PACIFIC JOURNAL OF MATHEMATICS
Vol. 31, No. 2, 1969

A NOTE ON THE OUTER GALOIS THEORY OF RINGS

H. F. KREIMER

Let G be a finite group of automorphisms of a ring B, and let A be the subring of G-invariant elements of B. Call B an outer semi-Galois extension of A, if the centralizer of A in B is the center of B and B is a separable extension of A (i.e., the (B, B)-bimodule homomorphism of $B \otimes_A B$ onto B, which is determined by the ring multiplication in B, splits). The principal result of this paper is more easily stated here under the additional hypothesis that A is a direct summand of the right A-module B.

THEOREM. If B is an outer semi-Galois extension of a subring A_0 and A_0 is a direct summand of the right A_0-module B, then the following statements are equivalent for an intermediate ring A.

(1) B is an outer semi-Galois extension of A and A is a direct summand of the right A-module B.

(2) B is a projective Frobenius extension of A.

(3) A is the subring of invariant elements of B with respect to a finite group of automorphisms of B (not necessarily a subgroup of G).

For outer Galois theory, this result is an improvement on the Galois theory for noncommutative rings presented by the author in [7] and by Y. Miyashita in [8], since the characterization of the intermediate ring in the Galois correspondence does not depend on the choice of G. If B is a commutative ring, then essentially the same result (with a different proof) can be found also in a forthcoming paper, "Galois theory in rings with infinitely many idempotents", by O. Villamayor and D. Zelinsky.

A general Galois correspondence between subrings of a ring B and subrings of the ring of endomorphisms of the additive group of B is described in §1, and the Galois closure of a subring in B is defined. These results are used to sharpen a theorem on Frobenius extensions, and the basic concepts of the Galois theory of rings are summarized. In §2, the concept of outer semi-Galois extension is introduced. The principal results of the paper are proved in §3.

1. Preliminaries.

For the most part, the terminology and notation in [7] are followed throughout this paper. The most notable exception is that, whereas the image of an element a under a mapping φ was denoted by $a\varphi$ in [7], the more common notation $\varphi(a)$ will be used in the sequel. In particular, ring will mean ring with identity element and subring of a ring will mean subring which contains the identity element of the ring.

Let B be a ring and let $\mathfrak{B}$ be the ring of all endomorphisms of the additive group of B. The operations of left multiplication on B by elements of B form a subring of $\mathfrak{B}$, which is naturally isomorphic to B. Thus $\mathfrak{B}$ may be regarded as an extension of B and $\mathfrak{B}$ supports the structure of a left B-module. If A is a subring of B and $\mathrm{Hom}(B_A, B_A)$ denotes the ring of right A-module endomorphisms of B, then $\mathrm{Hom}(B_A, B_A)$ is both a subring and a left B-submodule of $\mathfrak{B}$. But, if $\mathfrak{A}$ is a subring of $\mathfrak{B}$, then B is a left $\mathfrak{A}$-module; and, if $\mathfrak{A}$ is both a subring and a left B-submodule of $\mathfrak{B}$, then $\mathfrak{A}$ contains the ring of left multiplications on B by elements of B and the ring $\mathrm{Hom}({}_{\mathfrak{A}}B, {}_{\mathfrak{A}}B)$ of left $\mathfrak{A}$-module endomorphisms of B must be the ring $\bar{A}_R$ of right multiplications on B by elements of some subring $\bar{A}$ of B.

Let $\mathfrak{A} = \mathrm{Hom}(B_A, B_A)$ for a subring A of B. The subring $\bar{A}$ of B such that $\mathrm{Hom}({}_{\mathfrak{A}}B, {}_{\mathfrak{A}}B) = \bar{A}_R$ will be called the Galois closure of A in B. Clearly $A \subseteqq \bar{A}$ and $\bar{A}$ is the largest subring of B such that $\mathrm{Hom}(B_A, B_A) = \mathrm{Hom}(B_{\bar{A}}, B_{\bar{A}})$. If $A = \bar{A}$, A will be said to be Galois closed in B. $\mathfrak{A}$ is naturally isomorphic to $\mathrm{Hom}((B \otimes_A B)_B, B_B)$, which is the dual of the right B-module $B \otimes_A B$; and $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ is naturally isomorphic to the second dual of $B \otimes_A B$. Now suppose that B is a finitely generated, projective right A-module. Then $B \otimes_A B$ is a finitely generated, projective right B-module; $\mathfrak{A}$ is a finitely generated, projective left B-module; $\mathfrak{A}$ is naturally isomorphic to $B \otimes_A \mathrm{Hom}(B_A, A_A)$; and $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ is naturally isomorphic to $B \otimes_A B$. Since

$$\mathrm{Hom}(B_A, A_A) \subseteqq \mathrm{Hom}(B_A, \bar{A}_A) = \mathrm{Hom}(B_{\bar{A}}, \bar{A}_{\bar{A}}) ,$$

the natural homomorphism of $B \otimes_{\bar{A}} \mathrm{Hom}(B_{\bar{A}}, \bar{A}_{\bar{A}})$ into $\mathrm{Hom}(B_{\bar{A}}, B_{\bar{A}}) = \mathfrak{A}$ must be epic. Therefore B is a finitely genereted, projective right $\bar{A}$-module and $\mathfrak{A}$ is naturally isomorphic to $B \otimes_{\bar{A}} \mathrm{Hom}(B_{\bar{A}}, \bar{A}_{\bar{A}})$ by [1, proposition A.1]. Moreover $B \otimes_A B = B \otimes_{\bar{A}} B$.

The following proposition gives an application of the concept of Galois closure to the theory of (projective) Frobenius extensions [6].

PROPOSITION 1.1. *Let A be a subring of a ring B such that B is a finitely generated, projective right A-module; let $\mathfrak{A} = \mathrm{Hom}(B_A, B_A)$; and let $\bar{A}$ be the Galois closure of A in B.*

(1) *If B is a Frobenius extension of A, then $\mathfrak{A}$ is a Frobenius extension of B and* $\mathrm{Hom}(B_A, A_A) = \mathrm{Hom}(B_{\bar{A}}, \bar{A}_{\bar{A}})$.

(2) *If $\mathfrak{A}$ is a Frobenius extension of B, then B is a Frobenius extension of $\bar{A}$.*

Proof. According to the definition and Remark 1 in [6, §1, 2], $\mathfrak{A}$ is a Frobenius extension of B if and only if there is an $(\mathfrak{A}, B)$-bimodule isomorphism of $\mathrm{Hom}\,({}_B\mathfrak{A}, {}_BB)$ onto $\mathfrak{A}$. Since there is a natural isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathrm{Hom}\,({}_B\mathfrak{A}, {}_BB)$, $\mathfrak{A}$ is a Frobenius extension of B if and only if there is an $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$. Suppose B is a Frobenius extension of A. Then there is an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}\,(B_A, A_A)$ by Remark 1 of [6, §1.2]. Consequently, there is an $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_A B$ onto $B \otimes_A \mathrm{Hom}\,(B_A, A_A)$. But $B \otimes_A B = B \otimes_{\bar{A}} B$ and $B \otimes_A \mathrm{Hom}\,(B_A, B_A)$ is naturally isomorphic to $\mathfrak{A}$. Therefore there is an $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$.

Now suppose that there is an $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$, and let $\gamma \in \mathfrak{A}$ correspond to $1 \otimes 1 \in B \otimes_{\bar{A}} B$ under this isomorphism. If $b, b' \in B$ and $\varphi \in \mathfrak{A}$; then $\varphi \circ (b' \cdot \gamma \cdot b) = \varphi(b') \cdot \gamma \cdot b$, since both correspond to $\varphi(b') \otimes b$ under the given $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$. It follows readily from the definition of $\bar{A}$ that $\gamma \cdot b \in \mathrm{Hom}\,(B_{\bar{A}}, \bar{A}_{\bar{A}})$. Also $\gamma \cdot a = a \cdot \gamma$ for $a \in \bar{A}$. There must exist a positive integer n and elements b_j, b'_j of B, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} b_j \cdot \gamma \cdot b'_j$ is the identity map on B. If $x \in B$ and $\psi \in \mathrm{Hom}\,(B_{\bar{A}}, \bar{A}_{\bar{A}})$; then

$$\psi(x) = \psi\Big(\sum_{j=1}^{n} b_j \cdot \gamma(b'_j \cdot x)\Big) = \sum_{j=1}^{n} \psi(b_j) \cdot \gamma(b'_j \cdot x) = \gamma\Big(\Big(\sum_{j=1}^{n} \psi(b_j) \cdot b'_j\Big) \cdot x\Big) .$$

Thus $\psi = \gamma \cdot c$ for $c = \sum_{j=1}^{n} \psi(b_j) \cdot b'_j$. Therefore the composition of the $(\bar{A}, B)$-bimodule monomorphism of B into $B \otimes_{\bar{A}} B$ which maps b onto $1 \otimes b$ with the given $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$ is an $(\bar{A}, B)$-bimodule isomorphism of B onto $\mathrm{Hom}\,(B_{\bar{A}}, \bar{A}_{\bar{A}})$. Consequently B is a Frobenius extension of $\bar{A}$. Moreover, if the $(\mathfrak{A}, B)$-bimodule isomorphism of $B \otimes_{\bar{A}} B$ onto $\mathfrak{A}$ is derived from an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}\,(B_A, A_A)$, then $\gamma \in \mathrm{Hom}\,(B_A, A_A)$. Therefore $\gamma \cdot b \in \mathrm{Hom}\,(B_A, A_A)$ for $b \in B$, and

$$\mathrm{Hom}\,(B_A, A_A) = \mathrm{Hom}\,(B_{\bar{A}}, \bar{A}_{\bar{A}}) .$$

COROLLARY 1.2. *Let A be a Galois closed subring of a ring B such that B is a finitely generated, projective right A-module. B is a Frobenius extension of A if, and only if,* $\mathrm{Hom}\,(B_A, B_A)$ *is a Frobenius extension of B.*

The following three lemmas are restatements of results contained in [9].

LEMMA 1.3. *Let A be a subring of B, let* $\mathfrak{A} = \mathrm{Hom}\,(B_A, B_A)$, *and let $\mathscr{T}(B_A)$ be the trace ideal of the right A-module B.* $\mathscr{T}(B_A) = A$

if, and only if, B is a finitely generated, projective left $\mathfrak{A}$-module and Hom $({}_{\mathfrak{A}}B, {}_{\mathfrak{A}}B) = A_R$.

LEMMA 1.4. *Let $\mathfrak{A}$ be a subring and left B-submodule of $\mathfrak{B}$, let $\bar{A}$ be that subring of B such that* Hom $({}_{\mathfrak{A}}B, {}_{\mathfrak{A}}B) = \bar{A}_R$, *and let $\mathscr{T}({}_{\mathfrak{A}}B)$ be the trace ideal of the left $\mathfrak{A}$-module B. $\mathscr{T}({}_{\mathfrak{A}}B) = \mathfrak{A}$ if, and only if, B is a finitely generated, projective right $\bar{A}$-module and $\mathfrak{A} =$* Hom $(B_{\bar{A}}, B_{\bar{A}})$.

LEMMA 1.5. *Let A be a subring of B. $\mathscr{T}(B_A) = A$ if, and only if, A is a direct summand of the right A-module B.*

In the application of these results, the following lemma is useful.

LEMMA 1.6. *Let A be a subring of B such that B is a finitely generated, projective right A-module. $\mathscr{T}(B_A) = A$ if, and only if, B is a faithfully flat right A-module.*

Proof. Since B is a projective right A-module, B is a flat right A-module. Suppose $\mathscr{T}(B_A) = A$. Then A is a direct summand of the right A-module B by Lemma 1.5, and $A \otimes_A X$ is a direct summand of the additive group $B \otimes_A X$ for any unital left A-module X. But $A \otimes_A X$ is naturally isomorphic to X. Consequently, if $B \otimes_A X = 0$ then $X = 0$; and B is a faithfully flat right A-module by [3, Chapter 1, §3, No. 1, Proposition 1].

Conversely, suppose B is a faithfully flat right A-module. Let $\mathfrak{A} =$ Hom (B_A, B_A) and let τ be the evaluation map of Hom $(B_A, A_A) \otimes_{\mathfrak{A}} B$ into A. $\mathfrak{A}$ is naturally isomorphic to $B \otimes_A$ Hom (B_A, A_A), $B \otimes_A A$ is naturally isomorphic to B, and the map $1 \otimes \tau$ of $B \otimes_A$ Hom $(B_A, A_A) \otimes_{\mathfrak{A}} B$ into $B \otimes_A A$ corresponds to the natural isomorphism of $\mathfrak{A} \otimes_{\mathfrak{A}} B$ onto B. Therfore $1 \otimes \tau$ is an isomorphism, and τ is an isomorphism by [3, Chapter 1, §3, No. 1, Proposition 2]. Since $\mathscr{T}(B_A)$ is the image of τ, $\mathscr{T}(B_A) = A$.

From Lemmas 1.3 and 1.4 one obtains a Jacobson-Bourbaki type of correspondence [cf. 5] between the set of subrings A of B such that B is a finitely generated, projective right A-module and $\mathscr{T}(B_A) = A$, and the set of subrings $\mathfrak{A}$ of $\mathfrak{B}$ such that $\mathfrak{A}$ is a left B-submodule of $\mathfrak{B}$, B is a finitely generated, projective left $\mathfrak{A}$-module, and $\mathscr{T}({}_{\mathfrak{A}}B) = \mathfrak{A}$. Call B a generalized Galois extension of a subring A if B is a finitely generated, projective right A-module and $\mathscr{T}(B_A) = A$. In the definition of generalized Galois extension B of a subring A, the requirement that $\mathscr{T}(B_A) = A$ may be replaced by either of the equivalent conditions given in Lemmas 1.5 and 1.6. Lemma 1.3 asserts that $\mathscr{T}(B_A) = A$ is a sufficient condition for a subring A of B to be Galois closed in B. In particular, if B is a generalized Galois extension of a subring A, then A is Galois closed in B. It is a consequence of Corollary 1.2 that a generalized Galois extension B of a subring A is a Frobenius extension if, and only if, $\mathrm{Hom}(B_A, B_A)$ is a Frobenius extension of B. This assertion may be seen to be equivalent to the corollary in [6, §2.4] by observing that, if the right A-module B possesses a direct summand which is isomorphic to A, then there exists a right A-module homomorphism of B onto A and $\mathscr{T}(B_A) = A$.

Let G be a finite group of automorphism of a ring B, let A be the subring of G-invariant elements of B, and let $\varDelta$ be the crossed product of B and G with trivial factor set. Clearly A is Galois closed in B and there is a canonical ring homomorphism i of $\varDelta$ into $\mathrm{Hom}(B_A, B_A)$.

PROPOSITION 1.7. *The following statements are equivalent.*

(1) *G is a strongly independent group of automorphisms of B.*

(2) *There exist a positive integer n and elements x_j, y_j of B, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} \sigma(x_j)\cdot y_j = \delta_{1,\sigma}$ for all $\sigma \in G$.*

(3) *B is a finitely generated, projective right A-module and i is an isomorphism of $\varDelta$ onto* $\mathrm{Hom}(B_A, B_A)$.

Proof. If $\sum_{j=1}^{n} \sigma(x_j)\cdot y_j = \delta_{1,\sigma}$ for all $\sigma \in G$, then $\sum_{j=1}^{n} \sigma(x_j)\cdot \tau(y_j) = \tau(\sum_{j=1}^{n} \tau^{-1}\sigma(x_j)\cdot y_j) = \delta_{\sigma,\tau}$ for all $\sigma, \tau \in G$. Therefore, it is a consequence of [7, Proposition 2.3] that G is a strongly independent set of automorphisms of B if, and only if, there exists a positive integer n and elements x_j, y_j of B, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} \sigma(x_j)\cdot y_j = \delta_{1,\sigma}$ for all $\sigma \in G$. The equivalence of statements 2 and 3 is proved in [4, Th. 1].

Following the terminology in [2], call B a Galois extension of A relative to G if any of the statements of Proposition 1.7 is satisfied. Call B an outer Galois extension of A if B is a Galois extension of A and the centralizer of A in B is the center of B. Now suppose B is a Galois extension of A relative to G, and let $\mathfrak{A} = \mathrm{Hom}(B_A, B_A)$. Then G freely generates the left B-module $\mathfrak{A}$. Let $\{\sigma^* \mid \sigma \in G\}$ be the dual basis for the right B-module $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$. But $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ is also a left $\mathfrak{A}$-module; and, for $b \in B$ and $\rho, \sigma \in G$, $\rho\cdot\sigma^* = (\sigma\cdot\rho^{-1})^*$ and $b\cdot\sigma^* = \sigma^*\cdot\sigma(b)$. It is easily verified that the left B-module homomorphism of $\mathfrak{A}$ into $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ which maps σ onto $(\sigma^{-1})^*$, for $\sigma \in G$, is an $(\mathfrak{A}, B)$-bimodule isomorphism. Therefore $\mathfrak{A}$ is a Frobenius extension of B. B is a Frobenius extension of A by Corollary 1.2. Let n be a positive integer and let x_j, y_j be elements of B for $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} x_j \otimes y_j \in B \otimes_A B$ corresponds to $1^* \in \mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ under the natural isomorphism of $\mathrm{Hom}({}_B\mathfrak{A}, {}_BB)$ onto $B \otimes_A B$. Then

$$\sum_{j=1}^{n} x_j\cdot y_j = 1 \quad \text{and} \quad \sum_{j=1}^{n} bx_j \otimes y_j = \sum_{j=1}^{n} x_j \otimes y_j b$$

for every $b \in B$. Thus B is also a separable extension of A.

PROPOSITION 1.8. *Let B be a Galois extension of A with Galois group G. The following statements are equivalent.*

(1) *A is a direct summand of the right A-module B.*

(2) *B is a faithfully flat right A-module.*

(3) $\mathscr{T}(B_A) = A$.

(4) *There exists $c \in B$ such that $\sum_{\sigma \in G} \sigma(c) = 1$.*

Proof. Statements 1, 2, and 3 are equivalent by Lemmas 1.5 and 1.6. Also, statement 4 implies statement 1 by [7, Lemma 2.8]. Now suppose that B is a faithfully flat right A-module and let $\omega = \sum_{\sigma \in G} \sigma$. $1 \otimes \omega$ is a left B-module homomorphism of $B \otimes_A B$ into $B \otimes_A A$, and $B \otimes_A A$ is naturally isomorphic to B. There exist a positive integer n and elements x_j, y_j of $B, 1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} \sigma(x_j) \cdot y = \delta_{1,\sigma}$ for $\sigma \in G$. But then $\sum_{j=1}^{n} x_j \cdot \omega(y_j) = 1$; and, consequently, $1 \otimes \omega$ is an epimorphism. Since B is a faithfully flat right A-module, ω is an epimorphism and there must exist $c \in B$ such that $\omega(c) = 1$. Therefore statement 2 implies statement 4.

It follows from [7, Corollary 3.7 and Lemmas 3.2 and 2.8] that B is a K-ring with respect to G if, and only if, B is a Galois extension of A relative to G and there exists $c \in B$ such that $\sum_{\sigma \in G} \sigma(c) = 1$. Propositions 1.7 and 1.8 may be used to formulate a number of conditions equivalent to B being a K-ring with respect to G. In particular, B is a K-ring with respect to G if, and only if, B is a generalized Galois extension of A and i is an isomorphism of Δ onto $\mathrm{Hom}\,(B_A, B_A)$.

The preceding considerations are simpler in the case of commutative rings. For instance, suppose A is a commutative subring of a ring B such that B is a finitely generated, projective right A-module. Then $\mathscr{T}(B_A) = A$ by [1, proposition A.3], and so B is a generalized Galois extension of A. The situation for noncommutative rings is illustrated by the following example.

EXAMPLE 1.9 Let B be the ring of 3×3 matrices over a field F of characteristic two; and let e_{ij} denote the element of B with entry 1 in the i-th row and j-th column and entry 0 elsewhere, for $1 \leqq i, j \leqq 3$. Let σ be the inner automorphism of B determined by $e_{12} + e_{21} + e_{33}$. Then

$$\sigma \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} a_{22} & a_{21} & a_{23} \\ a_{12} & a_{11} & a_{13} \\ a_{32} & a_{31} & a_{33} \end{bmatrix} \quad \text{for} \quad a_{ij} \in F, \qquad 1 \leqq i, j \leqq 3 .$$

σ generates a subgroup G of order two in the group of all automorphisms of B. Let A be the subring of G-invariant elements of B. Since statement 2 of Proposition 1.7 is satisfied for $x_1 = e_{11} = y_1$, $x_2 = e_{22} = y_2$, $x_3 = e_{32}$, and $y_3 = e_{23}$; B is a Galois extension of A relative to G. But since the characteristic of F is two,

$$(1+\sigma)\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} a_{11}+a_{22} & a_{12}+a_{21} & a_{13}+a_{23} \\ a_{12}+a_{21} & a_{11}+a_{22} & a_{13}+a_{23} \\ a_{31}+a_{32} & a_{31}+a_{32} & 0 \end{bmatrix}$$

for $a_{ij} \in F$, $1 \leqq i, j \leqq 3$. Therefore there is no element c of B such that $(1+\sigma)(c)$ is the identity matrix and B is not a K-ring with respect to G. In particular, B is a finitely generated, projective right A-module and A is Galois closed in B, but B is not a generalized Galois extension of A [cf. 9, Remark 3]. Moreover, since B is a Frobenius extension of A, this example demonstrates that Corollary 1.2 is a sharper result than the corollary in [6, §2.4].

2. Outer semi-Galois extensions. The central idempotent elements of a ring play an important role in the outer Galois theory of rings, as the following lemma indicates.

LEMMA 2.1. *Let A be a subring of a ring B, such that the centralizer of A in B is the center of B and the left B-module* $\mathrm{Hom}(B_A, B_A)$ *is freely generated by a finite set M of automorphisms of B over A. $\eta \in \mathrm{Hom}(B_A, B_A)$ is a ring endomorphism such that $\eta(1) = 1$ if, and only if, $\eta = \sum_{\sigma \in M} e_\sigma \cdot \sigma$ where $\{e_\sigma \mid \sigma \in M\}$ is a set of pairwise orthogonal, central idempotents in B such that $\sum_{\sigma \in M} e_\sigma = 1$.*

Proof. Let $\eta \in \mathrm{Hom}(B_A, B_A)$; since the left B-module $\mathrm{Hom}(B_A, B_A)$ is freely generated by M, η has a unique representation as $\eta = \sum_{\sigma \in M} e_\sigma \cdot \sigma$ where $e_\sigma \in B$ for $\sigma \in M$. Suppose η is a ring endomorphism of B such that $\eta(1) = 1$. Then $\sum_{\sigma \in M} e_\sigma = \eta(1) = 1$, and $\eta(x) \cdot \sum_{\sigma \in M} e_\sigma \cdot \sigma(y) = \eta(x) \cdot \eta(y) = \eta(xy) = \sum_{\sigma \in M} e_\sigma \cdot \sigma(x) \cdot \sigma(y)$ for $x, y \in B$. Therefore $\sum_{\sigma \in M} \eta(x) \cdot e_\sigma \cdot \sigma = \sum_{\sigma \in M} e_\sigma \cdot \sigma(x) \cdot \sigma$ and $\eta(x) \cdot e_\sigma = e_\sigma \cdot \sigma(x)$ for $x \in B$ and $\sigma \in M$. Since $\eta, \sigma \in \mathrm{Hom}(B_A, B_A)$; e_σ must be an element of the centralizer of A in B, which is the center of B, for $\sigma \in M$. But then $e_\sigma \cdot \sigma = e_\sigma \cdot \eta = \sum_{\tau \in M} e_\sigma \cdot e_\tau \cdot \tau$ and $e_\sigma \cdot e_\tau = \delta_{\sigma,\tau} \cdot e_\sigma$ for $\sigma, \tau \in M$. Thus $\{e_\sigma \mid \sigma \in M\}$ is a set of pairwise orthogonal, central idempotents in B such that $\sum_{\sigma \in M} e_\sigma = 1$. Conversely, suppose $\{e_\sigma \mid \sigma \in M\}$ is a set of pairwise orthogonal, central idempotents in B such that $\sum_{\sigma \in M} e_\sigma = 1$. Then $\eta(1) = \sum_{\sigma \in M} e_\sigma = 1$, and $\eta(xy) = \sum_{\sigma \in M} e_\sigma \cdot \sigma(x) \cdot \sigma(y) = \eta(x) \cdot \eta(y)$ for $x, y \in B$. Therefore η is a ring endomorphism such that $\eta(1) = 1$.

Let E be the set of all central idempotent elements of a ring B, and partially order E by setting $e \leqq f$ if $e \cdot f = e$ for $e, f \in E$. E 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 $e, f \in E$. An automorphism of B restricts to an automorphism of the Boolean algebra E; and, thereby, any group of automorphisms of B is represented as a group of automorphisms of the Boolean algebra E.

Let A be a subring of a ring B; and let S be a finite set of pairwise orthogonal, central idempotents in B, such that $\sum_{e \in S} e = 1$. The right A-module B is a direct sum of its submodules $Be, e \in S$; and Be is a ring containing Ae as a subring for each $e \in S$. Now assume that $S \subseteqq A$. If Y is a right A-module then $\mathrm{Hom}\,(B_A, Y_A) = \prod_{e \in S} \mathrm{Hom}\,(Be_A, Y_A) = \prod_{e \in S} \mathrm{Hom}\,(Be_{Ae}, Ye_{Ae})$; and it is easily verified that B is a finitely generated, projective right A-module if, and only if, Be is a finitely generated, projective right Ae-module for each $e \in S$. Likewise, it is easily verified that A is a direct summand of the right A-module B, B is a Frobenius extension of A, A is Galois closed in B, the centralizer of A in B is the center of B, or B is a separable extension of A, if and only if the respective condition is satisfied by the ring Be and its subring Ae for each $e \in S$. Moreover the group of all automorphisms of B over A is canonically isomorphic to the direct product of the groups of automorphisms of Be over Ae, $e \in S$; and in the sequel it will be convenient to use this isomorphism to identify any group of automorphisms of Be over $Ae, e \in S$, with a subgroup of the group of automorphisms of B over A.

LEMMA 2.2. *Let T be a finite set of pairwise orthogonal, central idempotents in a ring B, such that $\sum_{e \in T} e = 1$; let g be a groupoid of ring isomorphisms between elements of the set $\{Be \mid e \in T\}$; let $g(Be, Be')$ be the set of isomorphisms in g which map Be onto Be' for $e, e' \in T$; and let $A = \{b \in B \mid \sigma(be) = be'$ for $\sigma \in g(Be, Be')$ and $e, e' \in T\}$. Then A is a subring of B; and there exist a finite set S of pairwise orthogonal, central idempotents in B, such that $\sum_{e \in S} e = 1$ and $S \subseteqq A$; and a group G_e of automorphisms of Be for each $e \in S$, satisfying the following conditions.*

(1) *For each $e \in S$, Ae is the subring of G_e-invariant elements of Be.*

(2) *If $g(Be, Be)$ is finite for each $e \in T$, then G_e is finite for each $e \in S$. If in addition, for each $e \in T$, there exists $c \in Be$ such that $\sum_{\sigma \in g(Be,Be)} \sigma(c) = e$; then, for each $e \in S$, there exists $c \in Be$ such that $\sum_{\sigma \in G_e} \sigma(c) = e$.*

(3) *If $G(Be, Be)$ is a finite, strongly independent group of automorphisms of Be for each $e \in T$, then G_e is a finite, strongly independent group of automorphisms of Be for each $e \in S$.*

Proof. The verification that A is a subring of B is straightforward and will be omitted. The condition that $g(Be, Be')$ be nonempty for $e, e' \in T$ defines an equivalence relation on T, and an equivalence class of elements of T will be called a component of the groupoid g. Letting $e_C = \sum_{e \in C} e$ for each component C of g, it is readily verified that $S = \{e_C \mid C \text{ is a component of } g\}$ is a finite set of pairwise orthogonal, central idempotents in B such that $\sum_{e \in S} e = 1$ and $S \subseteqq A$. Let C be a given component of g, let m be the cardinality of C, let $e_0, e_1, \cdots, e_{m-1}$ be an enumeration of the distinct elements of C, and choose $\tau_i \in g(Be_0, Be_i)$ for $0 \leqq i \leqq m-1$. Observe that $g(Be_i, Be_j) = \tau_j \cdot g(Be_0, Be_0) \cdot \tau_i^{-1}$ for $0 \leqq i, j \leqq m-1$. It is convenient to define τ_i for every integer i by requiring that $\tau_i = \tau_j$ if $i \equiv j (\text{mod } m)$. Setting $\bar{\tau}(\sum_{i=0}^{m-1} b \cdot e_i) = \sum_{i=0}^{m-1} \tau_{i+1} \cdot \tau_i^{-1}(b \cdot e_i)$ for $b \in B$, $\bar{\tau}$ is an automorphism of order m on the ring $B \cdot e_C$. Setting $\bar{\sigma}(\sum_{i=0}^{m-1} b \cdot e_i) = \sum_{i=0}^{m-1} \tau_i \cdot \sigma \cdot \tau_i^{-1}(b \cdot e_i)$ for $b \in B$ and $\sigma \in g(Be_0, Be_0)$, $\bar{\sigma}$ is an automorphism of the ring $B \cdot e_C$ and $\bar{\sigma} \cdot \bar{\tau} = \bar{\tau} \cdot \bar{\sigma}$. The correspondence of $\bar{\sigma}$ to $\sigma \in g(Be_0, Be_0)$ is a monomorphism of $g(Be_0, Be_0)$ into the group of automorphisms of $B \cdot e_C$; and, letting G be the subgroup of the group of automorphisms of $B \cdot e_C$ which is generated by the image of $g(Be_0, Be_0)$ and $\bar{\tau}$, G is the direct product of the image of $g(Be_0, Be_0)$ and the cyclic group of order m generated by $\bar{\tau}$. Therefore G is finite whenever $g(Be_0, Be_0)$ is finite. If $\rho \in g(Be_i, Be_j)$ for $0 \leqq i, j \leqq m-1$, then $\rho = \tau_j \cdot \sigma \cdot \tau_i^{-1}$ for some $\sigma \in g(Be_0, Be_0)$ and ρ coincides with the restriction of $\bar{\tau}^{j-i} \cdot \bar{\sigma}$ to Be_i. Consequently, the subring of G-invariant elements of $B \cdot e_C$ is $A \cdot e_C$. Now assume that $g(Be_0, Be_0)$ is finite. If there exists $c \in Be_0$ such that $\sum_{\sigma \in g(Be_0, Be_0)} \sigma(c) = e_0$, then $c \in B \cdot e_C$ and $\sum_{i=0}^{m-1} \sum_{\sigma \in g(Be_0, Be_0)} \bar{\tau}^i \bar{\sigma}(c) = \sum_{i=0}^{m-1} \tau_i(e_0) = \sum_{i=0}^{m-1} e_i = e_C$. If $g(Be_0, Be_0)$ is a strongly independent group of automorphisms of Be_0, then there exist a positive integer n and elements x_j, y_j of Be_0, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} \sigma(x_j) \cdot y_j = \delta_{1,\sigma} \cdot e_0$ for $\sigma \in g(Be_0, Be_0)$. But then $\tau_i(x_j), \tau_i(y_j)$, $0 \leqq i \leqq m-1$ and $1 \leqq j \leqq n$, are elements of $B \cdot e_C$; and, for any integer k and $\sigma \in g(Be_0, Be_0)$, $\sum_{i=0}^{m-1} \sum_{j=1}^{n} \bar{\tau}^k \bar{\sigma}(\tau_i(x_j)) \cdot \tau_i(y_j) = \sum_{i=0}^{m-1} \sum_{j=1}^{n} \tau_{i+k}(\sigma(x_j)) \cdot \tau_i(y_j)$, which is e_C if $k \equiv 0 \pmod{m}$ and $\sigma = 1$, but is 0 otherwise. Therefore G is a strongly independent group of automorphisms of $B \cdot e_C$. To each $e \in S$, there corresponds a component of the groupoid g and the preceding construction yields a group G_e of automorphisms of $B \cdot e$, satisfying the requirements of the lemma.

The technique of working with a groupoid g of ring isomorphisms, as in the preceding lemma, is due to Villamayor and Zelinsky [10]. Note that, if A is a subring of a ring B such that the centralizer of A in B is the center of B, then the center of A is the intersection of A with the center of B. The author is indebted to D. Zelinsky for suggesting the following theorem.

THEOREM 2.3. *Let A be a subring of a ring B such that the* *centralizer of A in B is the center of B. The following statements are equivalent.*

(1) *B is a separable extension of A and A is the subring of invariant elements of B with respect to a finite group of automorphisms of B.*

(2) *There exists a finite set S of pairwise orthogonal, central idempotents in A, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of Ae (relative to some finite group of automorphisms of Be) for each $e \in S$.*

Proof. Suppose B is a separable extension of A and A is the subring of invariant elements of B with respect to a finite group G of automorphisms of B. Since B is a separable extension of A, there exist a positive integer n and elements x_j, y_j of $B, 1 \leqq j \leqq n$, such that $\sum_{j=1}^n x_j \cdot y_j = 1$ and $\sum_{j=1}^n bx_j \otimes y_j = \sum_{j=1}^n x_j \otimes y_j b$ in $B \otimes_A B$ for every $b \in B$. Setting $e_\sigma = \sum_{j=1}^n \sigma(x_j) \cdot y_j$ for $\sigma \in G$, $\sigma(b) \cdot e_\sigma = e_\sigma \cdot b$ for $b \in B$ and $\sigma \in G$. Therefore e_σ is an element of the centralizer of A in B, which is the center of B, for $\sigma \in G$. Moreover, $e_\sigma^2 = \sum_{j=1}^n \sigma(x_j) \cdot y_j \cdot e_\sigma = \sum_{j=1}^n \sigma(x_j) \cdot e_\sigma \cdot y_j = \sum_{j=1}^n e_\sigma \cdot x_j \cdot y_j = e_\sigma$ for $\sigma \in G$. Therefore $\{\sigma(e_\tau) \mid \sigma, \tau \in G\}$ is a finintie set of central idempotents in B, which generates a finite, G-stable subalgebra E_0 of the Boolean algebra E of all central idempotents in B. Let T be the set of minimal elements of E_0. For $e \in T$ and $f \in E_0$, either $ef = e$ or $ef = 0$; and it is easily verified that T is a finite, G-stable set of pairwise orthogonal, central idempotents in B, such that $\sum_{e \in T} e = 1$. A groupoid g of ring isomorphisms between elements of the set $\{Be \mid e \in T\}$ is obtained by letting $g(Be, Be')$ be the set of isomorphisms of Be onto Be' which are restrictions of elements of G for $e, e' \in T$. Since A is the subring of G-invariant elements of B, $A = \{b \in B \mid \sigma(be) = be'$ for $\sigma \in g(Be, Be')$ and $e, e' \in T\}$. Since G is finite, $g(Be, Be)$ is finite for each $e \in T$. For $e \in T$ and $\rho \in G$, $\sum_{j=1}^n \rho(x_j) \cdot y_j e = e_\rho \cdot e$. Either $e_\rho \cdot e = e$ or $e_\rho \cdot e = 0$; but, if $e_\rho \cdot e = e$, then $\rho(b) \cdot e = \rho(b) \cdot e_\rho \cdot e = e_\rho \cdot b \cdot e = b \cdot e$ for $b \in B$. Consequently, $\sum_{j=1}^n \sigma(x_j e) \cdot y_j e = \delta_{1,\sigma} \cdot e$ for all $\sigma \in g(Be, Be)$; and $g(Be, Be)$ is a finite, strongly independent group of automorphisms of Be for $e \in T$. By Lemma 2.2, there exist a finite set S of pairwise orthogonal, central idempotents in A, such that $\sum_{e \in S} e = 1$; and, for each $e \in S$, a finite, strongly independent group G_e of automorphisms of Be, such that Ae is the subring of G_e-invariant elements of Be. Therefore Be is a Galois extension of Ae relative to G_e for each $e \in S$.

Conversely, suppose there exists a finite set S of pairwise orthogonal, central idempotents in A, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of Ae relative to a finite group G_e of automorphisms of Be for each $e \in S$. Since Be is a Galois extension of Ae, Be is a separable extension of Ae for $e \in S$. Therefore B is a separable extension of

A. Let G be the subgroup of the group of all automorphisms of B over A, which is generated by the G_e, $e \in S$. Clearly A is the subring of G-invariant elements of B. But G is the direct product of its subgroups G_e and G_e is a finite group for $e \in S$. Therefore G is finite.

DEFINITION 2.4. Let A be a subring of a ring B such that the centralizer of A in B is the center of B. Call B an outer semi-Galois extension of A if either statement of Theorem 2.3 is satisfied.

Suppose B is an outer semi-Galois extension of a subring A; and let S be a finite set of pairwise orthogonal, central idempotents in A, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of Ae relative to a finite group G_e of automorphisms of Be for each $e \in S$. Then for each $e \in S$, Be is a Frobenius extension of Ae and G_e freely generates the left Be-module $\mathrm{Hom}\,(Be_{Ae}, Be_{Ae})$. Therefore B is a Frobenius extension of A. Moreover, if G is the group of automorphisms of B which is generated by the G_e, $e \in S$, then G is finite and it is easily verified that G generates the left B-module $\mathrm{Hom}\,(B_A, B_A)$.

PROPOSITION 2.5. *Let B be an outer semi-Galois extension of a subring A. Any finite set of automorphisms of B over A generates a finite group of automorphisms of B.*

Proof. Let M be a finite set of automorphisms of B over A. First suppose B is a Galois extension of A relative to a finite group G of automorphisms of B. Then G freely generates the left B-module $\mathrm{Hom}\,(B_A, B_A)$; and any automorphism η of B over A has a unique representation as $\eta = \sum_{\sigma \in G} e_{\eta,\sigma} \cdot \sigma$, where $\{e_{\eta,\sigma} \mid \sigma \in G\}$ is a set of pairwise orthogonal, central idempotents in B such that $\sum_{\sigma \in G} e_{\eta,\sigma} = 1$, by Lemma 2.1. $\{\sigma(e_{\eta,\tau}) \mid \sigma, \tau \in G$ and either $\eta \in M$ or $\eta^{-1} \in M\}$ is a finite set of central idempotents in B, which generates a finite subalgebra E_0 of the Boolean algebra E of all central idempotents in B. Let H be the group of automorphisms of B generated by M. If $\theta \in H$, then it may be verified by straightforwad calculations that $e_{\theta,\sigma} \in E_0$ for $\sigma \in G$. Since E_0 is finite, H must be finite. Now suppose B is an outer semi-Galois extension of A; and let S be a finite set of pairwise orthogonal, central idempotents in A, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of Ae for each $e \in S$. But, for each $e \in S$, a finite set of automorphisms of Be over Ae is obtained by restricting the elements of M to Be, and it has now been established that this finite set of automorphisms of Be over Ae generates a finite group H_e of automorphisms of Be. Let H be the subgroup of the group of all automorphisms of B over A which is generated by the H_e, $e \in S$. Then $M \subseteqq H$, and H is a finite group since it is the direct product of its subgroups H_e, $e \in S$. Therefore the group of automorphisms of B generated by M must be finite.

Suppose B is a Galois extension of a subring A relative to a finite group G of automorphisms of B, and S is a finite set of pairwise orthogonal, central idempotents in B, such that $S \subseteqq A$ and $\sum_{e \in S} e = 1$. For $e \in S$, the canonical projection of the group of all automorphisms of B over A onto the group of automorphisms of Be over Ae determines a representation of G as a group of automorphisms of Be. Since A is the subring of G-invariant elements of B, Ae must be the subring of G-invariant elements of Be. Let n be a positive integer and x_j, y_j be elements of B for $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} \sigma(x_j) \cdot y_j = \delta_{1,\sigma}$ for all $\sigma \in G$. Then $x_j e$, $y_j e$ are elements of Be for $1 \leqq j \leqq n$, and $\sum_{j=1}^{n} \sigma(x_j e) \cdot y_j e = \delta_{1,\sigma} \cdot e$ for all $\sigma \in G$. Therefore only $1 \in G$ acts as the identity automorphism on Be, the representation of G as a group of automorphisms of Be is faithful, and Be is a Galois extension of Ae relative to G. It is evident from this observation, that to construct an example of an outer semi-Galois extension which is not a Galois extension one needs only to take the direct product of two outer Galois extensions which cannot have isomorphic Galois groups.

EXAMPLE 2.6. Let B be an outer Galois extension of a subring A relative to a nontrivial group G of automorphisms of B, and let $B \times B$ denote the direct product of B with itself. A faithful representation of G as a group of automorphisms of $B \times B$ is obtained by setting $\sigma(b, b') = (\sigma(b), \sigma(b'))$ for $\sigma \in G$ and $b, b' \in B$; and it is not difficult to verify that $B \times B$ is an outer Galois extension of its subring $A \times A$ relative to G. Since B is trivially an outer Galois extension of B, $B \times B$ is an outer semi-Galois extension of its subring $A \times B$. In particular, $B \times B$ is a Frobenius extension of $A \times B$. But $B \times B$ cannot be a Galois extension of $A \times B$.

3. Outer Galois theory.

LEMMA 3.1. *Let B be an outer Galois extension of a subring A_0 relative to a finite group G of automorphisms of B; and let A be a subring of B such that $A_0 \subseteqq A$ and B is a Frobenius extension of A.*

(1) *If A is Galois closed in B, then B is an outer semi-Galois extension of A.*

(2) *If B is a K-ring with respect to G, then B is a generalized Galois extension of A.*

Proof. Since the centralizer of A_0 in B is the center of B, the centralizer of A in B must be the center of B. Since B is a Galois extension of A_0, the left B-module $\mathrm{Hom}(B_{A_0}, B_{A_0})$ is freely generated by G. Finally, since B is a Frobenius extension of A, B is a finitely generated, projective right A-module and there is an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}(B_A, A_A)$. Let $\gamma \in \mathrm{Hom}(B_A, A_A)$ correspond to $1 \in B$ under an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}(B_A, A_A)$. Since $\gamma \in \mathrm{Hom}(B_{A_0}, B_{A_0})$, γ has a unique representation as $\gamma = \sum_{\sigma \in G} e_\sigma \cdot \sigma$ where $e_\sigma \in B$ for $\sigma \in G$. If $a \in A$; then $\sum_{\sigma \in G} a \cdot e_\sigma \cdot \sigma = a \cdot \gamma = \gamma \cdot a = \sum_{\sigma \in G} e_\sigma \cdot \sigma(a) \cdot \sigma$, since both correspond to a under the given (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}(B_A, A_A)$, and $a \cdot e_\sigma = e_\sigma \cdot \sigma(a)$ for $\sigma \in G$. Therefore e_σ must be an element of the centralizer of A_0 in B, which is the center of B, for $\sigma \in G$. Since there is a natural isomorphism of $B \otimes_A \mathrm{Hom}(B_A, A_A)$ onto $\mathrm{Hom}(B_A, B_A)$, there must exist a positive integer m and elements b_i, b'_i of B, $1 \leqq i \leqq m$, such that $\sum_{i=1}^m b_i \cdot \gamma \cdot b'_i = \sum_{\sigma \in G} \sum_{i=1}^m b_i \cdot e_\sigma \cdot \sigma(b'_i) \cdot \sigma$ is the identity automorphism of B. But then $\sum_{i=1}^m b_i \cdot e_\sigma \cdot \sigma(b'_i) = \delta_{1,\sigma}$ for $\sigma \in G$, and e_1 must be a unit in the center of B. Since an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}(B_A, A_A)$ is given also by the mapping $b \rightsquigarrow \gamma \cdot e_1^{-1} \cdot b$, $b \in B$; one may assume that an (A, B)-bimodule isomorphism of B onto $\mathrm{Hom}(B_A, A_A)$ has been chosen so that $e_1 = 1$.

Let n be a positive integer and x_j, y_j be elements of B, $1 \leqq j \leqq n$, such that $\sum_{j=1}^n \sigma(x_j) \cdot y_j = \delta_{1,\sigma}$ for all $\sigma \in G$. Then $e_\rho \cdot \rho = \sum_{j=1}^n \rho(x_j) \cdot \gamma \cdot y_j$ and $e_\rho \cdot \rho \in \mathrm{Hom}(B_A, B_A)$ for $\rho \in G$. Therefore $\sum_{\sigma \in G} e_\rho \cdot \rho(e_\sigma) \cdot \rho\sigma = e_\rho \cdot \rho \cdot \gamma = e_\rho \cdot \rho(1) \cdot \gamma = e_\rho \cdot \gamma = \sum_{\sigma \in G} e_\rho \cdot e_\sigma \cdot \sigma$, and $e_\rho \cdot \rho(e_\sigma) = e_\rho \cdot e_{\rho\sigma}$ for ρ, $\sigma \in G$. In particular, $e_\rho = e_\rho \cdot \rho(e_1) = e_\rho \cdot e_\rho$ for $\rho \in G$. Consequently, $\{\sigma(e_\tau) \mid \sigma, \tau \in G\}$ is a finite set of central idempotents in B, which generates a finite, G-stable subalgebra E_0 of the Boolean algebra E of all central idempotents in B. If T is the set of minimal elements of E_0; then T is a finite, G-stable set of pairwise orthogonal, central idempotents in B such that $\sum_{e \in T} e = 1$. Let $e \in T$, $b \in B$, and $\sigma \in G$. If $e_\sigma \cdot \sigma(e) = 0$, then $e_\sigma \cdot \sigma(be) = 0$; but if $e_\sigma \cdot \sigma(e) \neq 0$, then $e_\sigma \cdot \sigma(e) = \sigma(e)$ and $e_\sigma \cdot \sigma(be) = \sigma(be)$. Observe that for $e \in T$ and $\sigma, \tau \in G$ such that $e_\sigma \cdot \sigma(\tau(e)) = \sigma(\tau(e))$, $e_{\sigma\tau} \cdot \sigma\tau(e) = e_{\sigma\tau} \cdot e_\sigma \cdot \sigma\tau(e) = \sigma(e_\tau) \cdot e_\sigma \cdot \sigma\tau(e) = \sigma(e_\tau \cdot \tau(e))$. Therefore, if in addition $e_\tau \cdot \tau(e) = \tau(e)$, then $e_{\sigma\tau} \cdot \sigma\tau(e) = \sigma\tau(e)$. But letting $\tau = \sigma^{-1}$, one obtains from the preceding observation that, if $e_\sigma \cdot \sigma(\sigma^{-1}(e)) = \sigma(\sigma^{-1}(e))$, then $e_1 \cdot e = \sigma(e_{\sigma^{-1}} \cdot \sigma^{-1}(e))$ or $e_{\sigma^{-1}} \cdot \sigma^{-1}(e) = \sigma^{-1}(e)$ since $e_1 = 1$. With these facts it may be verified that a groupoid g of ring isomorphisms between elements of the set $\{Be \mid e \in T\}$ is obtained by letting $g(Be, Be')$ be the set of isomorphisms of Be onto Be' which are restrictions of elements σ of G satisfying $e_\sigma \cdot \sigma(e) = e'$ for $e, e' \in T$. Let $\bar{A}$ be the Galois closure of A in B. Clearly, $\bar{A} = \{b \in B \mid \gamma(xb) = \gamma(x) \cdot b$ for all $x \in B\}$. But $\gamma = \sum_{\sigma \in G} e_\sigma \cdot \sigma$ and $e_\sigma \cdot \sigma \in \mathrm{Hom}(B_A, B_A)$ for $\sigma \in G$. Therefore $\bar{A} = \{b \in B \mid e_\sigma \cdot \sigma(b) = e_\sigma \cdot b$ for $\sigma \in G\} = \{b \in B \mid \eta(be) = b \cdot e'$ for $\eta \in (Be, Be')$ and $e, e' \in T\}$.

Now let $e \in T$ and let H be the subgroup of automorphisms in G which restrict to elements of $g(Be, Be)$. Since G is finite, $g(Be, Be)$ is finite. Since $\sum_{j=1}^{n} \sigma(x_j e) \cdot y_j e = \delta_{1,\sigma} \cdot e$ for all $\sigma \in G$, $g(Be, Be)$ must be a strongly independent group of automorphisms of Be. Moreover, only $1 \in H$ restricts to the identity automorphism of Be. Therefore distinct elements of H restrict to distinct elements of $g(Be, Be)$. Suppose that B is a K-ring with respect to G. Then there exists $c \in B$ such that $\sum_{\sigma \in G} \sigma(c) = 1$. Let p be the index of H in G, let $\{\tau_k \mid 1 \leqq k \leqq p\}$ be a system of representatives of the left cosets of H in G, and let $c' = \sum_{k=1}^{p} \tau_k(c)$. Then $\sum_{\sigma \in H} \sigma(c') = 1$ and $\sum_{\eta \in g(Be,Be)} \eta(c'e) = e$. By Lemma (2.2) there exist a finite set S of pairwise orthogonal, central idempotents in $\bar{A}$, such that $\sum_{e \in S} e = 1$; and, for each $e \in S$, a group G_e of automorphisms of Be with the properties that Be is a Galois extension of $\bar{A}e$ relative to G_e, and Be is a K-ring with respect to G_e if B is a K-ring with respect to G. Therefore, if $A = \bar{A}$, then B is an outer semi-Galois extension of A. If B is a K-ring with respect to G, then Be is a generalized Galois extension of $\bar{A}e$ for each $e \in S$. But then B is a generalized Galois extension of $\bar{A}$ and $\mathscr{T}(B_{\bar{A}}) = \bar{A}$. Since $\mathrm{Hom}\,(B_A, A_A) = \mathrm{Hom}\,(B_{\bar{A}}, \bar{A}_{\bar{A}})$ by Proposition 1.1, $\mathscr{T}(B_{\bar{A}}) = \mathscr{T}(B_A) \subseteqq A \subseteqq \bar{A}$. Therefore $\mathscr{T}(B_A) = A$ and B is a generalized Galois extension of A.

THEOREM 3.2. *Let B be an outer semi-Galois extension of a subring A_0, and let A be a subring of B such that $A_0 \subseteqq A$. The following statements are equivalent*:

(1) *B is an outer semi-Galois extension of A.*

(2) *A is Galois closed in B and B is a Frobenius extension of A.*

(3) *A is the subring of invariant elements of B with respect to some finite group of automorphisms of B.*

Proof. Since B is an outer semi-Galois extension of A_0, B is a separable extension of A_0. Therefore B must be a separable extension of A, and the equivalence of statements 1 and 3 follows from Definition (2.4). The remarks following Definition (2.4) establish that statements 1 and 3 imply statement 2. But suppose A is Galois closed in B and B is a Frobenius extension of A; and let S be a finite set of pairwise orthogonal, central idempotents in A_0, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of $A_0 e$ for each $e \in S$. Then Be is an outer Galois extension of $A_0 e$, Ae is a Galois closed subring of Be such that $A_0 e \subseteqq Ae$, and Be is a Frobenius extension of Ae, for $e \in S$. By Lemma 3.1, Be is an outer semi-Galois extension of Ae for $e \in S$. It follows easily that B is an outer semi-Galois extension of A. Therefore statement 2 implies statement 1.

If, in addition to the hypotheses of Theorem 3.2, A_0 is a direct summand of the right A_0-module B; then Theorem 3.2 may be modified to read as follows:

THEOREM 3.3. *Let B be an outer semi-Galois extension of a subring A_0 such that A_0 is a direct summand of the right A_0-module B; and let A be a subring of B such that $A_0 \subseteqq A$. The following statements are equivalent*:

(1) *B is an outer semi-Galois extension of A such that A is a direct summand of the right A-module B.*

(2) *B is a Frobenius extension of A.*

(3) *A is the subring of invariant elements of B with respect to some finite group of automorphisms of B.*

Proof. Statement 1 implies statement 3 and statement 3 implies statement 2 by Theorem 3.2. Suppose B is a Frobenius extension of A; and let S be a finite set of pairwise orthogonal, central idempotents in A_0, such that $\sum_{e \in S} e = 1$ and Be is a Galois extension of A_0e relative to a finite group G_e of automorphisms of Be for each $e \in S$. Let $e \in S$. Then A_0e is a direct summand of the A_0e-module Be. Therefore Be is not only an outer Galois extension of A_0e, but Be is also a K-ring with respect to G_e. Moreover Ae is a subring of Be such that $A_0e \subseteqq Ae$ and Be is a Frobenius extension of Ae. By Lemma 3.1, Be is a generalized Galois extension of Ae. Therefore B is a generalized Galois extension of A. In particular, A is Galois closed in B and A is a direct summand of the right A-module B. It now follows from Theorem 3.2 that statement 2 implies statement 1.

Observe that in Theorem 3.3, the condition that A_0 (resp. A) be a direct summand of the right A_0(resp. A)-module B may be replaced by either of the equivalent conditions given in Lemmas 1.5 and 1.6. Also, in view of Proposition 2.5, the word "group" may be replaced by "set" in statement 3 of either Theorem 3.2 or 3.3.

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, *Algèbre commutative*, Hermann, Paris, 1961.

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

5. N. Jacobson, *Lectures in abstract algebra*, Vol. 3, *Theory of fields and Galois theory*, Van Nostrand, Princeton, N. J., 1964.

6. F. Kasch, *Projektive Frobenius-Erweiterung*, S.-B. Heidelberger Akad. Wiss. Math-Natur. Kl. 1960/1961, 87-109.

7. H. F. Kreimer, *A Galois theory for non-commutative rings,* Trans. Amer. Math. Soc. **127** (1967), 29-41.
8. Y. Miyashita, *Finite outer Galois theory of non-commutative rings,* J. Fac. Sci. Hokkaido Univ. Ser. I, **19** (1966), 114-134.
9. T. Nakayama, *On a generalized notion of Galois extensions of a ring,* Osaka J. Math. **15** (1963), 11-23.
10. O. E. Villamayor and D. Zelinsky, *Galois theory for rings with finitely many idempotents,* Nagoya Math. J. **27** (1966), 721-731.

Received September 16, 1968. The author gratefully acknowledges support in his research from the Florida State University Research Council and the National Science Foundation under grants GP-7098 and GP-8424.

FLORIDA STATE UNIVERSITY