

AUTOMORPHISMS OF COMMUTATIVE RINGS⁽¹⁾

BY

H. F. KREIMER

ABSTRACT. Let B be a commutative ring with 1, let G be a finite group of automorphisms of B , and let A be the subring of G -invariant elements of B . For any separable A -subalgebra A' of B , the following assertions are proved: (1) A' is a finitely generated, projective A -module; (2) for each prime ideal p of A , the rank of A'_p over A_p does not exceed the order of G ; (3) there is a finite group H of automorphisms of B such that A' is the subring of H -invariant elements of B . If, in addition, A' is G -stable, then every automorphism of A' over A is the restriction of an automorphism of B , and $\text{Hom}_A(A', A')$ is generated as a left A' -module by those automorphisms of A' which are the restrictions of elements of G .

Let E be any G -stable subalgebra of the Boolean algebra of all idempotent elements of B . The closure of G with respect to E is the set of all automorphisms ρ of B for which there exist a positive integer n and $e_i \in E$, $\sigma_i \in G$, such that $e_i \cdot \rho = e_i \cdot \sigma_i$ for $1 \leq i \leq n$ and $\bigcup_{i=1}^n e_i = 1$ in the Boolean algebra E .

PROPOSITION 1. *Let E be a G -stable subalgebra of the Boolean algebra of all idempotent elements of B , and let \bar{G} be the closure of G with respect to E .*

- (i) \bar{G} is a group of automorphisms of B over A , which contains G .
- (ii) \bar{G} is the set of all automorphisms ρ of B for which there exist a positive integer n , a G -stable set $\{e_1, \dots, e_n\}$ of n pairwise orthogonal elements of E , and $\sigma_i \in G$ for $1 \leq i \leq n$, such that $\rho = \sum_{i=1}^n e_i \cdot \sigma_i$.

PROOF. Clearly $G \subseteq \bar{G}$. Let ρ be an element of \bar{G} ; let n be a positive integer; and, for $1 \leq i \leq n$, let e_i be an element of E and σ_i be an element of G , such that $e_i \cdot \rho = e_i \cdot \sigma_i$ and $\bigcup_{i=1}^n e_i = 1$. If $a \in A$, then $e_i \cdot \rho(a) = e_i \cdot \sigma_i(a) = e_i \cdot a$ for $1 \leq i \leq n$; and, since $\bigcup_{i=1}^n e_i = 1$, it follows readily that ρ must be an automorphism of B over A . Also, for $1 \leq i \leq n$,

Received by the editors August 7, 1973.

AMS (MOS) subject classifications (1970). Primary 13B05, 13B10.

Key words and phrases. Automorphism, commutative ring, Galois extension.

(¹) The author gratefully acknowledges support in his research from the National Science Foundation under grant GP-19406.

Copyright © 1975, American Mathematical Society

$$\begin{aligned}
\rho^{-1}(e_i) &= \rho^{-1}(e_i \cdot \sigma_i \sigma_i^{-1}(e_i)) = \rho^{-1}(e_i \cdot \rho \sigma_i^{-1}(e_i)) = \rho^{-1}(e_i) \cdot \sigma_i^{-1}(e_i) \\
&= \sigma_i^{-1}(e_i) \cdot \rho^{-1}(e_i) = \sigma_i^{-1}(e_i \cdot \sigma_i \rho^{-1}(e_i)) \\
&= \sigma_i^{-1}(e_i \cdot \rho \rho^{-1}(e_i)) = \sigma_i^{-1}(e_i);
\end{aligned}$$

and $\bigcup_{i=1}^n \sigma_i^{-1}(e_i) = \rho^{-1}(\bigcup_{i=1}^n e_i) = 1$. From the equation $e_i \cdot \rho = e_i \cdot \sigma_i$, it follows that $\sigma_i^{-1}(e_i) \cdot \sigma_i^{-1} \rho = \sigma_i^{-1}(e_i) \cdot 1$, and $\sigma_i^{-1}(e_i) \cdot \sigma_i^{-1} = \sigma_i^{-1}(e_i) \cdot \rho^{-1}$ for $1 \leq i \leq n$. Therefore $\rho^{-1} \in \bar{G}$. Now let ρ' be an element of \bar{G} ; let n' be a positive integer; and, for $1 \leq j \leq n'$, let e'_j be an element of E and σ'_j be an element of G , such that $e'_j \cdot \rho' = e'_j \cdot \sigma'_j$ and $\bigcup_{j=1}^{n'} e'_j = 1$. Then

$$e_i \cdot \sigma_i(e'_j) \cdot \rho \rho' = e_i \cdot \sigma_i(e'_j) \cdot \sigma_i \rho' = e_i \cdot \sigma_i(e'_j) \cdot \sigma_i \sigma'_j$$

for $1 \leq i \leq n$ and $1 \leq j \leq n'$ and

$$\bigcup_{i=1}^n \bigcup_{j=1}^{n'} e_i \cdot \sigma_i(e'_j) = \bigcup_{i=1}^n \left(e_i \cap \sigma_i \left(\bigcup_{j=1}^{n'} e'_j \right) \right) = \bigcup_{i=1}^n e_i = 1.$$

Therefore $\rho \rho' \in \bar{G}$, and it has now been established that \bar{G} is a group of automorphisms of B over A . $\{\sigma(e_i) \mid \sigma \in G \text{ and } 1 \leq i \leq n\}$ is a finite subset of E , and it generates a finite, G -stable subalgebra of E . Letting f_1, \dots, f_m be the distinct minimal elements of this subalgebra, $\{f_1, \dots, f_m\}$ is a G -stable set of pairwise orthogonal elements of E such that $\sum_{j=1}^m f_j = 1$. Let j be any integer such that $1 \leq j \leq m$. Since $\bigcup_{i=1}^n e_i = 1$, there exists an integer i , $1 \leq i \leq n$, such that $f_j = f_j \cap e_i = f_j \cdot e_i$, and $f_j \cdot \rho = f_j \cdot e_i \rho = f_j \cdot e_i \cdot \sigma_i = f_j \cdot \sigma_i$. Hence, for $1 \leq j \leq n$, there exists $\tau_j \in G$ such that $f_j \cdot \rho = f_j \cdot \tau_j$; and $\rho = \sum_{j=1}^m f_j \cdot \rho = \sum_{j=1}^m f_j \cdot \tau_j$. Conversely, if ρ is an automorphism of B for which there exist pairwise orthogonal elements e_1, \dots, e_n of E and elements $\sigma_1, \dots, \sigma_n$ of G such that $\rho = \sum_{i=1}^n e_i \cdot \sigma_i$, then $e_i \rho = e_i \cdot \sigma_i$ for $1 \leq i \leq n$, $\bigcup_{i=1}^n e_i = \sum_{i=1}^n e_i = \rho(1) = 1$, and therefore $\rho \in \bar{G}$.

Notice that the closure of G as defined in [10, Definition 3.7], is just the closure of G with respect to the Boolean algebra of all idempotent elements of B ; and statement (ii) of Proposition 1 is a slight strengthening of Lemma 1.1 of [8]. Also, whenever e_1, \dots, e_n are pairwise orthogonal idempotent elements of B such that $\sum_{i=1}^n e_i = 1$, and $\sigma_i \in G$ for $1 \leq i \leq n$; then it is easily verified that the mapping $\eta = \sum_{i=1}^n e_i \cdot \sigma_i$ is a homomorphism of B into B .

PROPOSITION 2. *Let n be a positive integer, let $E = \{e_1, \dots, e_n\}$ be a G -stable set of n pairwise orthogonal idempotent elements of B such that $\sum_{i=1}^n e_i = 1$, and let $\sigma_i \in G$ for $1 \leq i \leq n$. $\eta = \sum_{i=1}^n e_i \cdot \sigma_i$ is an automorphism of B if, and only if, the mapping π of E into E , defined by the rule $\pi(e_i) = \sigma_i^{-1}(e_i)$ for $1 \leq i \leq n$, is a permutation of E . Moreover, if η is an*

automorphism of B , then $\eta^{-1} = \sum_{i=1}^n \pi(e_i) \cdot \sigma_i^{-1}$.

PROOF. Observe that E generates a finite, G -stable Boolean algebra of idempotent elements of B , and η induces a homomorphism of this algebra into itself. Now suppose that η is an automorphism of B . Then η and η^{-1} induce automorphisms of the finite Boolean algebra generated by E ; and, therefore, η and η^{-1} must induce permutations of E . From the equation $e_i = \eta\eta^{-1}(e_i) = \sum_{j=1}^n e_j \cdot \sigma_j \eta^{-1}(e_i)$, it follows that $e_i = \sigma_i \eta^{-1}(e_i)$ for $1 \leq i \leq n$. Therefore $\sigma_i^{-1}(e_i) = \eta^{-1}(e_i)$ for $1 \leq i \leq n$, and π is the permutation of E induced by η^{-1} . Conversely, suppose that π is a permutation of E ; and let $\theta = \sum_{i=1}^n \pi(e_i) \cdot \sigma_i^{-1}$. Then

$$\begin{aligned} \theta\eta &= \sum_{i,j=1}^n \pi(e_i) \cdot \sigma_i^{-1}(e_j) \cdot \sigma_i^{-1}\sigma_j \\ &= \sum_{i,j=1}^n \sigma_i^{-1}(e_i \cdot e_j) \cdot \sigma_i^{-1}\sigma_j = \sum_{i=1}^n \pi(e_i) \cdot 1 = 1, \end{aligned}$$

while

$$\begin{aligned} \eta\theta &= \sum_{i,j=1}^n e_i \cdot \sigma_i \pi_j(e_j) \cdot \sigma_i \sigma_j^{-1} = \sum_{i,j=1}^n \sigma_i(\pi(e_i) \cdot \pi(e_j)) \cdot \sigma_i \sigma_j^{-1} \\ &= \sum_{i=1}^n \sigma_i(\pi(e_i)) \cdot \sigma_i \sigma_i^{-1} = \sum_{i=1}^n e_i \cdot 1 = 1. \end{aligned}$$

Therefore η is an automorphism of B and $\theta = \eta^{-1}$.

COROLLARY. Let B_1 and B_2 be commutative rings; let H be a finite group, which is represented as a group of automorphisms of B_i by a homomorphism ϕ_i of H into the group of all automorphisms of B_i for $i = 1, 2$; and let ω be a homomorphism of B_1 into B_2 , such that $\omega(\phi_1(\sigma)(b)) = \phi_2(\sigma)(\omega(b))$ for $\sigma \in H$ and $b \in B_1$. Suppose that n is a positive integer; $E = \{e_1, \dots, e_n\}$ is a $\phi_1(H)$ -stable set of n pairwise orthogonal idempotent elements of B_1 , such that $\sum_{i=1}^n e_i = 1$; and $\sigma_i \in H$ for $1 \leq i \leq n$.

(i) If $\sum_{i=1}^n e_i \cdot \phi_1(\sigma_i)$ is an automorphism of B_1 , then $\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ is an automorphism of B_2 .

(ii) If $\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ is an automorphism of B_2 and with at most one exception $\omega(e_i) \neq 0$ for $1 \leq i \leq n$, then $\sum_{i=1}^n e_i \cdot \phi_1(\sigma_i)$ is an automorphism of B_1 .

PROOF. $\omega(E)$ is a finite set of idempotent elements of B_2 and $\sum_{i=1}^n \omega(e_i) = \omega(\sum_{i=1}^n e_i) = \omega(1) = 1$. Clearly the zero terms of $\sum_{i=1}^n \omega(e_i)$ and

$\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ may be disregarded and it is only necessary to consider the subset E_2 of nonzero elements of $\omega(E)$. Since E is $\phi_1(H)$ -stable and $\phi_2(\sigma)(\omega(e)) = \omega(\phi_1(\sigma)(e))$ for $\sigma \in H$ and $e \in E$, $\omega(E)$ and E_2 must be $\phi_2(H)$ -stable sets. Therefore, a mapping π_2 of E_2 into E_2 is obtained by restricting the correspondence $\omega(e_i) \rightsquigarrow \phi_2(\sigma_i^{-1})(\omega(e_i))$, $1 \leq i \leq n$, to the elements of E_2 . $\omega(e_i) \cdot \omega(e_j) = \omega(e_i e_j) = \omega(0) = 0$ for $i \neq j$ and $1 \leq i, j \leq n$. In particular, if $\omega(e_i) = \omega(e_j)$ for integers i and j such that $1 \leq i, j \leq n$ and $i \neq j$, then $\omega(e_i) = \omega(e_j) = \omega(e_i) \cdot \omega(e_j) = 0$. Therefore, the elements of E_2 are pairwise orthogonal; and it is easily deduced from Proposition 2 that $\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ is an automorphism of B_2 if, and only if, π_2 is a permutation of E_2 .

Now let $E_1 = \{e \in E \mid \omega(e) \neq 0\}$. Since $\phi_2(\sigma)(\omega(e)) = \omega(\phi_1(\sigma)(e))$ for $\sigma \in H$ and $e \in E$, E_1 and the complement of E_1 in E are $\phi_1(H)$ -stable subsets of E . Letting π denote the mapping of E into E defined by the rule $\pi(e_i) = \phi_1(\sigma_i^{-1})(e_i)$ for $1 \leq i \leq n$; a mapping π_1 of E_1 onto E_1 is obtained by restricting π to E_1 . The restriction of ω to E_1 is a bijection of E_1 onto E_2 . Since $\omega(\phi_1(\sigma_i^{-1})(e_i)) = \phi_2(\sigma_i^{-1})(\omega(e_i))$ for $1 \leq i \leq n$, $\omega\pi_1(e) = \pi_2\omega(e)$ for $e \in E_1$. Consequently, π_2 is a permutation of E_2 if and only if π_1 is a permutation of E_1 . Furthermore, π is a permutation of E if and only if $\sum_{i=1}^n e_i \cdot \phi_1(\sigma_i)$ is an automorphism of B_1 by Proposition 2. But if π is a permutation of E , then π_1 will be a permutation of E_1 . Thus, if $\sum_{i=1}^n e_i \cdot \phi_1(\sigma_i)$ is an automorphism of B_1 , then $\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ is an automorphism of B_2 . To prove statement (ii) of the Corollary, assume that, with at most one exception, $\omega(e_i) \neq 0$ for $1 \leq i \leq n$. Then E_1 contains every element of E except possibly one; so, if π_1 is a permutation of E_1 , then π must be a permutation of E . In this case, if $\sum_{i=1}^n \omega(e_i) \cdot \phi_2(\sigma_i)$ is an automorphism of B_2 , then $\sum_{i=1}^n e_i \cdot \phi_1(\sigma_i)$ is an automorphism of B_1 .

In agreement with [5, Definition 1.4], call B a Galois extension of A with Galois group G if there exist a positive integer n and elements x_i, y_i of B , $1 \leq i \leq n$, such that $\sum_{i=1}^n x_i \sigma(y_i) = \delta_{1, \sigma}$ for all σ in G .

PROPOSITION 3. *Let B' be a separable A -subalgebra of B , which is stable under G ; and let \bar{G} be the closure of G with respect to the Boolean algebra of all idempotent elements of B' . Then:*

(i) *There exists a finite set F of pairwise orthogonal idempotent elements of A , such that $\sum_{e \in F} e = 1$; and, for each $e \in F$, there exists a subgroup $G(e)$ of \bar{G} such that $(G(e) : 1) \leq (G : 1)$ and $B'e$ is a Galois extension of Ae with respect to the group of automorphisms of $B'e$ induced by elements of $G(e)$.*

(ii) $\text{Hom}_A(B', B')$ is generated as a left B' -module by those automorphisms of B' which are the restrictions of elements of G .

(iii) Every automorphism of B' over A is the restriction to B' of an element of \bar{G} .

PROOF. Let $x_1, \dots, x_n, y_1, \dots, y_n$ be elements of B' such that $\sum_{i=1}^n x_i y_i = 1$ and $\sum_{i=1}^n b x_i \otimes y_i = \sum_{i=1}^n x_i \otimes y_i b$ in $B' \otimes_A B'$ for all $b \in B'$. Setting $e_\sigma = \sum_{i=1}^n x_i \cdot \sigma(y_i)$, $e_\sigma \in B'$ for $\sigma \in G$. Moreover, $\sum_{i=1}^n b x_i \otimes \sigma(y_i) = \sum_{i=1}^n x_i \otimes \sigma(y_i b)$ in $B \otimes_A B$, and so $b \cdot e_\sigma = e_\sigma \cdot \sigma(b)$ for $b \in B'$ and $\sigma \in G$. Therefore,

$$e_\sigma^2 = \sum_{i=1}^n e_\sigma \cdot x_i \cdot \sigma(y_i) = \sum_{i=1}^n x_i \cdot e_\sigma \cdot \sigma(y_i) = \sum_{i=1}^n x_i \cdot y_i \cdot e_\sigma = e_\sigma,$$

for $\sigma \in G$; and $\{\sigma(e_\tau) | \sigma, \tau \in G\}$ is a finite, G -stable set of idempotent elements of B' . Clearly the set $\{\sigma(e_\tau) | \sigma, \tau \in G\}$ generates a finite, G -stable subalgebra of the Boolean algebra of all idempotent elements of B' ; let E be the set of minimal elements of this finite subalgebra. Then E is a finite, G -stable set of pairwise orthogonal idempotent elements of B' such that $\sum_{e \in E} e = 1$. A groupoid g of ring isomorphisms between elements of the set $\{Be | e \in E\}$ is obtained by letting $g(Be, Be')$ be the set of isomorphisms of Be onto Be' which are restrictions of elements of G for $e, e' \in E$. Since A is the subring of G -invariant elements of B , $A = \{b \in B | \sigma(be) = be' \text{ for } \sigma \in g(Be, Be')\}$. In Lemma 2.2 of [6], there is given a construction of a finite set F of pairwise orthogonal idempotent elements of A , such that $\sum_{e \in F} e = 1$; and, for each $e \in F$, a group $G(e)$ of automorphisms of Be for which Ae is the subring of invariant elements. Each element of $G(e)$ is induced by an automorphism of B which acts as the identity map on $B(1 - e)$, and thus $G(e)$ may be identified with a group of automorphisms of B . Although it is not explicitly stated there, it is obvious from the proof of [6, Lemma 2.2] that $G(e)$ is a subgroup of \bar{G} and $(G(e) : 1) \leq (G : 1)$. For each $e \in F$, let $H(e)$ be the group of automorphisms of $B'e$ induced by elements of $G(e)$. By careful analogy with the construction of the groups $G(e)$, the groups $H(e)$ may be constructed from the groupoid h of ring isomorphisms between elements of the set $\{B'e | e \in E\}$, obtained by letting $h(B'e, B'e')$ be the set of isomorphisms of $B'e$ onto $B'e'$ which are restrictions of elements of G for $e, e' \in E$, so as to satisfy Lemma 2.2 of [6]. For $e \in E$ and $\sigma \in G$, $\sum_{i=1}^n e x_i \cdot \sigma(y_i) = e \cdot e_\sigma$ and either $e \cdot e_\sigma = 0$ or $e \cdot e_\sigma = e$. But if $e \cdot e_\sigma = e$, then $e \cdot \sigma(b) = e \cdot e_\sigma \cdot \sigma(b) = e \cdot b \cdot e_\sigma = e \cdot b$ for $b \in B'$. Therefore $\sum_{i=1}^n (x_i e) \cdot \rho(y_i e) = \delta_{1, \rho} \cdot e$ for all $\rho \in h(B'e, B'e')$ and $e \in E$, and it follows from [6, Proposition 1.7 and Lemma

2.2] that $B'e$ is a Galois extension of Ae with Galois group $H(e)$ for every $e \in F$.

$\text{Hom}_A(B', B') = \sum_{e \in F} e \cdot \text{Hom}_A(B', B')$; and, for each $e \in F$, there is a natural isomorphism of $e \cdot \text{Hom}_A(B', B')$ onto $\text{Hom}_{Ae}(B'e, B'e)$. Since $B'e$ is a Galois extension of Ae with respect to a group of automorphisms of $B'e$ which are induced by elements of a subgroup $G(e)$ of \bar{G} , $\text{Hom}_{Ae}(B'e, B'e)$ is generated as a left $B'e$ -module by these induced automorphisms for $e \in F$. It follows easily from part (ii) of Proposition 1 that $\text{Hom}_A(B', B')$ is generated as a left B' -module by those automorphisms of B' which are the restrictions of elements of G . Finally, let ψ be an automorphism of B' over A . $\psi = \sum_{e \in F} e \cdot \psi$, and $e \cdot \psi$ induces an automorphism of $B'e$ over Ae for each $e \in F$. But for each $e \in F$, there exist pairwise orthogonal idempotent elements f_1, \dots, f_l of $B'e$ and elements τ_1, \dots, τ_l of $G(e)$, such that $e \cdot \psi$ and $\sum_{i=1}^l f_i \cdot \tau_i$ induce the same automorphism on $B'e$ by [5, Corollary 3.3]. From the construction given for the group $G(e)$, $e \in F$, it is easily deduced that ψ lies in the closure, with respect to the Boolean algebra of all idempotent elements of B' , of the group of automorphisms of B' which are the restrictions of elements of G . This fact is also a consequence of Lemma 3.14 of [10]. Therefore, there exist a G -stable set $\{f_1, \dots, f_h\}$ of h pairwise orthogonal idempotent elements of B' and $\sigma_i \in G$ for $1 \leq i \leq h$, such that ψ is the restriction of $\sum_{i=1}^h f_i \cdot \sigma_i$ to B' by part (ii) of Proposition 1. $\sum_{i=1}^h f_i = \psi(1) = 1$; and taking $B_1 = B'$ and $B_2 = B$, and letting ω be the inclusion map of B' into B , the Corollary to Proposition 2 may be applied to conclude that $\sum_{i=1}^h f_i \cdot \sigma_i$ is an automorphism of B . Clearly $\sum_{i=1}^h f_i \cdot \sigma_i$ is an element of \bar{G} .

Let X be a finitely generated, projective module over a commutative ring A , let p be a prime ideal of A , and recall that X_p is a free A_p -module of finite rank [3, Chapter 2, §5, Theorem 1]. The rank of the free A_p -module X_p is called the rank of X at p and it will be denoted simply by $\text{rank}(X_p)$.

LEMMA 1. *Let B' be any commutative A -algebra which is a finitely generated, projective A -module. If A' is a separable A -subalgebra of B' , then:*

- (i) B' is a finitely generated, projective A' -module.
- (ii) A' is an A' -module direct summand of B' .
- (iii) A' and B'/A' are finitely generated, projective A -modules.
- (iv) $\text{rank}(A'_p) + \text{rank}((B'/A')_p) = \text{rank}(B'_p)$ for every prime ideal p of A .

PROOF. Let A' be a separable A -subalgebra of B' . Since B' is a finitely generated A -module, certainly B' is a finitely generated A' -module. Statement (i) is a consequence of the well-known fact that any A' -module which is projective as an A -module is also projective as an A' -module. Indeed, A' is

a module of projective dimension zero over $A' \otimes_A A'$ by [4, Chapter IX, Proposition 7.7]; and, for any A' -module X which is projective as an A -module, it follows from [4, Chapter IX, Proposition 2.3] that $A' \otimes_A X$ is a projective $A' \otimes_A A$ -module. But $A' \otimes_A X$ is naturally isomorphic to X , and $A' \otimes_A A$ is naturally isomorphic to A' . B' is a finitely generated, projective left $\text{Hom}_{A'}(B', B')$ -module by [1, Proposition A.3]; and A' is an A' -module direct summand of B' according to [9, Proposition 1]. In particular, A' is an A -module direct summand of B' ; and, therefore, A' and B'/A' are finitely generated, projective A -modules. Moreover, for any prime ideal p of A , B'_p is isomorphic as an A_p -module to the direct sum of A'_p and $(B'/A')_p$; and, therefore, $\text{rank}(B'_p) = \text{rank}(A'_p) + \text{rank}((B'/A')_p)$.

If B' is a G -stable subring of B , then G is canonically represented as a group of automorphisms of B' by restricting each element of G to B' . Moreover, if K is the kernel of this representation, then G/K may be identified with a group of automorphisms of B' by this representation, and this identification will be made whenever it is convenient.

LEMMA 2. *Let B' be an A -subalgebra of B which is stable under G , let K be the kernel of the canonical representation of G as a group of automorphisms of B' , and let \bar{G} be the closure of G with respect to the Boolean algebra of all idempotent elements of B' . Assume that B' is a Galois extension of A with Galois group G/K , and let A' be a separable A -subalgebra of B' . Then:*

- (i) A' is a finitely generated, projective A -module;
- (ii) $\text{rank}(A'_p) \leq (G : K)$ for every prime ideal p of A ;
- (iii) there exists a finite subgroup H of \bar{G} such that A' is the subring of H -invariant elements of B .

PROOF. Let p be a prime ideal of A . Since B' is a Galois extension of A with Galois group G/K , B'_p is a finitely generated, projective A -module. By Lemma 1, A' is a finitely generated, projective A -module and $\text{rank}(A'_p) \leq \text{rank}(B'_p)$. But $\text{rank}(B'_p)$ equals the order of G/K by [5, Lemma 4.1]; and therefore $\text{rank}(A'_p) \leq (G : K)$. Also there exist a positive integer n and elements x_p, y_i of B' , $1 \leq i \leq n$, such that $\sum_{i=1}^n x_i \cdot \phi(y_i) = \delta_{1, \phi}$ for all $\phi \in G/K$. Since K is a normal subgroup of G , B^K is a G -stable subring of B . Clearly $B' \subseteq B^K$ and K is the kernel of the canonical representation of G as a group of automorphisms of B^K . Thus G/K is faithfully represented as a group of automorphisms of B^K , and B^K must be a Galois extension of A with Galois group G/K . But then the inclusion map of B' into B^K is an isomorphism by [5, Theorem 3.4]; and therefore $B' = B^K$.

B' is a separable A -algebra by [5, Theorem 1.3], and there exists a finite group \bar{H} of automorphisms of B' such that $A' = (B')^{\bar{H}}$ by [7, Lemma 1.5]. Each element ψ of \bar{H} is uniquely expressible as $\psi = \sum_{\phi \in G/K} e_{\psi, \phi} \cdot \phi$, where $\{e_{\psi, \phi} | \phi \in G/K\}$ is a set of pairwise orthogonal idempotent elements of B' , according to [5, Corollary 3.3]. The set $\{\sigma(e_{\psi, \phi}) | \sigma \in G, \psi \in \bar{H}, \text{ and } \phi \in G/K\}$ is finite, and it generates a finite, G -stable subalgebra of the Boolean algebra of all idempotent elements of B' . Letting e_1, \dots, e_m be the minimal elements of this finite subalgebra, $\{e_1, \dots, e_m\}$ is a G -stable set of pairwise orthogonal idempotent elements of B' such that $\sum_{i=1}^m e_i = 1$. It is easily verified that $S = \{\sum_{i=1}^m e_i \cdot \sigma_i | \sigma_i \in G \text{ for } 1 \leq i \leq m\}$ is a finite semigroup of homomorphisms of B into B , and every element of \bar{H} is the restriction to B' of an element of S . Let H be the subsemigroup of those elements of S , the restrictions of which are elements of \bar{H} . The Corollary to Proposition 2 may be applied to the rings B' and B to show that every element of H is an automorphism of B ; and Proposition 2 may be used to show that, whenever $\eta \in H$, $\eta^{-1} \in H$. Thus, it is apparent that H is a finite subgroup of \bar{G} , $K \subseteq H$, and $\bar{H} = H/K$. Therefore $A' = (B')^{\bar{H}} = (B^K)^{H/K} = B^H$.

THEOREM. *Let A' be a separable A -subalgebra of B , let $B' = \Pi_{\sigma \in G} \sigma(A')$, and let \bar{G} be the closure of G with respect to the Boolean algebra of all idempotent elements of B' .*

- (i) A' is a finitely generated, projective A -module.
- (ii) $\text{rank}(A'_p) \leq (G : 1)$ for every prime ideal p of A .
- (iii) There exists a finite subgroup H of \bar{G} such that A' is the subring of H -invariant elements of B .

PROOF. Since A' is a separable A -subalgebra of B , $\sigma(A')$ is a separable A -subalgebra of B for $\sigma \in G$; and B' is a homomorphic image of the tensor product of the $\sigma(A')$, so B' is a G -stable subalgebra of B which is separable by [2, Proposition 1.4 and Proposition 1.5]. By Proposition 3, there exists a finite set F of pairwise orthogonal idempotent elements of A , such that $\sum_{e \in F} e = 1$; and, for each $e \in F$, there exists a subgroup $G(e)$ of \bar{G} such that $(G(e) : 1) \leq (G : 1)$ and $B'e$ is a Galois extension of Ae with respect to the group of automorphisms of $B'e$ induced by elements of $G(e)$. Since $A'e$ is a homomorphic image of A' , $A'e$ is a separable Ae -subalgebra of Be for $e \in G$ [2, Proposition 1.4]. Let $\overline{G(e)}$ be the closure, with respect to the Boolean algebra of all idempotent elements of $B'e$, of the group of automorphisms of Be induced by elements of $G(e)$. It follows from Lemma 2 that, for each $e \in F$, $A'e$ is a finitely generated, projective Ae -module; $\text{rank}((A'e)_q) \leq (G : 1)$ for every prime ideal q of Ae ; and there exists a finite subgroup $H(e)$ of $\overline{G(e)}$ such

that $A'e$ is the subring of $H(e)$ -invariant elements of Be . Since $A = \sum_{e \in F} Ae$, $A' = \sum_{e \in F} A'e$, and $A'e$ is a finitely generated, projective Ae -module for each $e \in F$, A' must be a finitely generated, projective A -module. Let p be a prime ideal of A , and let e be an element of F such that $e \notin p$. $A'e$ is naturally isomorphic to the ring of fractions $e^{-1} \cdot A'$, Ae is naturally isomorphic to the ring of fractions $e^{-1} \cdot A$, pe is a prime ideal of Ae , and the complement of p in A is mapped onto the complement of pe in Ae by the canonical homomorphism of A onto Ae . Therefore, A_p is isomorphic to $(Ae)_{pe}$, and A'_p and $(A'e)_{pe}$ are isomorphic A_p -modules by [3, Chapter II, §2, Proposition 7]. Consequently, $\text{rank}(A'_p) = \text{rank}((A'e)_{pe}) \leq (G : 1)$. Finally, let H be the direct product of the groups $H(e)$, $e \in F$. H is a finite group, and the decomposition $B = \sum_{e \in F} Be$ may be used to define an isomorphism by which H may be identified with a group of automorphisms of B . Since $G(e)$ is a subgroup of \bar{G} , it follows readily that $H(e)$ is a subgroup of the closure, with respect to the Boolean algebra of all idempotent elements of $B'e$, of the group of automorphisms of Be induced by elements of G . Therefore, H is a subgroup of \bar{G} , and $A' = \sum_{e \in F} (Be)^{H(e)} = B^H$.

REFERENCES

1. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24. MR 22 #8034.
2. ———, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409. MR 22 #12130.
3. N. Bourbaki, *Éléments de mathématique*. Fasc. XXVII. *Algèbre commutative*, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961. MR 36 #146.
4. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956. MR 17, 1040.
5. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 15–33. MR 33 #4118.
6. H. F. Kreimer, *A note on the outer Galois theory of rings*, Pacific J. Math. **31** (1969), 417–432. MR 40 #5669.
7. ———, *Outer Galois theory for separable algebras*, Pacific J. Math. **32** (1970), 147–155. MR 42 #6045.
8. A. R. Magid, *Locally Galois algebras*, Pacific J. Math. **33** (1970), 707–724. MR 41 #8405.
9. T. Nakayama, *On a generalized notion of Galois extensions of a ring*, Osaka Math. J. **15** (1963), 11–23. MR 27 #1478.
10. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83–98. MR 39 #5555.

DEPARTMENT OF MATHEMATICS, FLORIDA STATE UNIVERSITY, TALLAHASSEE, FLORIDA 32306