_i(x) \in \mathfrak{J}$. Since $\mathfrak{J}$ is an ideal and p_i is a ring homomorphism, we have $p_i(xy) \in \mathfrak{J}$ for all $y \in S$. Furthermore, for $\sigma \in G$ we have $\sigma p_i = p_{\sigma(i)}$, while $\mathfrak{J}$ is invariant under G . Therefore $p_j(xy) \in \mathfrak{J}$ for all $y \in S$ and all j , whence by (1) it follows that $t(xy) \in \mathfrak{J}$. Since $\mathfrak{J} \cap R = 0$, we have $t(xy) = 0$ for all $y \in S$. It now follows from Proposition A.4 that $x = 0$.

From the fact that $p_i(S) \cap \mathfrak{J} = 0$ it follows that p_i followed by the canonical map $\psi: \Gamma \rightarrow \Omega$ is a monomorphism from S into Ω . In particular, ψp_1 is an imbedding of S as an R -algebra into Ω .

We now give another description of $\mathfrak{J}$. Let $x_1, \dots, x_n$ be a set of free generators of S over R . By Proposition A.4 there are elements $y_1, \dots, y_n$ in S with $t(x_i y_j) = \delta_{ij}$. Of course $y_1, \dots, y_n$ also form a set of free generators of S over R .

As $i_1, \dots, i_n$ range independently over $\{1, 2, \dots, n\}$, the elements $y_{i_1} \otimes y_{i_2} \otimes \dots \otimes y_{i_n}$ form a set of free generators of the R -module Γ . If some pair of the indices $i_1, \dots, i_n$ are equal, then $y_{i_1} \otimes \dots \otimes y_{i_n}$ is in H . Therefore if $\xi \in \Gamma$, we may write $\xi = \xi' + \sum_{\sigma} a(\sigma) \sigma(y_1 \otimes \dots \otimes y_n)$ with $\xi' \in H$ and $a(\sigma) \in R$. Set $Y = y_1 \otimes \dots \otimes y_n$. Then $\sigma(Y) - \epsilon(\sigma)Y \in H$, so that $\xi = \xi'' + \sum_{\sigma} \epsilon(\sigma) a(\sigma) Y$, with $\xi'' \in H$. We shall now find an explicit expression for $\sum_{\sigma} \epsilon(\sigma) a(\sigma)$.

Denote by t' the trace in the R -algebra Γ . Then it is clear that $t'(z_1 \otimes \dots \otimes z_n) = \prod_i t(z_i)$, and therefore that $t'(\sigma(\xi)) = t'(\xi)$. From the fact that $t(x_i y_j) = \delta_{ij}$, it follows that $t'((x_1 \otimes \dots \otimes x_n)(y_{i_1} \otimes \dots \otimes y_{i_n})) = 0$ if some pair of the indices $i_1, \dots, i_n$ are equal. In addition, we have $t'((x_1 \otimes \dots \otimes x_n)\sigma(Y)) = 0$ if $\sigma \neq 1$, and is equal to 1 if $\sigma = 1$.

Set $X = x_1 \otimes \dots \otimes x_n$. If $\xi = \xi' + \sum_{\sigma} a(\sigma) \sigma(Y)$, as above, then $a(\sigma) = t'(\xi \sigma(X))$. Consequently we have for any $\xi \in \Gamma$ that $\xi - \sum_{\sigma} \epsilon(\sigma) t'(\xi \sigma(X)) Y \in H$.

If $\xi \in \Gamma$, we set $\alpha(\xi) = \sum_{\sigma} \epsilon(\sigma) \sigma(\xi)$. With this notation we have, for $\xi \in \Gamma$,

$$(2) \quad \xi - t'(\xi \alpha(X)) Y \in H.$$

In particular, since Y is part of a set of free generators of Γ , we have:

$$(3) \quad \xi \in H \Leftrightarrow t'(\xi \alpha(X)) = 0.$$

Because S is separable over R , it follows from Proposition 1.5 that Γ is also separable over R . Applying Proposition A.4 to (3) above, we find:

$$(4) \quad \xi \in \mathfrak{J} \Leftrightarrow \xi\alpha(X) = 0.$$

Before we can apply (4), we need further information about α . In particular, we note the following fact. If $z_1, \dots, z_n \in S$, then $\alpha(z_1 \otimes \dots \otimes z_n) = \det(p_i(z_j))$. This may be verified for example by expanding $\det(p_i(z_j))$ as an alternating sum of $n!$ terms; these terms are precisely those in the sum $\alpha(z_1 \otimes \dots \otimes z_n) = \sum \epsilon(\sigma) \sigma(z_1 \otimes \dots \otimes z_n)$.

Now, we have $\alpha(X) = \det(p_i(x_j))$ and $\alpha(Y) = \det(p_i(y_j))$, so that $\alpha(X)\alpha(Y) = \det(r_{ij})$, where $r_{ij} = \sum_k p_k(x_i)p_k(y_j)$. But $r_{ij} = \sum_k p_k(x_i y_j)$, so that $r_{ij} - t(x_i y_j) \in \mathfrak{J}$. Because $t(x_i y_j) = \delta_{ij}$ we find

$$(5) \quad \alpha(X)\alpha(Y) - 1 \in \mathfrak{J}.$$

In view of (4) which asserts that $\mathfrak{J}$ is the annihilator of $\alpha(X)$, it follows from (5) that $\alpha(X)\alpha(Y)$ is idempotent. Furthermore, (4) and (5) also show that $\mathfrak{J}$ is generated by $\alpha(X)\alpha(Y) - 1$. The fact that $\mathfrak{J}$ is generated by an idempotent shows that Ω is Γ -projective, hence in particular Ω is R -projective.

Because Γ is R -separable, it follows from Proposition 1.4 that Ω is R -separable. To conclude that Ω is a Galois extension of R we shall show that Proposition A.6 is applicable. To do so we need some preliminary computations.

Let $z_1, \dots, z_n$ be in S . Then $z_j = \sum_k a_{jk} x_k$ with $a_{jk} \in R$ so that $p_i(z_j) = \sum_k a_{jk} p_i(x_k)$ and therefore $\det(p_i(z_j)) = a \det(p_i(x_k))$, or $\alpha(z_1 \otimes \dots \otimes z_n) = a\alpha(X)$. Therefore for any $\xi \in \Gamma$, we have $\alpha(\xi) = a\alpha(X)$, with $a \in R$. Since $t'(\alpha(X)Y) = 1$, we have $a = t'(\alpha(\xi)Y)$. However, it is clear that $t'(\alpha(\xi)Y) = t'(\xi\alpha(Y))$. Therefore we have:

$$(6) \quad \alpha(\xi) = t'(\xi\alpha(Y))\alpha(X)$$

for all $\xi \in \Gamma$.

If we set $\xi = \eta\alpha(X)$ in (6), then we find

$$(7) \quad \sum \sigma(\eta)\alpha(X) = t'(\eta\alpha(X)\alpha(Y))\alpha(X), \quad \eta \in \Gamma.$$

Let t'' be the trace in the R -algebra Ω . Suppose that $u \in \Omega$ and $\eta \in \Gamma$ such that $\psi(\eta) = u$. Then, $\psi(\eta\alpha(X)\alpha(Y)) = u$, while $\eta\alpha(X)\alpha(Y)$ annihilates $\mathfrak{J}$. Therefore

$$t''(u) = t'(\eta\alpha(X)\alpha(Y)),$$

or

$$t''(u)\alpha(X)\alpha(Y) = \sum \sigma(\eta)\alpha(X)\alpha(Y) \text{ by (7).}$$

But $\psi(\alpha(X)\alpha(Y)) = 1$, so that $t''(u) = \sum \sigma(u)$.

All that remains for the application of Proposition A.6 is the proof that the map $\delta: \Delta(\Omega; G) \rightarrow \text{Hom}_R(\Omega, \Omega)$ is a monomorphism. Before entering into

the proof of that statement, we note that $\sum \xi_i p_i(x) \in \mathfrak{F}$ for all $x \in S$ with $\xi_i \in \Gamma$ implies that $\xi_i \in \mathfrak{F}$. For, we have $\det(p_i(x_j)) = \alpha(X)$ which is a unit mod $\mathfrak{F}$.

To prove that $\delta: \Delta(\Omega; G) \rightarrow \text{Hom}_R(\Omega, \Omega)$ is a monomorphism, we must show the following: if $\xi(\sigma) \in \Gamma$ and $\sum \xi(\sigma)\sigma(\eta) \in \mathfrak{F}$ for all $\eta \in \Gamma$, then all $\xi(\sigma) \in \mathfrak{F}$. Assume that this is false, and suppose that the ξ 's have been chosen to have the least number of them not in $\mathfrak{F}$. Clearly the number of ξ 's not in $\mathfrak{F}$ must be at least two. (If $\xi(\sigma(\eta)) \in \mathfrak{F}$, we merely take $\eta = 1$ to conclude that $\xi \in \mathfrak{F}$.) Suppose $\xi(\rho) \notin \mathfrak{F}$. Then, we have:

$$\begin{aligned} \sum_{\sigma} \xi(\sigma)\sigma(\eta\eta') &\in \mathfrak{F}, \\ \sum_{\sigma} \xi(\sigma)\sigma(\eta)\rho(\eta') &\in \mathfrak{F}, \quad \text{all } \eta, \eta' \in \Gamma. \end{aligned}$$

By subtracting, we remove the ρ -term. Because of the minimality property of the ξ 's, it follows that $\xi(\sigma)(\sigma(\eta) - \rho(\eta)) \in \mathfrak{F}$, for all $\sigma \in G$ and all $\eta \in \Gamma$. Choose any $\sigma \neq \rho$; then there is an index $i \in \{1, 2, \dots, n\}$ such that $\sigma p_i = p_j$, $\rho p_i = p_k$ with $j \neq k$. We have then $\xi(\sigma)(p_i(x) - p_k(x)) \in \mathfrak{F}$, for all $x \in S$. By the observation in the preceding paragraph, it follows that $\xi(\sigma) \in \mathfrak{F}$. Since this is so for all $\sigma \neq \rho$, there is at most one ξ not in $\mathfrak{F}$, hence all ξ are in $\mathfrak{F}$. This completes the proof of the theorem.

REMARK. In applying Theorem A.7 to fields, the Galois extension Ω constructed as above will not be a field in general. However, the smallest Galois extension containing the given separable extension will be a factor ring of Ω . It should also be remarked that the requirement that S be R -free is undoubtedly too strong; however, a proof under weaker hypotheses is not available at this time.

The next theorem has no natural counterpart in the Galois theory of fields.

THEOREM A.8. *For $i = 1, 2$ let S_i be a Galois extension of R_i relative to G_i . Suppose that R_1 and R_2 are R -algebras for some commutative ring R such that $R_1 \otimes_R R_2$ is not 0. Represent $G_1 \times G_2$ by automorphisms of $S_1 \otimes_R S_2$ by means of: $(\sigma_1 \times \sigma_2)(x_1 \otimes x_2) = \sigma_1(x_1) \otimes \sigma_2(x_2)$. Then, $S_1 \otimes_R S_2$ is a Galois extension of $R_1 \otimes_R R_2$ relative to $G_1 \times G_2$.*

Proof. Since R_i is a direct summand of S_i it follows that $R_1 \otimes_R R_2$ is a subring of $S_1 \otimes_R S_2$ so that, in particular, $S_1 \otimes_R S_2 \neq 0$. It is clear that $S_1 \otimes_R S_2$ is a finitely generated projective $R_1 \otimes_R R_2$ -module. It is now only necessary to observe that $\Delta(S_1 \otimes_R S_2; G_1 \times G_2)$ is naturally isomorphic to $\Delta(S_1; G_1) \otimes_R \Delta(S_2; G_2)$ and that

$$\text{Hom}_{R_1 \otimes_R R_2}(S_1 \otimes S_2, S_1 \otimes S_2) \cong \text{Hom}_{R_1}(S_1, S_1) \otimes_R \text{Hom}_{R_2}(S_2, S_2).$$

There are several special cases of Theorem A.8 of sufficient importance to be mentioned explicitly. We may take $R_1 = R_2 = R$, so that the tensor product of two Galois extensions of the same ring is again a Galois extension. Or,

we may have $R_1 = R$ and $S_2 = R_2$, that is, $S \otimes_R R'$ is a Galois extension of R' if S is a Galois extension of R , with R' any R -algebra. As a special case, if $\mathfrak{a}$ is an ideal in R , then $S/\mathfrak{a}S$ is a Galois extension of $R/\mathfrak{a}$, with the two extensions having the same group.

The rest of the appendix consists of some results on Galois cohomology of rings. The results obtained are of a tentative nature in that the hypotheses imposed in a number of the theorems are stronger than needed; a final version is yet to be found. Nevertheless, the results obtained are adequate for application to the study of the Brauer group.

We shall denote by $U(S)$ the group of units of the commutative ring S . We remind the reader of some terminology already used in an earlier section: a projective R -module E is said to be of rank one if for every maximal ideal $\mathfrak{m}$ of R , the tensor product $R_{\mathfrak{m}} \otimes_R E$ is a free $R_{\mathfrak{m}}$ -module of rank one.

THEOREM A.9. *Let S be a Galois extension of R relative to G . If every finitely generated projective R -module of rank one is free (necessarily of rank one), then $H^1(G, U(S)) = (1)$.*

Proof. Let $f: G \rightarrow U(S)$ be a 1-cocycle so that $f(\rho\sigma) = \rho\{f(\sigma)\}f(\rho)$. We shall prove the existence of a unit $y \in U(S)$ such that $f(\rho) = \rho(y)y^{-1}$.

We associate to f the element $F \in \text{Hom}_R(S, S)$ given by $F = \delta(\sum f(\sigma)u_\sigma)$. Explicitly, $F(x) = \sum f(\sigma)\sigma(x)$, for $x \in S$. The fact that f is a cocycle translates into the following property of F ,

$$(1) \quad \rho\{F(x)\} = F(x)/f(\rho).$$

Thus the required result will follow if we show that the image of F meets $U(S)$.

Let $w \in S$ be such that $t(w) = 1$, and define $G: S \rightarrow S$ by $G(x) = F(wx)$. A simple calculation shows that $G^2 = G$. It follows that the image M of G is an R -direct summand of S , and therefore a finitely generated projective R -module.

Suppose that $yM = 0$ for some $y \in S$. Then $yG(wx) = 0$ for all $x \in S$, or $\sum yf(\sigma)\sigma(w)\sigma(x) = 0$. Since S is a Galois extension of R , it follows that $yf(\sigma)\sigma(w) = 0$ and therefore that $y\sigma(w) = 0$, because $f(\sigma) \in U(S)$. Summing over σ , and making use of the fact that $t(w) = 1$, it follows that $y = 0$. Thus we may conclude that M is a faithful R -module, and in particular, that $M \neq 0$.

Let $\omega \in \text{Hom}_R(S, S)$; we examine ωG . We have $\omega = \delta(\sum a_\sigma u_\sigma)$ with $a_\sigma \in S$. Now, $\omega G(x) = \sum_\sigma a_\sigma \sigma\{F(wx)\} = \sum_\sigma (a_\sigma/f(\sigma))F(wx)$, or $\omega G(x) = k(\omega)G(x)$ with $k(\omega) = \sum (a_\sigma/f(\sigma)) \in S$. Since M is a direct summand of S , every endomorphism of M as an R -module is induced by an endomorphism of S . In view of the calculation just performed and the fact that no nonzero element of S annihilates M , we may conclude that

$$\text{Hom}_R(M, M) \cong \{y \in S \mid yM \subset M\}.$$

Now suppose that $y \in S$ is such that $yM \subset M$. That is, if $x \in S$, there is an element $z \in S$ such that $yG(x) = G(z)$. If we compute G of both sides, and use the fact that $G^2 = G$, we find $G(yG(x)) = yG(x)$. Using the definition of G , we have immediately that $G(yG(x)) = t(wy)G(x)$. Thus $(y - t(wy))G(x) = 0$, so that $y - t(wy)$ annihilates M . Since $t(wy) \in R$, we conclude that y must be in R , and therefore that $\text{Hom}_R(M, M) = R$.

We may now apply the hypothesis. If $\mathfrak{m}$ is any maximal ideal in R , we know that $R_{\mathfrak{m}} \otimes M$ is a finitely generated free $R_{\mathfrak{m}}$ -module whose endomorphism ring is $R_{\mathfrak{m}}$ itself because of the fact that $\text{Hom}_R(M, M) = R$. It follows from this that $R_{\mathfrak{m}} \otimes M$ is a free $R_{\mathfrak{m}}$ -module of rank one and therefore that M is a free R -module of rank one: $M = Rz$. The proof will be complete when we show that $z \in U(S)$.

Since M is a direct summand of S , the map $M \rightarrow R$ defined by $z \rightarrow 1$ is induced by a map from S to R . Thus, there is an element $v \in S$ such that $t(vz) = 1$. That is, $1 = t(vz) = \sum \sigma(v)\sigma(z) = \sum (\sigma(v)/f(\sigma))z$, with $\sum \sigma(v)/f(\sigma) \in S$. Thus z is a unit in S and the proof is complete.

We shall now consider some of the relations between $H^2(G, U(S))$ and $\mathfrak{B}(R)$. If S is a Galois extension of R relative to G , and f is a 2-cocycle of G in $U(S)$, i.e., $f \in Z^2(G, U(S))$, we can define a crossed-product algebra $\Delta(f; S; G)$ as follows: $\Delta(f; S; G)$ is a free (left) S -module with free generators $\{u_{\sigma}\}$ indexed by the elements of G , with multiplication defined as follows: $(au_{\rho})(bu_{\sigma}) = a\rho(b)f(\rho, \sigma)u_{\rho\sigma}$. Just as in the classical theory of crossed-products, the fact that f is a cocycle is reflected in the associativity of multiplication in $\Delta(f; S; G)$. It is clear that replacing f by a cocycle cohomologous to f defines an algebra which is isomorphic to $\Delta(f; S; G)$. Every cohomology class is represented by a "normalized" cocycle, one for which we have $f(\rho, 1) = f(1, \rho) = 1$. If f is such a normalized cocycle, then u_1 is the unit element of $\Delta(f; S; G)$, and mapping $a \in S$ on au_1 imbeds S in $\Delta(f; S; G)$. We shall identify S with its image under this mapping. In every case we shall use normalized cocycles in constructing crossed-products.

We remark that $\Delta(1; S; G)$ is the algebra $\Delta(S; G)$ already considered above. Since S is a Galois extension of R , the algebra $\Delta(S; G)$ is isomorphic to $\text{Hom}_R(S, S)$ and is therefore a central separable algebra which is in the unit class of $\mathfrak{B}(R)$. (S is a finitely generated projective R -module.)

If S_1 and S_2 are Galois extensions of R relative to groups G_1 and G_2 , then $S_1 \otimes S_2$ is a Galois extension of R relative to $G_1 \times G_2$. If $f_i \in Z^2(G_i, U(S_i))$, then $f_1 \otimes f_2$ defines naturally an element of $Z^2(G_1 \times G_2, U(S_1 \otimes S_2))$, and it is obvious from the definition that

$$\Delta(f_1 \otimes f_2; S_1 \otimes S_2; G_1 \otimes G_2) \cong \Delta(f_1; S_1; G_1) \otimes \Delta(f_2; S_2; G_2).$$

It is also clear that $\Delta(f^{-1}; S; G) \cong \Delta(f; S; G)^0$.

Before continuing, we need the following lemma.

LEMMA A.10. *Let S be a Galois extension of R relative to G . Then, there are elements $e_\sigma \in S \otimes_R S$, for $\sigma \in G$, with the following properties:*

- (a) $e_\rho e_\sigma = 0$ for $\rho \neq \sigma$, $e_\sigma^2 = e_\sigma$, $\sum_\sigma e_\sigma = 1$.
- (b) $(\rho(x) \otimes 1)e_\rho = (1 \otimes x)e_\rho$, for $x \in S$.
- (c) $(\rho \times \sigma)(e_\tau) = e_{\rho\tau\sigma^{-1}}$.

Proof. We extend the ground ring from R to S by considering $S \otimes S$ as an extension of S , having first identified S with $1 \otimes S \subset S \otimes S$. Then $S \otimes S$ is a Galois extension of S relative to the group $G \times 1$. Define $f: S \otimes S \rightarrow S$ by $f(x \otimes y) = 1 \otimes xy$. Then $f \in \text{Hom}_S(S \otimes S, S)$, so that there is an element $e \in S \otimes S$ with $f = t \circ e$. Explicitly, we have:

$$(1) \quad \sum_\sigma (\sigma \times 1)(e)(\sigma(x) \otimes y) = 1 \otimes xy.$$

Set $e_\sigma = (\sigma \times 1)(e)$. By replacing x by ax in (1), and using the linear independence of the automorphisms, we get $(\sigma(a) \otimes 1)e_\sigma = (1 \otimes a)e_\sigma$. This is (b) of the lemma. It follows, in particular, that $e_1 \in A$, where A is the annihilator of the kernel J of $\phi: S \otimes S \rightarrow S$.

Applying the map ϕ to both sides of (b) gives $\phi(e_\sigma)\sigma(x) = \phi(e_\sigma)x$. Since S is a Galois extension of R , it follows that $\phi(e_\sigma) = 0$ if $\sigma \neq 1$ while $\phi(e_1) = 1$. (This incidentally gives another proof that S is separable over R , for $e_1 \in A$ and $\phi(e_1) = 1$.) By setting $x = y = 1$ in (1), we find $\sum e_\sigma = 1$.

Because $e_1 \in A$ and $\phi(e_1) = 1$, we have immediately that $e_1^2 = e_1$ and therefore also that $e_\sigma^2 = e_\sigma$ since $e_\sigma = (\sigma \times 1)(e_1)$. Finally, $e_\sigma \in J$ if $\sigma \neq 1$ so that $e_\sigma e_1 = 0$, and therefore $e_\rho e_\sigma = 0$ if $\rho \neq \sigma$. This proves (a).

To complete the proof, we consider $(\rho \times \rho)(e_1)$. From (b) we have $(\rho(x) \otimes 1)(\rho \times 1)(e_1) = (1 \otimes x)(\rho \times 1)(e_1)$, so that applying $1 \times \rho$ to both sides gives $(\rho(x) \otimes 1)(\rho \times \rho)(e_1) = (1 \otimes \rho(x))(\rho \times \rho)(e_1)$. This shows that $(\rho \times \rho)(e_1) \in A$. For any $x \in S \otimes S$, it is obvious that $\phi(\rho \times \rho)(x) = \rho\phi(x)$. Therefore, $\phi(\rho \times \rho)(e_1) = \rho\phi(e_1) = 1$, or $(\rho \times \rho)(e_1) = e_1$. Statement (c) follows immediately.

PROPOSITION A.11. *Let S be a Galois extension of R relative to G and $f \in Z^2(G, U(S))$. Then, $f \otimes 1 \in Z^2(G \times 1, U(S \otimes S))$, $1 \otimes f \in Z^2(1 \times G, U(S \otimes S))$ and $f \otimes f^{-1} \in Z^2(G \times G, U(S \otimes S))$ are all coboundaries. If $g \in Z^2(G, U(S))$, then $f \otimes g$ is cohomologous to $fg \otimes 1$.*

Proof. We make use of the elements $e_\sigma \in S \otimes S$ described in Lemma A.10. The fact that the e_σ are orthogonal idempotents whose sum is 1 enables us to express every $x \in S \otimes S$ in the form $\sum x e_\sigma$ and to observe that $x \in U(S \otimes S)$ if, and only if, each $x e_\sigma \in U(S \otimes S) e_\sigma$. Now define:

- (1) $h_1(\sigma) = \sum_\tau (1 \otimes f(\tau^{-1}, \sigma)) e_\tau$.
- (2) $h_2(\sigma) = \sum_\tau (f(\tau, \sigma)^{-1} \otimes 1) e_\tau$.
- (3) $k = \sum_\tau (f(\tau, \tau^{-1}) \otimes 1) e_\tau$.
- (4) $H(\sigma_1 \times \sigma_2) = h_1(\sigma_1)(\sigma_1 \times 1)(h_2(\sigma_2))(\sigma_1 \times \sigma_2)(k)(\sigma_1 \times 1)(k)^{-1}$.

Then a direct computation shows that

$$\begin{aligned} f \otimes 1 &= \delta h_1 & \text{on } G \otimes 1, \\ 1 \otimes f &= \delta h_2^{-1} & \text{on } 1 \otimes G, \\ f \otimes f^{-1} \otimes \delta H & & \text{on } G \times G. \end{aligned}$$

Finally, we have $(f \otimes g)(fg \otimes 1)^{-1} = g^{-1} \otimes g$ which is a coboundary, so that $f \otimes g$ is cohomologous to $fg \otimes 1$.

Combining the discussion preceding Lemma A.10 with Proposition A.11, we have:

THEOREM A.12. *Let S be a Galois extension of R relative to G . If $f \in Z^2(G, U(S))$, then $\Delta(f; S; G)$ is a central separable algebra over R which contains S as a maximal commutative subring and is split by S . The map $f \rightarrow \Delta(f, S; G)$ induces a homomorphism $H^2(G, U(S)) \rightarrow \mathfrak{B}(R)$.*

Proof. We have $\Delta(f, S; G) \otimes_R S \cong \Delta(f \otimes 1, S \otimes S; G \times 1)$. Since $f \otimes 1 \sim 1$, it follows that

$$\Delta(f \otimes 1, S \otimes S; G \times 1) \cong \Delta(1, S \otimes S; G \times 1).$$

Because S is a Galois extension of R relative to G , we know by Theorem A.8 that $S \otimes_R S$ is a Galois extension of S relative to $G \times 1$. Here we consider $S \otimes S$ as an S -algebra by means of the imbedding $x \rightarrow 1 \otimes x$. Thus we have $\Delta(f, S; G) \otimes_R S \cong \text{Hom}_S(S \otimes_R S, S \otimes_R S)$.

It follows from this that $\Delta(f, S; G) \otimes_R S$ is a central separable algebra over S . Since S is also separable over R , we conclude by Theorem 2.3 that $\Delta(f, S; G) \otimes_R S$ is separable over R . Since R is a direct summand of S it follows from Proposition 1.7 that $\Delta(f, S; G)$ is separable over R . Finally, if C is the center of $\Delta(f, S; G)$, then $C \otimes_R S$ is the center S of $\Delta(f, S; G) \otimes S$, from which it follows that $C = R$. Thus $\Delta(f, S; G)$ is a central separable algebra over R , and is split by S .

Under the isomorphism $\Delta(f, S; G) \otimes S \cong \text{Hom}_S(S \otimes S, S \otimes S)$ the subring S of $\Delta(f, S; G)$ corresponds to the endomorphisms of $S \otimes S$ given by multiplication by the elements $x \otimes 1$, $x \in S$. It follows from this that an element of $\text{Hom}_S(S \otimes S, S \otimes S)$ which commutes with the image of S under the isomorphism above lies in $\text{Hom}_{S \otimes S}(S \otimes S, S \otimes S) = S \otimes S$, and therefore that the image of S generates in $\text{Hom}_S(S \otimes S, S \otimes S)$ a maximal commutative subring. Hence S is a maximal commutative subring of $\Delta(f, S; G)$.

If $f, g \in Z^2(G, U(S))$, then

$$\Delta(f, S; G) \otimes_R \Delta(g, S; G) \cong \Delta(f \otimes g, S \otimes S; G \times G).$$

However, $f \otimes g \sim fg \otimes 1$ and therefore,

$$\begin{aligned} \Delta(f, S; G) \otimes \Delta(g, S; G) \\ \cong \Delta(fg \otimes 1, S \otimes S; G \times G) \cong \Delta(fg, S; G) \otimes \Delta(1, S; G). \end{aligned}$$

Since $\Delta(1, S; G) \sim 1$, we find

$$\Delta(f, S; G) \otimes \Delta(g, S; G) \sim \Delta(fg, S; G)$$

and the proof is complete.

The description of the kernel and image of the mapping $H^2(G, U(S)) \rightarrow \mathfrak{B}(R)$ cannot be given completely at this time; this question will be answered under restrictive hypotheses. Suppose that a central separable algebra Λ over R is split by a Galois extension S of R . Then, by Theorem 5.7, there is an algebra equivalent to Λ which contains S as a maximal commutative subring. Therefore, in studying the subgroup of $\mathfrak{B}(R)$ of algebra classes which are split by a given Galois extension S of R , we may restrict our attention to algebras which contain S as a maximal commutative subring.

PROPOSITION A.13. *Let S be a Galois extension of R relative to G and Λ a central separable algebra over R containing S as a maximal commutative subalgebra. If each element of G can be extended to an inner automorphism of Λ , then Λ is isomorphic to a crossed-product $\Delta(f; S; G)$.*

Proof. For each $\sigma \in G$ there is a unit $t_\sigma \in \Lambda$ such that $\sigma(x) = t_\sigma x t_\sigma^{-1}$, for $x \in S$. Therefore the inner automorphism defined by $f(\rho, \sigma) = t_\rho t_\sigma t_{\rho\sigma}^{-1}$ is the identity in S . Because S is a maximal commutative subalgebra of Λ , it follows that $f(\rho, \sigma) \in U(S)$. It is clear from the form of $f(\rho, \sigma)$ that we have $f \in Z^2(G, U(S))$. We form $\Delta(f; S; G)$ and define $h: \Delta(f; S; G) \rightarrow \Lambda$ by $h(\sum a_\sigma u_\sigma) = \sum a_\sigma t_\sigma$. Then h is an algebra homomorphism so that the kernel of h has the form $\mathfrak{a}\Delta(f; S; G)$ with $\mathfrak{a}$ an ideal of R . Since h is the identity map on R , it follows that $\mathfrak{a} = 0$ and h is a monomorphism. We identify $\Delta(f; S; G)$ with its image under h and note that h is the identity map on S . Then we have $\Lambda = \Delta(f; S; G) \otimes_R \Omega$, with Ω the commutant of $\Delta(f; S; G)$ in Λ . In particular, the elements of Ω commute with those of S , so that $\Omega \subset S$. It follows immediately that $\Omega = R$ and that $\Delta(f; S; G) = \Lambda$, completing the proof.

The following general lemma will be needed in the proof of Theorem A.15.

LEMMA A.14. *Let R be a local ring (not necessarily noetherian) and let S be a separable R -algebra which is a free R -module of rank n . Let E be a finitely generated projective faithful S -module whose rank over R is also n . Then E is a free S -module of rank 1.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R , and let $\mathfrak{M}_1, \dots, \mathfrak{M}_t$ be the maximal ideals of S , so that $\mathfrak{N} = \mathfrak{M}_1 \cap \dots \cap \mathfrak{M}_t$ is the radical of S . By Proposition 2.2 of [1], the fact that S is separable over R implies that $\mathfrak{m}S = \mathfrak{N}$.

We have $S/\mathfrak{N} = S/\mathfrak{M}_1 + \dots + S/\mathfrak{M}_t$ (direct sum) and therefore $E/\mathfrak{N}E = E/\mathfrak{M}_1E + \dots + E/\mathfrak{M}_tE$ (direct sum). Since E is a faithful S -module, we have $\mathfrak{M}_iE \neq E$. Otherwise there would be an element $a \in \mathfrak{M}_i$ such that $(1+a)E = 0$. Thus, $E/\mathfrak{M}_iE$ is a nonzero vector space over the field $S/\mathfrak{M}_i$.

so that $E/\mathfrak{M}_i E$ contains an isomorphic copy of $S/\mathfrak{M}_i$. Therefore, $E/\mathfrak{M}E$ contains an isomorphic copy of $S/\mathfrak{M}$. Since $S/\mathfrak{M}$ is semi-simple, we have $E/\mathfrak{M}E \cong S/\mathfrak{M} \dot{+} I$ (direct sum), with I some $S/\mathfrak{M}$ -submodule of $E/\mathfrak{M}E$.

Since $\mathfrak{M} = \mathfrak{m}S$, the dimension of $S/\mathfrak{M}$ over $R/\mathfrak{m}$ equals the rank of S over R , that is, n . Similarly, the dimension of $E/\mathfrak{M}E$ over $R/\mathfrak{m}$ is also n . Hence $I = 0$, or $E/\mathfrak{M}E \cong S/\mathfrak{M}$. Because E is a finitely generated projective S -module, it follows from the Remark at the end of §3 that $E \cong S$.

THEOREM A.15. *Let S be a Galois extension of R relative to G , and suppose that S has the property that every finitely generated projective S -module of rank one is free. Then the sequence $(1) \rightarrow H^2(G, U(S)) \rightarrow \mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$ is exact.*

Proof. Suppose first that Λ is a central separable algebra over R which is split by S ; we may assume that Λ contains S as a maximal commutative subring. Therefore by Proposition A.13 we need to show that each element of G as an automorphism of S can be extended to an inner automorphism of Λ .

Considering Λ as a left S -module, we have from Theorem 5.6 that Λ is S -projective, that Λ is $S \otimes_R \Lambda^0$ -projective and that $\text{Hom}_S(\Lambda, \Lambda) \cong S \otimes_R \Lambda^0$. Denote $S \otimes_R \Lambda^0$ by Ω . If $\sigma \in G$ we consider the automorphism $\sigma \otimes 1: \Omega \rightarrow \Omega$. The automorphism induces a new Ω -module structure in Ω under which $\sigma \otimes 1$ is a module isomorphism, which means that this new module is Ω -free. The changes of rings under $\sigma \otimes 1$ gives a new Ω -module structure $\bar{\Lambda}$ on Λ ($(s \otimes \lambda)x = \sigma(s)x\lambda$). Since Λ is Ω -projective, it follows that $\bar{\Lambda}$ is again Ω -projective. Then, by the appendix of [2], there is a finitely generated projective S -module N such that $\bar{\Lambda}$ and $N \otimes_S \Lambda$ are Ω -isomorphic. It is clear that N has rank one and therefore that $N \cong S$. We have therefore an Ω -isomorphism $h: \bar{\Lambda} \rightarrow \Lambda$. Thus, h is a 1-1 map of Λ onto itself with the property $h(\sigma(s)x\lambda) = sh(x)\lambda$, for $s \in S$ and $x, \lambda \in \Lambda$. By setting $s = x = 1$, we find $h(\lambda) = h(1)\lambda$, so that $u = h(1)$ is a unit in Λ . Finally, setting $x = \lambda = 1$, we find $u\sigma(s) = h(\sigma(s)) = sh(1) = su$ and therefore σ has an extension to an inner automorphism of Λ . This shows that the kernel of the map $\mathfrak{B}(R) \rightarrow \mathfrak{B}(S)$ is contained in the image of $H^2(G, U(S)) \rightarrow \mathfrak{B}(R)$. We know already that the image of $H^2(G, U(S)) \rightarrow \mathfrak{B}(R)$ is contained in $\ker(\mathfrak{B}(R) \rightarrow \mathfrak{B}(S))$ (Theorem A.12).

Now suppose $f \in Z^2(G, U(S))$ is such that $\Delta(f, S; G) \sim 1$. Then there exists a finitely generated projective R -module E whose endomorphism ring (over R) is $\Delta(f, S; G)$. Then E is finitely generated and projective over $\Delta(f, S; G)$, while $\Delta(f, S; G)$ is finitely generated and free over S . Hence E is a finitely generated projective S -module which we shall prove is of rank one.

Let $\mathfrak{M}$ be a maximal ideal in S and let $\mathfrak{p} = \mathfrak{M} \cap R$, so that $\mathfrak{p}$ is a prime ideal in R . We wish to show that $E \otimes_S S_{\mathfrak{M}}$ is a free $S_{\mathfrak{M}}$ -module of rank one. It will be sufficient for this, to show that $E \otimes_R R_{\mathfrak{p}}$ is a free $S \otimes_R R_{\mathfrak{p}}$ -module of rank one. Then, set $R' = R_{\mathfrak{p}}$, $S' = S \otimes_R R_{\mathfrak{p}}$ and $E' = E \otimes_R R_{\mathfrak{p}}$. Now, R' is a local ring, S' is semi-local and separable over R' , while E' is a finitely generated projective R' -module. Furthermore, S is a Galois extension of R , so that S' is also a

Galois extension of R' relative to G . Therefore S' is a free R' -module of rank n , where, it is easy to verify, n is the order of G . Since $\Delta(f, S; G) \cong \text{Hom}_R(E, E)$, we have $R' \otimes \Delta(f, S; G) \cong \text{Hom}_{R'}(E', E')$ and therefore E' is a free R' -module of the same rank n . We may now apply Lemma A.14 and conclude that E' is a free S' -module of rank one. We therefore conclude that E has rank one over S , and hence by the hypothesis of the theorem that E is a free S -module of rank one: $E = Se_0$.

If $\sigma \in G$, define $v_\sigma: E \rightarrow E$ by $v_\sigma(ae_0) = \sigma(a)e_0$, for $a \in S$. It is clear that v_σ commutes with R , so that $v_\sigma \in \Delta(f, S; G)$. Clearly, $v_\sigma v_\tau = v_{\sigma\tau}$. Let $b \in S$ and $x = ae_0 \in E$. Then, $v_\sigma b v_\sigma^{-1}(x) = v_\sigma b \sigma^{-1}(a)e_0 = \sigma(b \sigma^{-1}(a))e_0 = \sigma(b)ae_0 = \sigma(b)x$, i.e., $v_\sigma b v_\sigma^{-1} = \sigma(b)$ for $b \in S$. But this shows that the inner automorphism of $\Delta(f, S; G)$ defined by $g(\sigma) = u_\sigma v_\sigma^{-1}$ induces the identity automorphism in S , so that $g(\sigma) \in U(S)$. It is clear that $f = \delta g$. This completes the proof of the theorem.

REFERENCES

1. M. Auslander and D. A. Buchsbaum, *Ramification theory in noetherian rings*, Amer. J. Math. vol. 81 (1959) pp. 749-765.
2. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. vol. 97 (1960) pp. 1-24.
3. G. Azumaya, *On maximally central algebras*, Nagoya Math. J. vol. 2 (1951) pp. 119-150.
4. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton, 1956.
5. S. Eilenberg, A. Rosenberg and D. Zelinsky, *On the dimension of modules and algebras*. VIII, Nagoya Math. J. vol. 12 (1957) pp. 71-93.
6. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloquium Publications, vol. 37, 1956.
7. O. F. G. Schilling, *The theory of valuations*, Amer. Math. Soc. Math. Surveys, vol. 4, 1950.
8. O. Teichmüller, *Verschränkte Produkte mit Normalringen*, Deutsche Math. vol. 1 (1936) pp. 92-102.
9. C. C. Tsen, *Divisionalgebren über Funktionenkörpern*, Nach. Ges. Wiss. Göttingen (1933) pp. 335-339.

BRANDEIS UNIVERSITY,
WALTHAM, MASSACHUSETTS