PACIFIC JOURNAL OF MATHEMATICS
Vol. 23, No. 1, 1967

ON AUTOMORPHISMS OF SEPARABLE ALGEBRAS

L. N. CHILDS AND F. R. DEMEYER

This paper presents a Galois theory for separable algebras over a (not necessarily Noetherian) semi-local ring. Our theory is patterned after, but independent of the Galois theory of G. Hochschild; over a perfect field Hochschild's theory and ours coincide.

In order to present this theory we first present some results concerning separable algebras over semilocal rings. The most important of these is a generalization of the Skolem-Noether theorem. Our theorem states that any algebra monomorphism of a separable subalgebra without central idempotents into a central separable algebra whose center is semilocal extends to an inner automorphism.

We assume throughout this paper that all rings have identity, all subrings contain the identity of the larger ring, all modules are unitary and all ring homomorphisms carry identity to identity. The notation $[S:R]$ will denote the rank of S as a free R-module, and if R is a commutative ring, the statement "R is connected" will mean that R has no idempotents other than 0 and 1. We will assume the reader is familiar with [1] and [6], all unexplained notation is as in [1].

We begin by noting the following facts, which we will sometimes employ without reference in the sequel. They will eliminate the need for assumptions of finite generation and projectivity in many places as we proceed:

LEMMA. *If $R \subsetneqq S \subsetneqq A$ are rings with S separable over R and commutative, and A finitely generated and projective over R, then S is finitely generated and projective over R. If in addition R is semi-local, then S is semi-local.*

Proof. S is separable over R and A is a finitely generated, faithful and projective R-module, so A is a finitely generated, faithful, and projective S-module by Lemma 2 of [10]. Since S is commutative, Theorem A.3 of [2] implies that there exist f_i in $\mathrm{Hom}_S(A, S)$ and x_i in A so that $1 = \sum f_i(x_i)$. Define $f: A \rightarrow S$ by $f(x) = \sum f_i(xx_i)$, f is easily seen to be an S-module epimorphism which is split by the inclusion map of S into A. Thus S is an S-direct summand of A, so is finitely generated and projective over R, since A is. If R is semi-local, letting J be the (Jacobson) radical of R, R/J is a finite direct sum of fields, and S/JS is a finite dimensional algebra over R/J so that S/JS has only a finite number of maximal ideals. S is integral over R, so maximal ideals of S contract to maximal ideals of R ([12], p. 208), and thus JS is contained in the radical of S, and maximal ideals of S correspond to maximal ideals of S/JS. We conclude that S is semi-local.

THEOREM 1.1. *Let Y be a central separable algebra over C, a semi-local ring. If A and A' are two finitely generated projective left Y-modules which are isomorphic as C-modules, then they are isomorphic as Y-modules.*

Proof. Write C/N as a direct sum of fields $C_1, \cdots, C_n$, and correspondingly write Y/NY as a direct sum of central simple C_i-algebras Y_i. This gives a decomposition of the Y/NY-module A/NA into the direct sum of Y/NY-submodules A_i. The Y_i-isomorphism class of A_i is determined by the dimension of A_i over C_i. Since A and A' are isomorphic as C-modules, so are A/NA and A'/NA'. Hence, if we decompose A' as we decomposed A above, we have that the dimension of A'_i over C_i is equal to the dimension of A_i over C_i. Thus we may conclude that A/NA and A'/NA' are isomorphic as Y/NY-modules, and so also as Y-modules. Let $f: A/NA \rightarrow A'/NA'$ be a Y-module isomorphism. Since A is Y-projective, f lifts to a Y-module homomorphism $f^*: A \rightarrow A'$. We have $f^*(A) + NA' = A'$, and since A' is finitely generated it follows that $f^*(A) = A'$. Let Q denote the kernel of f^*. Since A' is Y-projective, Q is a direct Y-module summand of A, and so is also finitely generated. Moreover, since $Q \subset NA$, we have $Q = NQ$, whence $Q = (0)$. Thus f^* is an isomorphism, and the theorem is proved.

It seems unlikely that Theorem 1.1 can be extended much further since it fails even in the case where C is a principal ideal domain. For let C be the ring of integers in $Q(\sqrt{3})$(Q the rationals), and let Y be a maximal order in the quaternion algebra over $Q(\sqrt{3})$. Utilizing the work of H. Bass ([4], p. 31 and p. 46) one can show that Y is central separable over C, but that the map $\gamma_Y(P) \rightarrow \gamma_C(P)$ from $K^\circ(Y)$ to $K^\circ(C)$ (see [4] p. 31 for the meaning of this notation) is not a monomorphism which it must be if Theorem 1.1 holds.

THEOREM 1.2. *Let R be a semi-local ring, let A be a separable, finitely generated projective R-algebra with center K, let B be a separable R-subalgebra of A with connected center C containing K, and let σ be an R-algebra monomorphism of B into A leaving K fixed, then σ can be extended to an inner automorphism of A.*

Proof. Let $Y = B \otimes_K A^0$, and define left Y-module structures on A via $(b \otimes a)x = bxa$ and $(b \otimes a)x = \sigma(b)xa$, calling the resulting modules A_1 and A_2. They are both projective Y-modules. C and $\sigma(C)$ are semilocal, so over each A is free. Thus A_1 and A_2 are isomorphic as C-modules. Applying Theorem 1.1, we obtain that $A_1 \cong A_2$ as left Y-modules via a map h. Then $h(1 \cdot a) = h(1)a$ for all a in A, so $h(1)$ is a unit of A; $h(b) = h(1)b = \sigma(b)h(1)$, so $\sigma(b) = h(1)bh(1)^{-1}$. Thus σ extends to an inner automorphism of A.

Theorem 1.2 also fails over a principal ideal domain. For if A, A' are two nonisomorphic separable orders over a principal ideal domain R in a central simple K-algebra Σ, where K is the quotient field of R, then since by [1], 7.2, A and A' are in the same class in the Brauer group of R (see [1]), there are isomorphic matrix algebras M, M' over R such that $A \otimes_R M \cong A' \otimes_R M'$. The isomorphism of M to M' cannot extend, else the extension, when restricted to A, would yield an isomorphism of A and A'. An example of such an A and A' is found in [11].

We will make strong use of Theorem 1.2 in the next section. Now we can obtain, in analogy with the field case, the following:

COROLLARY 1.3. *If K is a semi-local ring, A is a central separable K-algebra, B is a separable subalgebra of A with connected center C containing K, and A^B is the commutator of B in A, then $[A:K] = [B:K] \cdot [A^B:K]$.*

Proof. (In this Proof $\otimes$ will be $\otimes_K$ and M will denote $\mathrm{End}_K(B)$.) C is a projective K-algebra, so all the ranks make sense. Consider B inside $A \otimes M = L$ via $B \otimes K = B'$ and $K \otimes B = B''$. If σ is the obvious isomorphism of B' to B'', then by Theorem 1.2 σ extends to an inner automorphism τ of L. By restriction τ defines an isomorphism of $L^{B'}$ onto $L^{B''}$. Now

$$L^{B'} \cong \mathrm{Hom}_{B' \otimes L^\circ}(L, L) \cong \mathrm{Hom}_{B \otimes K \otimes A \otimes M^\circ}(A \otimes M, A \otimes M) .$$

Since A and M° are finitely generated and projective as $B \otimes A^\circ$ and $K \otimes M^\circ$ modules, respectively, an application of ϕ_3 of [5], p. 210, yields that

$$L^{B'} \cong \mathrm{Hom}_{B' \otimes A^\circ}(A, A) \otimes \mathrm{Hom}_{K \otimes M^\circ}(M, M) \cong A^B \otimes M .$$

Similarly, $L^{B''} \cong A \otimes M^B = A \otimes B^\circ$. Considering the ranks of $L^{B'}$ and $L^{B''}$ as K-modules, we obtain that

$$[A^B : K] \cdot [B : K]^2 = [A : K] \cdot [B : K] ,$$

and thus the desired result.

We recall a definition from [7] (cf. [6], 1.3b):

DEFINITION. Let A be a ring with unit and G a finite group of automorphisms of A with fixed ring B. A is a Galois extension of B with group G if there exist elements $x_1, \cdots, x_n, y_1, \cdots, y_n$ of A such that for all σ in G, $\sum_i x_i\sigma(y_i) = \begin{cases} 0 & \sigma \neq e \\ 1 & \sigma = e. \end{cases}$

With this extended definition of Galois extension, the statement and proof of [6], Lemma 3.4, remains valid. We insert it without proof as:

LEMMA 1.4. *Let A, B be Galois extensions of C with group G. Let $f: A \to B$ be a ring homomorphism such that $f(c) = c$ for all c in C and $f(\sigma(x)) = \sigma(f(x))$ for all x in A, σ in G. Then f is an isomorphism.*

We use this lemma in:

THEOREM 1.5. *Let A be a separable, projective algebra over the connected commutative ring K, and let J be a finite group of ring automorphisms of A with the property that J restricted to K is isomorphic to J. Let R be the subring of elements of K left fixed by J and assume K is separable and finitely generated as an R-algebra. If B is the subring of A left fixed by J, then B is a separable R-algebra and $A \cong B \otimes_R K$.*

Proof. By [6], Theorem 1.3, K is a Galois extension of R with group J. It then follows directly from the definition of Galois extension that A is a Galois extension of B with group J, and also, if J is defined on $B \otimes_R K$ via $\sigma(b \otimes k) = b \otimes \sigma(k)$, that $B \otimes_R K$ is a Galois extension of B with group J. Defining $h: B \otimes_R K \to A$ via $h(b \otimes k) = bk$, h is an isomorphism by Lemma 1.4. Since $R \cdot 1$ is an R-direct summand of K by [1], Prop. A.3, by [5], IX, 7.1, B is separable over R.

The next result, due to D. K. Harrison, appears with proof in [9]; we state it for later reference as:

THEOREM 1.6. *Let T be a connected commutative ring, projective and separable over a subring R, then there is a connected ring E containing T which is a Galois extension of R.*

COROLLARY 1.7. *Let T, R be as in Theorem 1.6 and let S and*

S' be separable R-subalgebras of T, then $S \cap S'$ is a separable R-algebra.

Proof. Embed T inside a Galois extension E of R with Galois group G. Since S and S' are separable subalgebras of E, they are the fixed rings of subgroups H and H', respectively. Then $S \cap S'$ is the fixed ring of the subgroup of G generated by H and H', so is separable over R.

REMARK. If in Theorem 1.5 the center of A is connected and B' is any R-separable subalgebra of A containing B, then $B' \cap K$ is separable over R by Corollary 1.7. In this case Theorem 1.5 can be easily adapted to generalize the outer Galois theory for central separable algebras of [7], Theorem 3 (and hence of [10], Theorem 5).

We conclude this section with a technical lemma needed in Theorem 2.2R:

LEMMA 1.8. *Let L be a finitely generated separable K-algebra with K a semi-local ring, then L is generated as a K-algebra by its units.*

Proof. If Z is the center of L then Z is finitely generated and separable over K, hence semi-local. Let N be the radical of Z, then L/NL is semi-simple, so is even generated as a ring by its units. The result will follow once we show that NL is the radical of L, for since units mod radical lift to units, each element of L differs from an element generated by its units by at most an element of NL and each x in NL can be written as $1-(1-x)$ which is a sum of units.

Now, since the radical of L is the intersection of two-sided ideals of L containing the ideals m_vL for m_v maximal ideals of Z ([3], p. 125), and since two-sided ideals of L are precisely of the from aL for a an ideal of Z, the radical of L is $\bigcap_v m_vL = NL$.

2. Throughout this section we shall adhere to the following notations and assumptions:

R is a commutative semi-local ring, and A is a separable, finitely generated, projective R-algebra with center K. Thus K is semi-local, by the lemma preceding Theorem 1.1. We assume also that K is connected. G is the group of all R-algebra automorphisms of A; we assume that the ring of all elements of A left fixed by G is precisely R.

If H is a subgroup of G we let H_0 be the normal subgroup of H

consisting of those elements which are inner automorphisms of A, $R(H)$ be the subring of A generated as a K-algebra by all the units giving the inner automorphisms of A, and A^H be the fixed ring of H. If B is an R-subalgebra of A we let G_B be the group of all elements of G leaving B elementwise fixed.

Call a subgroup H of G complete if every inner automorphism of A by an element of $R(H)$ is in H. If $R(H)$ is a separable K-algebra with connected center, then $R(H)$ is a finitely generated free K-module, so we define the reduced order of H to be $(H/H_0:1)\cdot[R(H):K]$. Following [8] we call a subgroup H of G regular if H is complete, $R(H)$ is a separable K-algebra with connected center, and H has finite reduced order. We note that in our situation this last assumption is redundant: H/H_0 is finite because by Theorem 3.5 of [6] G/G_0 is finite.

If B is an R-subalgebra of A we call B regular if B is separable as an R-algebra and $B \otimes_{B\cap K} K$ has connected center.

If R is a perfect field these definitions reduce to those in [8]. For the same reasons as in the field theory it is the regular subgroups and the regular subalgebras which the Galois theory relates.

THEOREM 2.1G. *If H is a regular subgroup of G, then A^H is a regular R-subalgebra of A, and H is the group of all automorphisms of A leaving A^H fixed. Moreover, the reduced order of H is equal to $[A:R]/[A^H:R]$.*

Proof. An easy computation shows that A^{H_0} is the commutator of $R(H)$ in A, thus by Theorem 2 of [10], A^{H_0} is a separable R-algebra. Now H leaves $R(H)$ setwise invariant, so H leaves its commutator in A, A^{H_0}, invariant. Thus restricting H to A^{H_0} yields a group of automorphisms H' of A^{H_0} leaving A^H fixed which is isomorphic to H/H_0. Similarly H leaves K invariant. Since all automorphisms of A leaving K fixed are inner, H restricted to K is also isomorphic to H/H_0 and can be viewed as the restriction of H' to K. Since H/H_0 is contained in G/G_0, the Galois group of K over R, $K^{H'} = K^H = K \cap A^H$ is separable over R by Theorem 2.2 of [6]. The center of A^{H_0}, being the same as the center of $R(H)$, is projective and separable over K. Furthermore, K, being the center of A, is projective and separable over R, so A^{H_0} is projective and separable over R. H' is a finite group, so we may apply Theorem 1.5 to obtain that A^H is separable over K^H, and $A^{H_0} = A^H \otimes K$ (tensor over K^H). Since $K^H = A^H \cap K$ is separable over R, A^H is separable over R, while the center of A^{H_0} is connected by the assumption on $R(H)$. Thus A^H is a regular subalgebra of A.

H is the full group of automorphisms of A leaving A^H fixed: for H_0 contains all the inner automorphisms of A^H since H is complete, while $H' = H/H_0$ contains all the automorphisms of A^{H_0} leaving A^H fixed by Theorem 3.5 of [9].

Since for rings $R \subseteqq S \subseteqq T$, $[T:R] = [S:R]\cdot[T:S]$ whenever these ranks are defined, the statement about the reduced order of H is proved as follows:

$$\begin{aligned}[R(H):K]\cdot(H/H_0:1) &= [R(H):K]\cdot[K:K^H] \text{ by Theorem 4.1 of [6]}\\ &= ([A:K]/[A^{H_0}:K])\cdot[K:K^H] \text{ by Corollary 1.3}\\ &= ([A:R]/[A^{H_0}:R])\cdot[K:K^H]\\ &= [A:R]/[A^H:R] \text{ since } A^{H_0} = A^H \otimes K \text{ (tensor over } K^H).\end{aligned}$$

We note that, except for the statement about reduced orders, this part of the Galois theory does not depend on Theorem 1.2 and hence holds whenever all K-projective modules are free.

THEOREM 2.1R. *Let B be a regular subalgebra of A containing R, then the group G_B is a regular subgroup of B and B is the fixed ring of G_B.*

Proof. If Z is the center of B, then $Z \otimes_{B\cap K} K$ is the center of $B \otimes_{B\cap K} K$, so $Z\cdot K$ is the center of $B\cdot K$ and is separable over R. Hence $Z\cdot K$ is projective over R. Once we show that $Z\cdot K$ is connected, we can apply Corollary 1.7 to infer that $Z \cap K = B \cap K$ is separable over R.

To show that $Z\cdot K$ is connected we show that $j : B \otimes_{B\cap K} K \to B\cdot K$ is an isomorphism. For $\ker(j) = I\cdot(B \otimes_{B\cap K} K)$, where I is an ideal of $Z \otimes_{Z\cap K} K$. Thus j induces by restriction an exact sequence of $Z \otimes_{Z\cap K} K$-modules:

$$0 \to I \to Z \otimes_{Z\cap K} K \to Z\cdot K \to 0 .$$

$Z\cdot K$ is a projective R-module, so since $Z \otimes_{Z\cap K} K$ is a separable R-algebra $Z\cdot K$ is a projective $Z \otimes_{Z\cap K} K$ module. Hence the sequence splits and I is generated by an idempotent. Since $Z \otimes_{Z\cap K} K$ is connected, $I = 0$ and j is an isomorphism.

Now G/G_0 is a group of automorphisms of K leaving R fixed, so by [6], Theorem 3.5, G/G_0 is finite and K is a Galois extension of R. $B \cap K$ is separable over R, so K is a Galois extension of $B \cap K$ with group $J' \subseteqq G/G_0$. Extend each σ' in J' to $B\cdot K = B \otimes_{B\cap K} K$ via

$$\sigma'(bk) = b\sigma'(k) .$$

Lift σ', viewed in G/G_0, to an element σ of G. Then σ, restricted to

K, $= \sigma'$, so $\sigma^{-1}\sigma' : B\cdot K \to A$ leaves K fixed. Since $B\cdot K$ has connected center, $\sigma^{-1}\sigma'$ extends by Theorem 1.2 to an inner automorphism τ of A. Now σ' is $\sigma\tau$ restricted to $B\cdot K$, so σ' extends to an automorphism of A. Each σ' in J' in this way extends to an element of G_B, and since J' defined on $B\cdot K$ leaves exactly B fixed, G_B must leave exactly B fixed.

The commutator L in A of B is the commutator in A of $B\cdot K$, so is finitely generated and separable over K with connected center. Clearly any inner automorphism of G_B comes from a unit in L and every unit in L forms an inner automorphism in G_B. To show that $L = R(G_B)$ and consequently that G_B is regular, it suffices to show that L is generated as a K-algebra by units, and this is a consequence of Lemma 1.8.

We retain the notation of Theorem 2.1 in:

THEOREM 2.2. *If B is a regular subalgebra of A and G_B is a normal subgroup of G, then G/G_B is the group of all R-algebra automorphisms of B.*

Proof. If $G_B = H$ is a normal subgroup of G then $H' = H/H_0$ is a normal subgroup of $G' = G/G_0$. So $B \cap K$ is a Galois extension of R with group G'/H' and G'/H' contains all automorphisms of $B \cap K$ leaving R fixed. Let σ' be an R-algebra automorphism of B. σ' restricted to $B \cap K$ is in G'/H' so lifts to an element σ of G. Then $\tau' = \sigma^{-1}\sigma'$ is an automorphism of B leaving $B \cap K$ fixed. Define τ' on $B \otimes_{B\cap K} K = B\cdot K$ by $\tau'(bk) = \tau'(b)k$, then τ' is an automorphism of $B\cdot K$ leaving K fixed, so extends by Theorem 1.2 to an automorphism τ of G. So $\sigma\tau$ restricted to B is equal to σ', that is, σ' is in G/H. It is easy to see that G/H is contained in the group of all R-algebra automorphisms of B.

Following [8] we call a subalgebra B of A almost regular in case B is separable over R and $B\cdot K$ has connected center. Every regular subalgebra is almost regular; in our context the converse also holds.

THEOREM 2.3. *With A, K, R, and G as above, every almost regular R-subalgebra of A is regular.*

Proof. Let B be an almost regular subalgebra of A. Since $B\cdot K$ has connected center, it suffices to show that the natural map

$$j : B \otimes_{B\cap K} K \to B\cdot K$$

is an isomorphism. As in the proof of theorem 2.1R it suffices to show that the map $j' : Z \otimes_{Z \cap K} K \to Z \cdot K$ is an isomorphism, where Z is the center of B.

Since $Z \cdot K$ is connected, $Z \cap K = L$ is separable over R by Corollary 1.7, thus $Z \otimes_L K$ and $Z \cdot K$ are projective (hence free) over L, and j' splits as an L-module map, so that as L-modules $Z \otimes_L K = Z \cdot K + W$. We shall show $W = 0$ by comparing the ranks of $Z \otimes_L K$ and $Z \cdot K$ as free L-modules.

Using Theorem 1.6, let S be a Galois extension of L containing $Z \cdot K$ with Galois group G. Let G_Z, G_K and $G_{Z \cdot K}$ be the groups of all automorphisms of G leaving Z, K and $Z \cdot K$ elementwise fixed, respectively. K is a Galois extension of L so G_K is a normal subgroup of G. Since $G_Z \cdot G_K$ leaves exactly L fixed, by [6], Theorem 3.5, it is G; it follows by a standard isomorphism theorem that $G_{Z \cdot K}$ is a normal subgroup of G_Z, $Z \cdot K$ is a Galois extension of Z, and $G_Z / G_{Z \cdot K} \cong G / G_K =$ the Galois group of K over L. But then, using [6], Theorem 4.1,

$$\begin{aligned}[][Z \cdot K : L] &= [Z : L] \cdot [Z \cdot K : Z] = [Z : L] \cdot (G_Z / G_{Z \cdot K} : 1) \\ &= [Z : L] \cdot [K : L] = [Z \otimes_L K : L] ,\end{aligned}$$

proving the theorem.

Most of the results in this paper were obtained independently and without knowledge of the other's work by the two authors; except that the method of proof of Theorem 1.1 is largely due to DeMeyer. The work of Childs forms part of his doctoral dissertation at Cornell University under the direction of A. Rosenberg. Childs would like to express his appreciation to Professor Rosenberg for his advice and encouragement. DeMeyer would like to thank G. J. Janusz and E. Davis for many helpful conversations.

BIBLIOGRAPHY

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

2. ———, *Maximal orders,* Trans, Amer. Math. Soc. **97** (1960), 1-24.

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

4. H. Bass, *K-theory and stable algebra,* Publ. Math. I.H.E.S. **22** (1964), 5-60.

5. H. Cartan and S. Eilenberg, *Homological Algebra,* Princeton, 1956.

6. S. Chase, D. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings,* Mem. Amer. Math. Soc. **52** (1965), 15-33.

7. F. R. DeMeyer, *Some notes on the general Galois theory of rings,* Osaka J. Math. **2** (1965), 117-127.

8. G. Hochschild, *Automorphisms of simple algebras,* Trans. Amer. Math. Soc. **69** (1950), 292-301.

9. G. J. Janusz, *Separable algebras over commutative rings,* Trans. Amer. Math. Soc. (1966).

10. T. Kanzaki, *On commutor rings and Galois theory of separable algebras*, Osaka J. Math. **1** (1964), 103-115.
11. R. G. Swan, *Projective modules over group rings and maximal orders*, Ann. of Math. **76** (1962), 55-61.
12. O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1, Princeton, D. Van Nostrand Co., 1960.

Received March 15, 1966 and in revised form October 13, 1966.