PACIFIC JOURNAL OF MATHEMATICS
Vol. 34, No. 3, 1970

ON THE GALOIS THEORY OF SEPARABLE ALGEBRAS

H. F. KREIMER

This note presents a Galois theory for a separable algebra A over a semi-local ring R without imposing any restrictions on the presence of idempotent elements in A. If suitable restrictions are placed on the existence of idempotent elements in A, then such a Galois theory has been obtained by L. N. Childs and F. R. DeMeyer; and the results presented here are extensions of results obtained by Childs and DeMeyer. In more recent work, DeMeyer has extended the Galois theory to algebras over a class of commutative rings more general than semi-local rings. After treating the simpler case of algebras over a semi-local ring, it is indicated in an addendum to this paper how the Galois theory presented here may also be extended to algebras over this more general class of commutative rings.

Galois theory. Throughout this paper, ring will mean ring with identity element and subring of a ring will mean subring which contains the identity element of the ring. Analogously, an algebra over a commutative ring R will mean an R-algebra which is a unital R-module and has an identity element, and a subalgebra of an algebra will mean a subalgebra which contains the identity element of the algebra. Let G be a group of automorphisms of a ring A, and let A^G designate the subring of G-invariant elements of A. If C is the center of A, let G_0 denote the subgroup of all automorphisms in G which leave elements of C invariant. C is G-stable and G_0 is a normal subgroup of G. Moreover, the restriction of elements of G to C induces a faithfull representation of G/G_0 as a group of automorphisms of C. The set E of central, idempotent elements of A is a Boolean algebra in which the intersection $e \cap f$ is $e \cdot f$, the union $e \cup f$ is $e + f - e \cdot f$, and the complement of e is $1 - e$, for $e, f \in E$. In agreement with [14, Definition 3.7], define the closure of G to be the set of all automorphisms τ of A for which there exist a positive integer n, and $\sigma_i \in G$ and $e_i \in E$ for $1 \leqq i \leqq n$, such that $e_i \cdot \tau(x) = e_i \cdot \sigma_i(x)$ for $x \in A$ and $1 \leqq i \leqq n$ and the identity element of E is the least upper bound for the subset $\{e_i \mid 1 \leqq i \leqq n\}$ of E. Call G closed if it is equal to its closure.

Let Γ be a subring of A and let A^Γ designate the centralizer of Γ in A. Also let M be a left A-module and let N be a Γ-submodule of M. A canonical A-module homomorphism φ of $A \otimes_\Gamma N$ into M is determined by the correspondence of $\alpha \cdot x$ to $\alpha \otimes x$ for $\alpha \in A$ and

$x \in N$. It will be convenient to write $M = \Lambda \otimes_\Gamma N$ when φ is an isomorphism. Also, tacit use will be made of the following proposition [13, Proposition 1.1]: If Λ is a separable algebra over a commutative ring R such that Λ is a projective R-module, then Λ is a finitely generated R-module. Finally, if Λ is a commutative ring and p is a prime ideal in Λ, let Λ_p denote the local ring of Λ at p and let $M_p = \Lambda_p \otimes_\Lambda M$.

In the sequel, let Λ be a given ring with identity element 1, and let C be the center of Λ.

PROPOSITION 1. *Let G be a group of automorphisms of Λ such that G/G_0 is finite. Let $\Gamma = \Lambda^G$ and let Z be the center of Γ. Assume that $\bar{G}$ is a closed group of automorphisms of Λ over Γ such that $G \subseteqq \bar{G}$ and C is a separable algebra over $\Gamma \cap C$. Then $\Lambda^{\bar{G}_0} = \Gamma \otimes_{\Gamma \cap C} C$ and $Z \otimes_{\Gamma \cap C} C$ is the center of $\Lambda^{\bar{G}_0}$. Moreover, if Λ is a finitely generated, projective left $Z \otimes_{\Gamma \cap C} C$-module and p is a prime ideal in Z, then Λ_p is a free module over $(Z \otimes_{\Gamma \cap C} C)_p$.*

The proof consists of the following steps:

(1.1) $\Lambda^{\bar{G}_0} = \Gamma \otimes_{\Gamma \cap C} C$ and $Z \otimes_{\Gamma \cap C} C$ is the center of $\Lambda^{\bar{G}_0}$.

Proof. C is a commutative ring and $\Gamma \cap C$ is the subring of G/G_0-invariant elements of C. Since G/G_0 is finite and C is a separable algebra over $\Gamma \cap C$, C is an outer semi-Galois extension of $\Gamma \cap C$ [10, Definition 2.4]. Clearly Γ and C are subrings of $\Lambda^{\bar{G}_0}$. Since $\bar{G}_0$ is a normal subgroup of $\bar{G}$, $\Lambda^{\bar{G}_0}$ is $\bar{G}$-stable. $G_0 = G \cap \bar{G}_0$ and the restriction of elements of G to $\Lambda^{\bar{G}_0}$ induces a faithful representation of G/G_0 as a group of automorphisms of $\Lambda^{\bar{G}_0}$. Moreover, Γ is the subring of G/G_0-invariant elements of $\Lambda^{\bar{G}_0}$. Letting Z' be the center of $\Lambda^{\bar{G}_0}$, $C \subseteqq Z'$ and C and Z' are G/G_0-stable. Suppose there exists an idempotent $e \in C$ and $\sigma \in G$, such that $\sigma(ex) = ex$ for all $x \in C$. Then $\sigma(e) = e$; and, setting $\tau(x) = e \cdot \sigma(x) + (1 - e) \cdot x$ for $x \in \Lambda$, it is readily verified that τ is an automorphism of Λ which leaves the elements of C invariant. Since $\bar{G}$ is closed, $\tau \in \bar{G}_0$. Therefore, $x = e \cdot \sigma(x) + (1 - e)x$ and $ex = e \cdot \sigma(x) = \sigma(ex)$ for all $x \in \Lambda^{\bar{G}_0}$. Lemma 1.2 of [11] may be applied to the group G/G_0 and subrings C and Z' of $\Lambda^{\bar{G}_0}$ to establish that $Z' = (\Gamma \cap Z') \otimes_{\Gamma \cap C} C$ and $\Lambda^{\bar{G}_0} = \Gamma \otimes_{\Gamma \cap Z'} Z'$. Consequently, $\Lambda^{\bar{G}_0} = \Gamma \otimes_{\Gamma \cap C} C$. Clearly Λ^Γ is the centralizer of $\Lambda^{\bar{G}_0}$ in Λ; so $Z' = \Lambda^{\bar{G}_0} \cap \Lambda^\Gamma$ and $\Gamma \cap Z' = \Gamma \cap \Lambda^\Gamma = Z$. Thus $Z' = Z \otimes_{\Gamma \cap C} C$.

(1.2) Let p be a prime ideal in Z, and let $T = (Z \otimes_{\Gamma \cap C} C)_p$. T is a semi-local ring and G acts transitively on the set of maximal ideals of T.

Proof. Let $S = Z_p$. It follows from [3, § 2, No. 1, Proposition 2] that the inclusion map of Z into $Z \otimes_{\Gamma \cap C} C$ induces an injection of S into T by which S may be identified with a subring of T, and every element of G/G_0 induces an automorphism of T over S. Any element of T has the form a/s, $a \in Z \otimes_{\Gamma \cap C} C$ and $s \in Z - p$. If a/s is a G/G_0-invariant, then there exist $t_\sigma \in Z - p$ such that $t_\sigma \cdot (\sigma(a) - a) = 0$ for each $\sigma \in G/G_0$ by [3, § 2, No. 2, Proposition 4]. Letting

$$t = \prod_{\sigma \in G/G_0} t_\sigma, \; t \in Z - p \quad \text{and} \quad \sigma(ta) = t \cdot \sigma(a) = ta$$

for all $\sigma \in G/G_0$. Therefore $ta \in \Gamma \cap (Z \otimes_{\Gamma \cap C} C) = Z$ and $a/s = at/st \in S$. Thus S is the subring of G/G_0-invariant elements of T. There is a natural isomorphism of $T = Z_p \otimes_Z (Z \otimes_{\Gamma \cap C} C)$ onto $Z_p \otimes_{\Gamma \cap C} C$, and therefore T is a separable algebra over S by [2, Corollary 1.6]. Since T is a commutative ring, T is an outer semi-Galois extension of S. But S is a local ring and cannot have any nontrivial idempotents. It follows from [10, Th. 2.3] that T must be a Galois extension of S relative to some finite group H of automorphisms of T. By [5, Th. 1.3, part (c)], T is a finitely generated, projective S-module and the left T-module $\mathrm{Hom}_s(T, T)$ is generated by H. T is a semi-local ring by the first lemma in [6], and it will now be shown that G acts transitively on the set of maximal ideals of T. Let m be a maximal ideal in T and let $q = \bigcap_{\sigma \in G/G_0} \sigma(m)$. q is a G/G_0-stable ideal in T. But by [14, Lemma 3.5], the left T-module $\mathrm{Hom}_s(T, T)$ is generated by the automorphisms of T induced by elements of G/G_0. Therefore, q is a left $\mathrm{Hom}_s(T, T)$-module and it follows from [5, Th. 1.3, part (d)] that $q = T \otimes_s (S \cap q)$. Let m' be a maximal ideal in T. T is integral over S [15, p. 254] and $S \cap m'$ must be the unique maximal ideal in S [15, p. 259]. Therefore, $S \cap q \subset S \cap m'$ and $q = T \cdot (S \cap q) \subset m'$. Since m' is a prime ideal, $\sigma(m) \subseteq m'$ whence, since $\sigma(m)$ is a maximal ideal in T, $\sigma(m) = m'$ for some $\sigma \in G/G_0$.

(1.3) If A is a finitely generated, projective left $Z \otimes_{\Gamma \cap C} C$-module and p is a prime ideal in Z, then A_p is a free module over $(Z \otimes_{\Gamma \cap C} C)_p$.

Proof. Assume that A is a finitely generated, projective left $Z \otimes_{\Gamma \cap C} C$-module. Let p be a prime ideal in Z, let $X = A_p$, and let $T = (Z \otimes_{\Gamma \cap C} C)_p$. Since there is a natural isomorphism of X onto the tensor product of T and A over $Z \otimes_{\Gamma \cap C} C$, X is a finitely generated, projective left T-module. X is a free left T-module if the rank of X over T is well defined [3, § 5, No. 3, Proposition 5]; and X is projective of rank n over T, for some integer n, if for every maximal ideal m in T the left T_m-module X_m is free of rank n [3, § 5, No. 3, Th. 2]. But, for every maximal ideal m in T, the left T_m-module X_m is free of finite rank by [3, § 5, No. 2, Th. 1]. Therefore, it remains

only to show that, for two maximal ideals m and m' in T, the rank of the left T_m-module X_m equals the rank of the left $T_{m'}$-module $X_{m'}$. $m' = \tau(m)$ for some $\tau \in G$, however; and one may readily verify that any such τ induces an isomorphism of T_m onto $T_{m'}$ and a one-to-one semi-linear transformation of X_m onto $X_{m'}$. Consequently, the ranks of these two free modules are equal.

PROPOSITION 2. *Let R be a semi-local ring; let Λ be a separable R-algebra which is a projective R-module; and let σ be an automorphism of Λ over R. Let Γ be a separable R-subalgebra of Λ, and let Z be the center of Γ. If Λ_p is a free left $(Z \otimes_R C)_p$-module for every prime ideal p in Z, then there is an inner automorphism τ of Λ such that $\tau \cdot \sigma$ leaves the elements of Γ invariant.*

Letting Λ^0 denote the opposite ring of Λ, Λ^0 is also a separable R-algebra with center C. Therefore $\Gamma \otimes_R \Lambda^0$ is a separable R-algebra with center $T = Z \otimes_R C$ by [2, Proposition 1.5]; and it follows from [2, Th. 2.3] that C, Z, and T are separable algebras over R, while $\Gamma \otimes_R \Lambda^0$ is a separable algebra over T. The crucial steps for the proof of this proposition will be treated separately.

(2.1) *T is a semi-local ring which extends Z.*

Proof. The subring $R \cdot 1$ of Λ is a semi-local ring, since it is a homomorphic image of R. Clearly Λ and Γ are separable algebras over $R \cdot 1$; Λ is a projective $R \cdot 1$-module; and σ is an automorphism of Λ over $R \cdot 1$. Therefore, R may be replaced by $R \cdot 1$, and consequently it may be assumed that Λ is a faithful R-algebra without loss of generality. Therefore, C and Z are finitely generated, projective R-modules by the first lemma of [6]; and consequently, T is a finitely generated, projective R-module. By a second application of the lemma of [6], it follows that T is a semi-local ring. Moreover the inclusion map of R into C induces an injection of $Z = Z \otimes_R R$ into T by which Z may be identified with a subring of T.

Now let Λ_1 designate the structure of a left $\Gamma \otimes_R \Lambda^0$-module on Λ which is determined by the rule $(\gamma \otimes \lambda)x = \gamma \cdot x \cdot \lambda$ for $\gamma \in \Gamma$ and λ, $x \in \Lambda$; and let Λ_2 designate the structure of a left $\Gamma \otimes_R \Lambda^0$-module on Λ which is determined by the rule $(\gamma \otimes \lambda)x = \sigma(\gamma) \cdot x \cdot \lambda$ for $\gamma \in \Gamma$ and λ, $x \in \Lambda$. Λ_1 and Λ_2 are finitely generated and projective as modules over R; and, therefore, Λ_1 and Λ_2 are finitely generated and projective as left modules over $\Gamma \otimes_R \Lambda^0$ and as left modules over T by [8, Lemma 2].

(2.2) If Λ_p is a free left T_p-module for every prime ideal p in Z, then Λ_1 and Λ_2 are isomorphic left $\Gamma \otimes_R \Lambda^0$-modules.

Proof. Assume that $\Lambda_p = (\Lambda_1)_p$ is a free left T_p-module for every prime ideal p in Z. Let m be a maximal ideal in T and let $p = Z \cap m$. Then p is a prime ideal in Z, $T_p = Z_p \otimes_Z T$ is naturally isomorphic to $Z_p \otimes_R C$, and σ induces a one-to-one semi-linear transformation of $(\Lambda_1)_p$ onto $(\Lambda_2)_p$ which has $1 \otimes \sigma$ as its associated automorphism on $Z_p \otimes_R C$. Therefore, $(\Lambda_1)_p$ and $(\Lambda_2)_p$ are free left T_p-modules of the same rank; and, consequently, they must be isomorphic. There is a unique extension of the canonical homomorphism of T onto the field T/m to a homomorphism of T_p onto T/m by [3, § 2, No. 1, Proposition 1], and there are natural isomorphisms

$$(T/m) \otimes_{T_p} (\Lambda_i)_p \cong (T/m) \otimes_{T_p} (T_p \otimes_T \Lambda_i) \cong (T/m) \otimes_T \Lambda_i \text{ for } i = 1, 2 .$$

Therefore, $(T/m) \otimes_T \Lambda_i$, $i = 1, 2$, are isomorphic left T-modules. Let $m_1, m_2, \cdots, m_k$ be the distinct maximal ideals in T, and let $q = \bigcap_{j=1}^k m_j$. q is the radical of T, T/q is canonically isomorphic to the direct sum $\sum_{j=1}^k T/m_j$, and $(T/q) \otimes_T \Lambda_i$ is naturally isomorphic to the direct sum $\sum_{j=1}^k (T/m_j) \otimes_T \Lambda_i$ for $i = 1, 2$. Therefore, $(T/q) \otimes_T \Lambda_i$, $i = 1, 2$, are isomorphic left T-modules. Since Λ_1 and Λ_2 are finitely generated, projective left T-modules; a T-module isomorphism of $(T/q) \otimes_T \Lambda_1$ onto $(T/q) \otimes_T \Lambda_2$ may be lifted to a T-module homomorphism of Λ_1 into Λ_2, which must be an isomorphism by [9, Lemma 1.7]. But then Λ_1 and Λ_2 are isomorphic left $\Gamma \otimes_R \Lambda^0$-modules by [6, Th. 1.1].

To complete the proof of the proposition, suppose that Ψ is a $\Gamma \otimes_R \Lambda^0$-module isomorphism of Λ_1 onto Λ_2. Then $\Psi(\lambda) = \Psi(1) \cdot \lambda$ for all $\lambda \in \Lambda$. Similarly $\Psi^{-1}(\lambda) = \Psi^{-1}(1) \cdot \lambda$ for $\lambda \in \Lambda$, and $\Psi^{-1}(1) \cdot \Psi(1) = 1 = \Psi(1) \cdot \Psi^{-1}(1)$. Thus $\Psi(1)$ is a unit in Λ. Let τ be the inner automorphism of Λ given by the rule $\tau(x) = \Psi(1)^{-1} \cdot x \cdot \Psi(1)$ for $x \in \Lambda$. For $\gamma \in \Gamma$, $\Psi(1) \cdot \gamma = \Psi(\gamma) = \sigma(\gamma) \cdot \Psi(1)$ and $\tau\sigma(\gamma) = \gamma$.

Any inner automorphism of a ring Λ leaves the elements of C invariant. Let R be a semi-local ring; let Λ be a separable R-algebra which is a projective R-module; and let G be a group of automorphisms of Λ over R. Λ is a separable algebra over C and C is a separable algebra over R by [2, Th. 2.3]. Therefore, C is a semi-local ring by the first lemma of [6], and it follows from [2, Th. 3.6] that every element of G_0 is an inner automorphism. Thus G_0 is the subgroup of inner automorphisms in G. Let $C(G)$ be the subalgebra of Λ which is generated over C by all units of Λ giving rise to inner automorphisms contained in G. Call G complete if every inner automorphism of Λ by a unit of $C(G)$ is an element of G. Call G regular if G is complete, $C(G)$ is a separable algebra over C, and G is the closure of a

group H of automorphisms of Λ such that H/H_0 is finite. Let Γ be a R-subalgebra of Λ and let Z be the center of Γ. Call Γ regular if Γ and $\Gamma \cap C$ are separable algebras over R; Λ^Γ is generated as an algebra over C by its units; and, for every prime ideal p in Z, Λ_p is a free left $(Z \otimes_{\Gamma \cap C} C)_p$-module.

It can be shown that the conditions of regularity given in the preceding paragraph are a generalization of the definitions of regularity presented in [6]. Indeed, if Λ is a ring with no nontrivial, central idempotents, then every group of automorphisms of Λ is closed. Now let Λ be a separable algebra over a commutative ring R, such that Λ is a projective R-module; let Γ be a separable R-subalgebra of Λ; let Z be the center of Γ; and assume that $Z \otimes_{\Gamma \cap C} C$ has no nontrivial idempotents. It is demonstrated in the proof of [6, Th. 2.1 R] that the subalgebra $Z \cdot C$ of Λ is separable over R and isomorphic to $Z \otimes_{\Gamma \cap C} C$. $\Gamma \cap C = Z \cap C$ is a separable algebra over R by [6, Corollary 1.7]; and Λ is a finitely generated, projective $Z \otimes_{\Gamma \cap C} C$-module by [8, Lemma 2]. Suppose further that R is a semi-local ring. Then $Z \otimes_{\Gamma \cap C} C$ is a semi-local ring by the first lemma of [6]; and it follows from [3, § 4, No. 3, Corollary 2, and § 5, No. 2, Th. 1] that the rank of the left $Z \otimes_{\Gamma \cap C} C$-module Λ is well defined. Therefore, Λ is a free left $Z \otimes_{\Gamma \cap C} C$-module by [3, § 5, No. 3, Proposition 5]; and it follows readily that Λ_p is a free left $(Z \otimes_{\Gamma \cap C} C)_p$-module for every prime ideal p in Z.

LEMMA. *Let Λ be a separable algebra over a commutative ring R; let G be a group of automorphisms of Λ over R, such that G/G_0 is finite; and let $\bar{G}$ be the closure of G. Every automorphism of C over $\Lambda^G \cap C$ is the restriction to C of an element of $\bar{G}$.*

Proof. Λ is a separable algebra over C and C is a separable algebra over R by [2, Th. 2.3]. $\Lambda^G \cap C$ is the subring of G/G_0-invariant elements of C and C is a separable algebra over $\Lambda^G \cap C$. Since C is commutative, C is an outer semi-Galois extension of $\Lambda^G \cap C$; and it follows from [10, Definition 2.4] and [14, Proposition 3.15] that C is weakly Galois over $\Lambda^G \cap C$. Let τ be an automorphism of C over $\Lambda^G \cap C$. τ is in the closure of G/G_0 by [14, Proposition 3.14]. Therefore, there exist a positive integer n, and $\sigma_i \in G$ and idempotents $e_i \in C$ for $1 \leqq i \leqq n$, such that $e_i \cdot \tau(x) = e_i \cdot \sigma_i(x)$ for $x \in C$ and $1 \leqq i \leqq n$ and $1 = \bigcup_{i=1}^n e_i$ in the Boolean algebra of idempotent elements of C. A set $\{\bar{e}_i \mid 1 \leqq i \leqq n\}$ of pairwise orthogonal idempotents in C, such that $\sum_{i=1}^n \bar{e}_i = 1$, is defined inductively by the rules $\bar{e}_1 = e_1$, and $\bar{e}_i = e_i \cdot (1 - \sum_{j=1}^{i-1} \bar{e}_j)$ for $2 \leqq i \leqq n$. Moreover, $\tau(x) = \sum_{i=1}^n \bar{e}_i \cdot \tau(x) = \sum_{i=1}^n \bar{e}_i \cdot \sigma_i(x)$ for $x \in C$. One may also verify that an endomorphism φ of the R-algebra Λ is given by the rule $\varphi(x) = \sum_{i=1}^n \bar{e}_i \cdot \sigma_i(x)$ for $x \in \Lambda$.

φ extends τ, and similarly τ^{-1} can be extended to an R-algebra endomorphism ψ of Λ. $\varphi\psi$ and $\psi\varphi$ are endomorphisms of Λ over C, and it follows from [2, Corollary 3.4] that $\varphi\psi$ and $\psi\varphi$ are automorphisms of Λ. Therefore, φ must be an automorphism of Λ. Clearly $\varphi \in \bar{G}$.

THEOREM. *Let R be a semi-local ring; let Λ be a separable R-algebra which is a projective R-module; and let G be a regular group of automorphisms of Λ over R. The classical Galois correspondence is a bijection between the set of regular subgroups of G and the set of regular subalgebras of Λ which contain Λ^G.*

First let H be a regular subgroup of G, let $\Gamma = \Lambda^H$, and let Z be the center of Γ. Clearly $\Lambda^G \subseteqq \Gamma$. Let K be a group of automorphisms of Λ such that K/K_0 is finite and H is the closure of K. It is easily verified that H is a closed group, K is a subgroup of H, and $\Lambda^K = \Gamma$. Since C is a separable algebra over R by [2, Th. 2.3], C must be a separable algebra over $\Gamma \cap C$. By Proposition 1, $\Lambda^{H_0} = \Gamma \otimes_{\Gamma\cap C} C$ and $Z \otimes_{\Gamma\cap C} C$ is the center of Λ^{H_0}. It will be shown by the following steps, that Γ is a regular subalgebra of Λ and H is the group of all automorphisms of Λ over Γ.

(3.1) Λ^{H_0} is a separable algebra over $\Gamma \cap C$ and $C(H)$ is the centralizer of Λ^{H_0} in Λ. Moreover, C is a projective $\Gamma \cap C$-module of which $\Gamma \cap C$ is a direct summand.

Proof. Since H_0 is the subgroup of all inner automorphisms in H, it is obvious that $\Lambda^{H_0} = \Lambda^{C(H)}$. But $C(H)$ is a separable algebra over C; and, therefore, Λ^{H_0} is a separable algebra over C and $C(H)$ is the centralizer of Λ^{H_0} in Λ by [8, Th. 2]. Since C is a separable algebra over R, Λ^{H_0} is a separable algebra over R. Consequently, Λ^{H_0} is a separable algebra over $\Gamma \cap C$. Furthermore, K/K_0 is a finite group of automorphisms of C and $\Gamma \cap C$ is the subring of K/K_0-invariant elements of C. Therefore, C is a projective $\Gamma \cap C$-module by [11, Lemma 1.5]; and it follows from [1, Proposition A. 3] and [12, Proposition 1] that $\Gamma \cap C$ is a $\Gamma \cap C$-module direct summand of C.

(3.2) Γ is a regular subalgebra of Λ.

Proof. Since $\Lambda^{H_0} = \Gamma \otimes_{\Gamma\cap C} C$, it is evident that Λ^Γ is the centralizer of Λ^{H_0} in Λ. Therefore, $\Lambda^\Gamma = C(H)$ and Λ^Γ is generated as an algebra over C by its units. Also $C \otimes_R C$ is a projective $(\Gamma \cap C) \otimes_R (\Gamma \cap C)$-module by [4, Chapter IX, Corollary 2.5]. Since C is a separable algebra over R, C is a projective $C \otimes_R C$-module; and, therefore, C is a projective $(\Gamma \cap C) \otimes_R (\Gamma \cap C)$-module. But $\Gamma \cap C$ is a $(\Gamma \cap C) \otimes_R (\Gamma \cap C)$-

module direct summand of C. Therefore, $\Gamma \cap C$ is a projective $(\Gamma \cap C) \otimes_R (\Gamma \cap C)$-module and $\Gamma \cap C$ is a separable algebra over R. Γ is a separable algebra over $\Gamma \cap C$ by [2, Proposition 1.7]; and, consequently, Γ is a separable algebra over R. Since $Z \otimes_{\Gamma \cap C} C$ is the center of Λ^{H_0}, $Z \otimes_{\Gamma \cap C} C$ is a separable algebra over R by [2, Th. 2.3] and Λ is a finitely generated, projective left $Z \otimes_{\Gamma \cap C} C$-module by [8, Lemma 2]. For every prime ideal p in Z, Λ_p is a free left $(Z \otimes_{\Gamma \cap C} C)_p$-module by Proposition 1. Thus Γ is a regular subalgebra of Λ.

(3.3) H is the group of all automorphisms of Λ over Γ.

Proof. If $\bar{H}$ is the group of all automorphism of Λ over Γ, then H is a subgroup of $\bar{H}$ and $\bar{H}_0$ is the group of all inner automorphisms of Λ over Γ. But every inner automorphism of Λ over Γ is given by a unit in $\Lambda^\Gamma = C(H)$. Since H is complete, it follows that $H_0 = \bar{H}_0$. H/H_0 is the group of all automorphisms of C over $\Gamma \cap C$ by the preceding lemma; and, therefore, $H/H_0 = \bar{H}/\bar{H}_0$ and $H = \bar{H}$.

Now let Γ be a regular subalgebra of Λ which contains Λ^G, and let H be the group of all automorphism of Λ over Γ. In the first part of the proof, it has been established that G is the group of all automorphisms of Λ over Λ^G, G/G_0 is the group of all automorphisms of C over $\Lambda^G \cap C$, C is a separable algebra over $\Lambda^G \cap C$, and $\Lambda^G \cap C$ is the subring of invariant elements of C with respect to some finite subgroup of G/G_0. Furthermore, since Λ and Γ are separable algebras over R, they are separable algebras over $\Gamma \cap C$. H must be a subgroup of G, and the proof will be completed by showing that H is regular and $\Gamma = \Lambda^H$.

(4.1) H is the closure of a group K such that $L = K/K_0$ is finite and $C^L = \Gamma \cap C$.

Proof. Since $\Gamma \cap C$ is a separable algebra over R, $\Gamma \cap C$ is a semi-local ring by the first lemma of [6], Λ is a projective $\Gamma \cap C$-module by [8, Lemma 2], and $\Gamma \cap C$ is a separable algebra over $\Lambda^G \cap C$. There exists a finite group L of automorphisms of C such that $\Gamma \cap C$ is the subring of L-invariant elements of C by [11, Lemma 1.5]. Let ρ be any automorphism of C over $\Gamma \cap C$. Then $\rho \in G/G_0$ and there exists $\sigma \in G$ which extends ρ to an automorphism of Λ over $\Gamma \cap C$. By Proposition 2, there exists an inner automorphism τ of Λ such that $\tau \cdot \sigma$ leaves the elements of Γ invariant. But then $\tau \cdot \sigma$ is an automorphism of Λ over Γ which coincides with ρ on C. Thus every automorphism of C over $\Gamma \cap C$ can be extended to an automorphism of Λ over Γ, and H/H_0 is the group of all automorphisms

of C over $\Gamma \cap C$. Let K be the subgroup of H such that $H_0 \subseteqq K$ and $K/H_0 = L$. Clearly $K_0 = H_0$, and therefore $K/K_0 = L$ which is finite. Letting $\bar{K}$ be the closure of K, it follows from the preceding lemma that $\bar{K}$ must contain representatives from all the cosets of H/H_0. Since $H_0 \subseteqq K$, $\bar{K} = H$.

(4.2) H is regular and $\Gamma = A^H$.

Proof. It is evident that H is closed, $A^K = A^H$, and $A^K \cap C = C^L = \Gamma \cap C$; and it follows from Proposition 1, that $A^{H_0} = A^H \otimes_{\Gamma \cap C} C$. C is a finitely generated, projective $\Gamma \cap C$-module by [11, Lemma 1.5]; and it follows from [1, Proposition A.3] and [12, Proposition 1] that $\Gamma \cap C$ is a $\Gamma \cap C$-module direct summand of C. C is a faithfully flat $\Gamma \cap C$-module by [10, Lemmas 1.5 and 1.6], and the inclusion map of Γ into A^H induces an injection of $\Gamma \otimes_{\Gamma \cap C} C$ into A^{H_0} by which $\Gamma \otimes_{\Gamma \cap C} C$ may be identified with a subring of A. $\Gamma \otimes_{\Gamma \cap C} C$ is a separable algebra over C by [2, Corollary 1.6], and obviously A^Γ is the centralizer of $\Gamma \otimes_{\Gamma \cap C} C$ in A. By [8, Th. 2], A^Γ is a separable algebra over C and $\Gamma \otimes_{\Gamma \cap C} C$ is the centralizer of A^Γ in A. But every inner automorphism of A over Γ is determined by a unit in A^Γ and A^Γ is generated as an algebra over C by its units. Therefore $C(H) = A^\Gamma$. Thus $C(H)$ is a separable algebra over C, and clearly H must be complete. Consequently, H is a regular subgroup of G. Moreover, since A^{H_0} is the centralizer of $C(H)$ in A, $\Gamma \otimes_{\Gamma \cap C} C = A^{H_0}$. Since C is a faithfully flat $\Gamma \cap C$-module, $\Gamma = A^H$.

Addendum. The Galois theory, which has been presented here for a separable algebra over a semi-local ring, can be extended to a separable algebra over a more general type of ring; and such an extension will be considered now. Let R be a commutative ring and let $B(R)$ be the Boolean algebra of idempotent elements of R. If x is a prime ideal in $B(R)$ and M is an R-module; let R_x be the ring of fractions of R with respect to the multiplicatively closed set $B(R) - x$, and let $M_x = R_x \otimes_R M$. In [7], F. R. DeMeyer considers the following condition on R.

(*) R_x is a semi-local ring for every prime ideal x in $B(R)$.

R_x is a homomorphic image of R for every prime ideal x in $B(R)$ by [14, Equations 2.5 and 2.6]; and, therefore, any semi-local ring will satisfy condition (*). The first lemma in [6] may be generalized to include the following result.

LEMMA. *Let $R \subseteq S \subseteq A$ be rings with S separable over R and commutative, and A finitely generated and projective over R. If R satisfies condition (*), then S satisfies condition (*).*

Proof. Suppose that R satisfies the condition (*), and let x be a prime ideal in $B(S)$. $B(R)$ is a subring of $B(S)$ and $y = x \cap B(R)$ is a prime ideal in $B(R)$. Therefore, R_y is a semi-local ring. Moreover, $S_y = R_y \otimes_R S$ is a separable algebra over R_y by [2, Corollary 1.6], and $A_y = R_y \otimes_R A$ is a finitely generated and projective module over R_y. Since R_y is a flat R-module [3, § 2, No. 4, Th. 1], the inclusion maps of R into S and S into A induce injections of $R_y = R_y \otimes_R R$ into S_y and S_y into A_y, by which R_y and S_y may be identified with subrings of A_y. It follows from the first lemma of [6] that S_y is a semi-local ring. By [3, § 2, No. 1, Corollary 2 and No. 2, Proposition 6] the canonical homomorphism of S into S_x factors as the composition of the canonical homomorphism of S into S_y and a unique homomorphism of S_y into S_x. But the canonical homomorphism of S into S_x is epic, and therefore S_x is a homomorphic image of S_y. Consequently, S_x must be a semi-local ring, and S satisfies the condition (*).

Let R be a commutative ring which satisfies condition (*); let Λ be a separable R-algebra which is a projective R-module; and let G be a group of automorphisms of Λ over R. Λ is a separable algebra over C and C is a separable algebra over R by [2, Th. 2.3]. Therefore, C satisfies condition (*) by the preceding lemma, and it follows from [7, Th. 4] that every element of G_0 is an inner automorphism. The definitions of regular group of automorphisms and regular subalgebra may be applied to Λ, and the proof of the theorem of this paper can be carried out in this case once the following generalization of Proposition 2 has been established.

PROPOSITION 3. *Let R be a commutative ring which satisfies condition (*); let Λ be a separable R-algebra which is a projective R-module; and let σ be an automorphism of Λ over R. Let Γ be a separable R-subalgebra of Λ, and let Z be the center of Γ. If Λ_p is a free left $(Z \otimes_R C)_p$-module for every prime ideal p in Z, then there is an inner automorphism τ of Λ such that $\tau \cdot \sigma$ leaves the elements of Γ invariant.*

Proof. Γ is a finitely generated module over Z by [2, Ths. 2.1 and 2.3], Z is a finitely generated module over R by the first lemma in [6], and therefore Γ is a finitely generated module over R. Let n be a positive integer and let $\{a_i \mid 1 \leqq i \leqq n\}$ be a set of generators

for the R-module Γ. Let x be a prime ideal in $B(R)$. R_x is a semi-local ring; and, by [2, Corollary 1.6], $\Lambda_x = R_x \bigotimes_R \Lambda$ is a separable R_x-algebra with center $C_x = R_x \bigotimes_R C$ and $\Gamma_x = R_x \bigotimes_R \Gamma$ is a separable R_x-algebra with center $Z_x = R_x \bigotimes_R Z$. Also Λ_x is a projective R_x-module, and $1 \otimes \sigma$ is an automorphism of Λ_x. Since R_x is a flat R-module [3, § 2, No. 4, Th. 1], the inclusion map of Γ into Λ induces an injection of Γ_x into Λ_x by which Γ_x may be identified with a subalgebra of Λ_x. Let q be a prime ideal in Z_x, let $i(x/Z)$ be the canonical homomorphism of Z into Z_x, and let $p = \{i(x/Z)\}^{-1}(q)$. By [3, § 2, No. 2, Proposition 6 and No. 5, Proposition 11], p is a prime ideal in Z and $(Z_x)_q = Z_p$. There is a natural isomorphism of Λ_x onto $Z_x \bigotimes_Z \Lambda$, and it follows readily that $(\Lambda_x)_q = \Lambda_p$ and $(Z_x \bigotimes_{R_x} C_x)_q = (Z \bigotimes_R C)_p$. Now suppose that Λ_p is a free left $(Z \bigotimes_R C)_p$-module for every prime ideal p in Z. By Proposition 2, there is an inner automorphism $\bar{\tau}$ of Λ_x such that $\bar{\tau} \cdot (1 \otimes \sigma)$ leaves the elements of Γ_x invariant. Since R_x is isomorphic to $R/R \cdot x$ [14, Equation 2.6], Λ_x is isomorphic to $\Lambda/\Lambda \cdot x$ and there must exist elements $b(x), c(x)$ in Λ such that $b(x) \cdot c(x) \equiv 1 (\mathrm{mod}\, \Lambda \cdot x)$, $c(x) \cdot b(x) \equiv 1 (\mathrm{mod}\, \Lambda \cdot x)$ and $b(x) \cdot \sigma(a_i) \cdot c(x) \equiv a_i (\mathrm{mod}\, \Lambda \cdot x)$ for $1 \leqq i \leqq n$. By [14, Lemma 2.8], there exists $e(x) \in X$ such that $b(x) \cdot c(x) \cdot (1 - e(x)) = 1 - e(x)$, $c(x) \cdot b(x) \cdot (1 - e(x)) = 1 - e(x)$, and $b(x) \cdot \sigma(a_i) \cdot c(x) \cdot (1 - e(x)) = a_i(1 - e(x))$. Since $1 - e(x) \notin x$, the ideal of $B(R)$ which is generated by the set $\{1 - e(x) \mid x$ is a prime ideal in $B(R)\}$ cannot be contained in any prime ideal of $B(R)$ and therefore must equal $B(R)$. Thus, in the Boolean algebra $B(R)$, 1 must be a linear combination of finitely many of the $1 - e(x)$. But if m is a positive integer and x_j is a prime ideal in $B(R)$ for $1 \leqq j \leqq m$, such that 1 is a linear combination of the elements $1 - e(x_j)$ in $B(R)$, then 1 must be the least upper bound for the subset $\{1 - e(x_j) \mid 1 \leqq j \leqq m\}$ of $B(R)$. A set $\{f_j \mid 1 \leqq j \leqq m\}$ of pairwise orthogonal idempotent elements of R, such that $\sum_{j=1}^m f_j = 1$, is defined inductively by the rules $f_1 = 1 - e(x_1)$, and

$$f_j = (1 - e(x_j)) \cdot \left(1 - \sum_{k=1}^{j-1} f_k\right)$$

for $2 \leqq j \leqq m$. Setting $b = \sum_{j=1}^m f_j \cdot b(x_j)$ and $c = \sum_{j=1}^m f_j \cdot c(x_j)$, one obtains that $b \cdot c = 1 = c \cdot b$ and $b \cdot \sigma(a_i) \cdot c = a_i$ for $1 \leqq i \leqq n$. Thus $c = b^{-1}$; and, letting τ be the inner automorphism of Λ given by the rule $\tau(\lambda) = b \cdot \lambda \cdot b^{-1}$ for $\lambda \in \Lambda$, $\tau\sigma(a_i) = a_i$ for $1 \leqq i \leqq n$. Since $\{a_i \mid 1 \leqq i \leqq n\}$ is a set of generators for the R-module Γ, $\tau\sigma(\gamma) = \gamma$ for all $\gamma \in \Gamma$.

Finally, let it be observed that in the definition of a regular subalgebra Γ of an algebra Λ over a commutative ring R, the requirement that $\Gamma \cap C$ be separable over R is redundant. Indeed, let R be a commutative ring and let Λ be a separable R-algebra which is a projective R-module. Let Γ be a separable R-subalgebra of Λ, let

Z be the center of Γ, and observe that $\Gamma \cap C = Z \cap C$. C and Z are separable R-algebras by [2, Th, 2.3], and $Z \cap C$ is a separable R-algebra by [7, Lemma 10].

REFERENCES

1. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1-24.
2. ———, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367-409.
3. N. Bourbaki, *Algebre commutative*, Chap. 2, Hermann, Paris, 1961 (Act. Scient. et Ind. 1290).
4. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, Princeton, N. J., 1956.
5. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1965), 15-33.
6. L. N. Childs and F. R. DeMeyer, *On automorphisms of separable algebras*, Pacific J. Math. **23** (1967), 25-34.
7. F. R. DeMeyer, *On automorphisms of separable algebras*, II (to appear in the Pacific J. Math.)
8. T. Kanzaki, *On commutor rings and Galois theory of separable algebras*, Osaka J. Math. **1** (1964), 103-115.
9. H. F. Kreimer, *Galois theory for noncommutative rings and normal bases*, Trans. Amer. Math. Soc. **127** (1967), 42-49.
10. ———, *A note on the outer Galois theory of rings*, Pacific J. Math. **31** (1969), 417-432.
11. ———, *Outer Galois theory for separable algebras*, Pacific J. Math. **32** (1970), 147-155.
12. T. Nakayama, *On a generalized notion of Galois extension of a ring*, Osaka J. Math. **15** (1963), 11-23.
13. O. E. Villamayor and D. Zelinsky, *Galois theory for rings with finitely many idempotents*, Nagoya Math. J. **27** (1966), 721-731.
14. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83-98.
15. O. Zariski and P. Samuel, *Commutative algebra*, vol. 1, D. Van Nostrand Co., Inc., Princeton, N. J., 1958.

Received October 29, 1969. The author gratefully acknowledges receiving support in his research from the National Science Foundation under grant GP-8424.

THE FLORIDA STATE UNIVERSITY