A GALOIS THEORY FOR NONCOMMUTATIVE RINGS(1)

BY
H. F. KREIMER

Introduction. In 1944, Jacobson [4] developed a Galois theory for nonnormal and nonseparable fields; and, in 1949, Hochschild [3] used the techniques of Jacobson to present a Galois theory for division rings. These same techniques will be used in this paper to present a Galois theory for rings with identity element. The theory presented here is the analogue of the outer Galois theory for division rings and it extends the Galois theory of commutative rings developed by Chase, Harrison, and Rosenberg [1].

1. **Generalized Galois theory.** For any ring A with identity element, let 1 denote the identity element of A; and for $a \in A$, let a_L denote the mapping $x \to ax$ of A into itself and let a_R denote the mapping $x \to xa$ of A into itself. In subsequent use, ring will mean ring with identity element and subring of a ring will mean subring which contains the identity element of the ring. A homomorphism ϕ of a ring A into a ring B is an additive map of A into B such that $a_R \circ \phi = \phi \circ (a\phi)_R$, $a \in A$, where $a\phi$ denotes the image of a under ϕ and "$\circ$" denotes composition of maps. Generalized Galois theory involves a formal study of the ways in which additive maps between rings may relate to the multiplicative ring structure.

Let Z denote the ring of integers and let $\mathrm{Hom}_Z(A, B)$ denote the abelian group of additive maps of a ring A into a ring B. $\mathrm{Hom}_Z(A, B)$ is an A-B bimodule and a B-A bimodule according to the rules $a\phi b = a_R \circ \phi \circ b_R$ and $b\phi a = a_L \circ \phi \circ b_L$ for $a \in A$, $b \in B$, $\phi \in \mathrm{Hom}_Z(A, B)$. Let K_0 be a free unital A-B bimodule on one generator g_0. If $\phi \in \mathrm{Hom}_Z(A, B)$, there is a unique A-B bimodule homomorphism f_ϕ of K_0 into $\mathrm{Hom}_Z(A, B)$ mapping g_0 onto ϕ. The kernel J_ϕ of f_ϕ is an A-B submodule of K_0 and gives the relations between ϕ and the multiplicative ring structures of A and B.

(1.1) DEFINITION. Let $\mathscr{J}$ be the lattice of A-B submodules of K_0 and let $\mathscr{R}$ be the lattice of B-A submodules of $\mathrm{Hom}_Z(A, B)$. For $J \in \mathscr{J}$, let $R(J) = \{\phi \in \mathrm{Hom}_Z(A, B) \mid J \subseteq J_\phi\}$; and, for $R \in \mathscr{R}$, let $J(R) = \bigcap_{\phi \in R} J_\phi$.

For $J \in \mathscr{J}$, $R(J)$ is a B-A submodule of $\mathrm{Hom}_Z(A, B)$; and, for $R \in \mathscr{R}$, $J(R)$ is an A-B submodule of K_0. The mappings $J \to R(J)$ and $R \to J(R)$ constitute a Galois connection between the lattices $\mathscr{J}$ and $\mathscr{R}$, in the terminology of Ore [6]. For $J \in \mathscr{J}$, $\bar{J} = J(R(J))$ is the (Galois) closure of J and J is (Galois) closed if it

Presented to the Society, August 30, 1966; received by the editors January 21, 1966 and, in revised form, April 15, 1966.

(1) The author gratefully acknowledges support in his research from the National Science Foundation under grants GP-3800 and GP-3895.

is equal to its closure. Similarly, for $R \in \mathscr{R}$, $\bar{R} = R(J(R))$ is the (Galois) closure of R and R is (Galois) closed if it is equal to its closure. The mappings $J \to R(J)$, $R \to J(R)$ are anti-isomorphisms between the lattice of closed elements of $\mathscr{J}$ and the lattice of closed elements of $\mathscr{R}$, with one map being the inverse of the other. Note that the lattice of closed elements of $\mathscr{J}$ (resp. $\mathscr{R}$) is not a sublattice of $\mathscr{J}$ (resp. $\mathscr{R}$). Indeed, in the lattice $\mathscr{J}$ (resp. $\mathscr{R}$), the intersection of a family of closed elements is again closed, but the union of this family need not be closed and it is the closure of this union which is the least upper bound for this family in the lattice of closed elements of $\mathscr{J}$ (resp. $\mathscr{R}$).

To each $\phi \in \mathrm{Hom}_Z(A, B)$ corresponds the mapping $k \to 1(kf_\phi)$, $k \in K_0$; and this correspondence is a B-A bimodule isomorphism of $\mathrm{Hom}_Z(A, B)$ onto $\mathrm{Hom}_B(K_0, B)$. By this isomorphism, identify $\mathrm{Hom}_Z(A, B)$ with $\mathrm{Hom}_B(K_0, B)$, which is the dual of the right B-module K_0. $1(kf_{\phi a}) = 1(a_L \circ (kf_\phi)) = a(kf_\phi) = 1(a_R \circ (kf_\phi)) = 1((ak)f_\phi)$, for $a \in A$, $k \in K_0$, and $\phi \in \mathrm{Hom}_Z(A, B)$. Therefore, if $J \in \mathscr{J}$, $J^\perp = \{\phi \in \mathrm{Hom}_Z(A, B) \mid 1(kf_\phi) = 0,\ k \in J\} = \{\phi \in \mathrm{Hom}_Z(A, B) \mid kf_\phi = 0,\ k \in J\} = \{\phi \in \mathrm{Hom}_Z(A, B) \mid J \subseteq J_\phi\} = R(J)$; and, if $R \in \mathscr{R}$, $R^\perp = \{k \in K_0 \mid 1(kf_\phi) = 0,\ \phi \in R\} = \{k \in K_0 \mid kf_\phi = 0,\ \phi \in R\} = \bigcap_{\phi \in R} J_\phi = J(R)$. For $J \in \mathscr{J}$, $\bar{J}/J = J^{\perp\perp}/J$ is the kernel of the natural right B-module homomorphism h of K_0/J into $\mathrm{Hom}_B(J^\perp, B) = \mathrm{Hom}_B(R(J), B)$. h is an A-B bimodule homomorphism, and J is closed if and only if h is a monomorphism. If B is a semisimple Artinian ring, then K_0/J is a projective right B-module, h is a monomorphism, and J is closed for any $J \in \mathscr{J}$. Let $\mathscr{K}$ be the set of cyclic A-B bimodules K_0/J, $J \in \mathscr{J}$, and make $\mathscr{K}$ into a lattice anti-isomorphic to $\mathscr{J}$ under the correspondence $J \leftrightarrow K_0/J$. If K is a cyclic, unital A-B bimodule with generator g, there is an A-B bimodule isomorphism of K_0/J onto K which maps $g_0 + J$ onto g for a unique $J \in \mathscr{J}$. Thus $\mathscr{K}$ may be regarded as a lattice of isomorphism types of cyclic, unital A-B bimodules. $g_0 + J$ will be called the canonical generator of K_0/J. For K, $K' \in \mathscr{K}$, $K \leqq K'$ if and only if there is an A-B bimodule homomorphism of K' onto K which maps the canonical generator of K' onto the canonical generator of K. It is the pair of lattices $\mathscr{K}$ and $\mathscr{R}$ which Hochschild considers in [3]. For $J \in \mathscr{J}$, the natural left B-module isomorphism of $R(J) = J^\perp$ onto $\mathrm{Hom}_B(K_0/J, B)$ is a B-A bimodule isomorphism; and $\mathrm{Hom}_B(K_0/J, B)$ is the relations space of the cyclic A-B bimodule K_0/J, as defined by Hochschild. For a division ring B, Dieudonné [2] characterizes the Galois closed elements of $\mathscr{R}$ as those B-A submodules of $\mathrm{Hom}_Z(A, B)$ which are closed and linearly compact with respect to the finite topology on $\mathrm{Hom}_Z(A, B)$.

(1.2) PROPOSITION. *If ϕ is a homomorphism of ring A into ring B, then J_ϕ is a closed element of $\mathscr{J}$, $R(J_\phi) = \{\phi \circ b_L \mid b \in B\}$, and there is a right B-module isomorphism of K_0/J_ϕ onto $(1\phi) \cdot B$ which maps $g_0 + J$ onto 1ϕ.*

Proof. For any $\phi \in \mathrm{Hom}_Z(A, B)$, $J_\phi \subseteq \bar{J}_\phi = \bigcap_{\psi \in R(J_\phi)} J_\psi$. Since $\phi \in R(J_\phi)$, $\bar{J}_\phi = J_\phi$ and J_ϕ is a closed element of $\mathscr{J}$. Let ϕ be a ring homomorphism of A into B. For $a \in A$ and $\psi \in R(J_\phi)$, $ag_0 - g_0(a\phi) \in J_\phi$ and $a\psi = 1(a_R \circ \psi) = 1(\psi \circ (a\phi)_R) = (1\psi)(a\phi)$

$=a(\phi \circ (1\psi)_L)$. Therefore $R(J_\phi)=\{\phi \circ b_L \mid b \in B\}$. There is an A-B bimodule monomorphism of K_0/J_ϕ into $\mathrm{Hom}_Z(A, B)$ which maps g_0+J_ϕ onto ϕ, and the mapping $\psi \to 1\psi$ is a right B-module homomorphism of $\mathrm{Hom}_Z(A, B)$ onto B. That the composite of these two maps is a right B-module isomorphism of K_0/J_ϕ onto $(1\phi)\cdot B$ follows readily from the identities $ag_0+J_\phi=g_0(a\phi)+J_\phi$ and $a(\phi \circ b_R)=(a\phi)\cdot(1(\phi \circ b_R))$ for $a \in A$ and $b \in B$.

2. Strongly independent homomorphisms.

(2.1) DEFINITION. A set S of homomorphisms of ring A into ring B is independent if $\{R(J_\phi) \mid \phi \in S\}$ is an independent set of B-A submodules of $\mathrm{Hom}_Z(A, B)$, i.e., whenever m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, then $R(J_{\phi_1}) \cap \sum_{i=2}^m R(J_{\phi_i})=0$.

Since $R(J_\phi)=\{\phi \circ b_L \mid b \in B\}$ for any homomorphism ϕ of ring A into ring B, a set S of homomorphisms of ring A into ring B is independent if and only if, whenever m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, there does not exist a nontrivial relation $\sum_{i=1}^m \phi_i \circ (b_i)_L=0$, $b_i \in B$ for $1 \leqq i \leqq m$.

(2.2) DEFINITION. A set S of homomorphisms of ring A into ring B is strongly independent if, whenever m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, then $J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}=K_0$.

If m is a positive integer and $\phi_i \in \mathrm{Hom}_Z(A, B)$, $1 \leqq i \leqq m$, are such that $J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}=K_0$, then

$$0 = R(K_0) = R\left(\overline{J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}}\right) = R(J_{\phi_1}) \cap R\left(\bigcap_{i=2}^m J_{\phi_i}\right)$$

$$= R(J_{\phi_1}) \cap \overline{\sum_{i=2}^m R(J_{\phi_i})} \supseteq R(J_{\phi_1}) \cap \sum_{i=2}^m R(J_{\phi_i}).$$

Therefore a strongly independent set of homomorphisms of ring A into ring B is independent.

(2.3) PROPOSITION. *A set S of homomorphisms of ring A into ring B is strongly independent if and only if, whenever m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^n (x_j\phi_1)\cdot y_j=1\phi_1$ and $\sum_{j=1}^n (x_j\phi_i)\cdot y_j=0$ for $2 \leqq i \leqq m$.*

Proof. If $J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}=K_0$, then $g_0=k+k'$ where $k \in J_{\phi_1}$ and $k' \in \bigcap_{i=2}^m J_{\phi_i}$. Suppose $k'=\sum_{j=1}^n x_j g_0 y_j$, where n is a positive integer and $x_j \in A$, $y_j \in B$ for $1 \leqq j \leqq n$. Then $\sum_{j=1}^n (x_j\phi_1)\cdot y_j=1(k'f_{\phi_1})=1(g_0f_{\phi_1})=1\phi_1$, since $g_0-k'=k \in J_{\phi_1}$; and $\sum_{j=1}^n (x_j\phi_i)\cdot y_j=1(k'f_{\phi_i})=0$ for $2 \leqq i \leqq m$, since $k' \in \bigcap_{i=2}^m J_{\phi_i}$.

Conversely, suppose there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^n (x_j\phi_1)\cdot y_j=1\phi_1$ and $\sum_{j=1}^n (x_j\phi_i)\cdot y_j=0$ for $2 \leqq i \leqq m$. Let $k'=\sum_{j=1}^n x_j g_0 y_j$ and $k=g_0-k'$. For $a \in A$, $a(k'f_{\phi_1})=(a\phi_1)\cdot(1(k'f_{\phi_1}))=(a\phi_1)\cdot(1\phi_1)=a(g_0f_{\phi_1})$ and $a(k'f_{\phi_i})=(a\phi_i)\cdot(1(k'f_{\phi_i}))=0$, $2 \leqq i \leqq m$. Therefore $k' \in \bigcap_{i=2}^m J_{\phi_i}$ and $k=g_0-k' \in J_{\phi_1}$. Consequently $g_0 \in J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}$ and $J_{\phi_1}+\bigcap_{i=2}^m J_{\phi_i}=K_0$. The proposition is now immediate.

Let m be a positive integer, let $\phi_i \in \mathrm{Hom}_Z(A, B)$ for $1 \leqq i \leqq m$, and let $J_0 = \bigcap_{i=1}^m J_{\phi_i}$. $J_0 \subseteq J_{\phi_i}$ and there is an A-B bimodule epimorphism of K_0/J_0 onto K_0/J_{ϕ_i} which maps the canonical generator of K_0/J_0 onto the canonical generator of K_0/J_{ϕ_i}, $1 \leqq i \leqq m$. These epimorphisms determine a canonical A-B bimodule monomorphism of K_0/J_0 into the direct product $\prod_{i=1}^m K_0/J_{\phi_i}$. It is an easy consequence of Proposition (2.3) that a set S of homomorphisms of ring A into ring B is strongly independent if and only if, whenever m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, the canonical A-B bimodule monomorphism of K_0/J_0, $J_0 = \bigcap_{i=1}^m J_{\phi_i}$, into $\prod_{i=1}^m K_0/J_{\phi_i}$ is an isomorphism.

(2.4) PROPOSITION. *If B is a quasi-Frobenius ring, then any independent set S of homomorphism of a ring A into B is strongly independent.*

Proof. Suppose that m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S. Letting $J_0 = \bigcap_{i=1}^m J_{\phi_i}$, there is an A-B bimodule monomorphism of K_0/J_0 into $\prod_{i=1}^m K_0/J_{\phi_i}$. But $\prod_{i=1}^m K_0/J_{\phi_i}$ is a finitely generated right B-module and B, being quasi-Frobenius, is right Noetherian. Therefore K_0/J_0 is a finitely generated right B-module. Since B is quasi-Frobenius, the mappings $J \to R(J) = J^\perp$ and $R \to J(R) = R^\perp$ are anti-isomorphisms between the sublattice $\{J \in \mathscr{J} \mid J_0 \subseteq J\}$ of $\mathscr{J}$ and the sublattice $\{R \in \mathscr{R} \mid R \subseteq R(J_0)\}$ of $\mathscr{R}$. In particular, if S is independent,

$$K_0 = J(0) = J\left(R(J_{\phi_1}) \cap \sum_{i=2}^m R(J_{\phi_i})\right) = J(R(J_{\phi_1})) + \bigcap_{i=2}^m J(R(J_{\phi_i})) = J_{\phi_1} + \bigcap_{i=2}^m J_{\phi_i}.$$

Consequently, S is strongly independent.

(2.5) DEFINITION. Let G be a group of automorphisms of a ring B and let $I(G) = \{b \in B \mid b\sigma = b,\ \sigma \in G\}$. A subring A of B is G-admissible if: (i) $I(G) \subseteq A$, (ii) the set S of restrictions of elements of G to A is a finite, strongly independent set of homomorphisms of A into B, and (iii) $I(G)$ is a direct summand of the left $I(G)$-module A.

(2.6) LEMMA. *Let G be a group of automorphisms of a quasi-Frobenius ring B and let S be the set of restrictions of elements of G to a subring A of B. If $I(G) \subseteq A$, A is a finitely generated right $I(G)$-module, and S is an independent set of homomorphisms of A into B; then S is finite and strongly independent.*

Proof. S is strongly independent by Proposition (2.4). Suppose m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S. Letting $J_0 = \bigcap_{i=1}^m J_{\phi_i}$, the A-B bimodules K_0/J_0 and $\prod_{i=1}^m K_0/J_{\phi_i}$ are isomorphic; and the right B-modules K_0/J_{ϕ_i} and $B = (1\phi_i) \cdot B$ are isomorphic, $1 \leqq i \leqq m$. Therefore K_0/J_0 is a free right B-module on m generators. Since B is quasi-Frobenius, B is right Artinian and it is possible to show that no set of fewer than m elements can be a set of generators for the right B-module K_0/J_0. But the mapping $a \to ag_0 + J_0$ carries a set of generators for the right $I(G)$-module A onto a set of generators for the right B-module K_0/J_0. Therefore m cannot exceed the number of elements in a finite set of generators for the right $I(G)$-module A, and S is finite.

(2.7) PROPOSITION. *Let G be a group of automorphisms of a division ring B such that the full Galois group of B over $I(G)$ is outer. A subring A of B such that $I(G) \subseteq A$ and A is a finitely generated right $I(G)$-module, is G-admissible.*

Proof. $I(G)$ is a division subring of B and A is a left vector space over $I(G)$. $I(G)$ is a subspace of A and a direct summand of the left $I(G)$-module A. The set S of restrictions of elements of G to A is independent by [5, Proposition 7.6.1]. Since B is a division ring, it is quasi-Frobenius and A is G-admissible by Lemma (2.6).

(2.8) LEMMA. *Let G be a group of automorphisms of a ring B and let S be the set of restrictions of elements of G to a subring A of B. If $I(G) \subseteq A$, S is finite, and there exists $c \in A$ such that $\sum_{\phi \in S} (c\phi) = 1$; then $I(G)$ is a direct summand of both the left $I(G)$-module A and the right $I(G)$-module A.*

Proof. Let $a \in A$. Since S is the set of restrictions of elements of the group G to A, $\sum_{\phi \in S} (a\phi) \in I(G)$. $c_R \circ (\sum_{\phi \in S} \phi)$ is a left $I(G)$-module homomorphism of A into $I(G)$, $c_L \circ (\sum_{\phi \in S} \phi)$ is a right $I(G)$-module homomorphism of A into $I(G)$, and both are right inverses for the injection map of $I(G)$ into A. Consequently, $I(G)$ is a direct summand of both the left $I(G)$-module A and the right $I(G)$-module A.

Following Chase, Harrison, and Rosenberg [1], a set S of homomorphisms of a ring A into a ring B is said to be strongly distinct if for any two distinct elements ϕ_1, ϕ_2 of S and any nonzero idempotent $e \in B$ there exists $a \in A$ such that $(a\phi_1)e \neq (a\phi_2)e$.

(2.9) PROPOSITION. *Let G be a group of automorphisms of a commutative ring B. A subring A of B such that $I(G) \subseteq A$, A is a separable algebra over $I(G)$, A is a finitely generated $I(G)$-module, and the set S of restrictions of elements of G to A is a strongly distinct set of homomorphisms of A into B, is G-admissible.*

Proof. Let $H = \{\sigma \in G \mid a\sigma = a, a \in A\}$ and let η be the injection map of A into B. $A \otimes_{I(G)} A$ and $A \otimes_{I(G)} B$ are commutative rings; $1 \otimes \eta$ is a ring homomorphism of $A \otimes_{I(G)} A$ into $A \otimes_{I(G)} B$; and the map π of $A \otimes_{I(G)} B$ into B such that $(x \otimes y)\pi = xy$ for $x \in A$, $y \in B$, is a ring homomorphism of $A \otimes_{I(G)} B$ into B. Since A is a separable $I(G)$-algebra, there exists an idempotent $e \in A \otimes_{I(G)} A$ such that $e(1 \otimes \eta)\pi = 1$ and $ae = ea$ for $a \in A$. If $\sigma \in G$, then $1 \otimes \sigma$ is an automorphism of $A \otimes_{I(G)} B$ and $e_\sigma = e(1 \otimes \eta)(1 \otimes \sigma)\pi$ is an idempotent in B. But $a \cdot e_\sigma = (ae)(1 \otimes \eta)(1 \otimes \sigma)\pi = (ea)(1 \otimes \eta)(1 \otimes \sigma)\pi = e_\sigma(a\sigma)$ for $a \in A$. Since S is strongly distinct, $e_\sigma = 0$ for $\sigma \notin H$. If $\sigma \in H$, $e_\sigma = e(1 \otimes \eta)(1 \otimes \sigma)\pi = e(1 \otimes \eta)\pi = 1$. Therefore, if $e = \sum_{j=1}^{n} x_j \otimes y_j$ where n is a positive integer and x_j, $y_j \in A$ for $1 \leqq j \leqq n$, then $\sum_{j=1}^{n} x_j(y_j\sigma) = 1$ for $\sigma \in H$ and $\sum_{j=1}^{n} x_j(y_j\sigma) = 0$ for $\sigma \in G$ but $\sigma \notin H$.

Suppose m is a positive integer and ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S. Let $\sigma_i \in G$ be such that ϕ_i is the restriction of σ_i to A, $1 \leqq i \leqq m$; and let $z_j = y_j\sigma_1$,

$1 \leqq j \leqq n$. $\sum_{j=1}^{n} (x_j\tau)\cdot z_j = 1$ for $\tau \in H\sigma_1$ and $\sum_{j=1}^{n} (x_j\tau)\cdot z_j = 0$ for $\tau \notin H\sigma_1$. Since the ϕ_i, $1 \leqq i \leqq m$, are distinct elements of S, $\sigma_i \notin H\sigma_1$ for $2 \leqq i \leqq m$. Therefore

$$\sum_{j=1}^{n} (x_j\phi_1)\cdot z_j = \sum_{j=1}^{n} (x_j\sigma_1)\cdot z_j = 1$$

and

$$\sum_{j=1}^{n} (x_j\phi_i)\cdot z_j = \sum_{j=1}^{n} (x_j\sigma_i)\cdot z_j = 0 \text{ for } 2 \leqq i \leqq m.$$

By Proposition (2.3), S is strongly independent. B is a commutative ring and it is possible to show that a free B-module on m generators cannot be generated by any subset of fewer than m elements. Therefore the argument in the proof of Lemma (2.7) may be applied to show that S is finite. Letting $\omega = \sum_{\phi \in S} \phi$, ω is an $I(G)$-module homomorphism of A onto an ideal I in $I(G)$. But $\sum_{j=1}^{n} x_j\cdot(y_j\omega) = 1$; therefore $I\cdot A = A$. Since $I(G)$ is a commutative ring and A is a finitely generated $I(G)$-module, there exists $b \in I$ such that $(1-b)A = 0$ [7, Lemma 2, p. 215]. But then $b = 1$ and there exists $c \in A$ such that $1 = c\omega = \sum_{\phi \in S} c\phi$. It now follows from Lemma (2.8) that A is G-admissible.

3. Finite Galois theory.

(3.1) DEFINITION. Let G be a group of automorphisms of a ring B. B is a K-ring (after W. Krull) with respect to G if any finite subset of B is contained in a G-admissible subring of B.

(3.2) LEMMA. *Let B be a K-ring with respect to a group G of automorphisms of B, and let S be the set of restrictions of elements of G to a subring A of B. If $I(G) \subseteq A$ and S is a finite, strongly independent set of homomorphisms of A into B, then there exists $c \in A$ such that $\sum_{\phi \in S} (c\phi) = 1$.*

Proof. Suppose ϕ_i, $1 \leqq i \leqq m$, are the distinct elements of S for a positive integer m. If S is strongly independent, there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} (x_j\phi_1)\cdot y_j = 1\phi_1 = 1$ and $\sum_{j=1}^{n} (x_j\phi_i)\cdot y_j = 0$ for $2 \leqq i \leqq m$. Let C be a G-admissible subring of B such that $\{y_j \mid 1 \leqq j \leqq n\} \subseteq C$. Letting $\omega = \sum_{\phi \in S} \phi$, ω is a right $I(G)$-module homomorphism of A into $I(G)$ and $\omega \otimes 1$ is a right C-module homomorphism of $A \otimes_{I(G)} C$ into $I(G) \otimes_{I(G)} C \cong C$. The cokernel of $\omega \otimes 1$ is canonically isomorphic to $(\operatorname{coker} \omega) \otimes_{I(G)} C$. But $\sum_{j=1}^{n} (x_j\omega)\cdot y_j = 1$, therefore $\omega \otimes 1$ is an epimorphism and $(\operatorname{coker} \omega) \otimes_{I(G)} C = 0$. Since $I(G)$ is a direct summand of the left $I(G)$-module C, $\operatorname{coker} \omega = 0$, ω is an epimorphism, and there exists $c \in A$ such that $1 = c\omega = \sum_{\phi \in S} (c\phi)$.

(3.3) COROLLARY. *Let B be a K-ring with respect to a group G of automorphisms of B. A subring A of B is G-admissible if, and only if, $I(G) \subseteq A$ and the set of restrictions of elements of G to A is a finite, strongly independent set of homomorphisms of A into B.*

Proof. The corollary is an immediate consequence of Definition (2.5) and Lemma (2.8).

Let G be a group of automorphisms of a ring B, let T be a subset of B, let $H=\{\sigma \in G \mid b\sigma=b,\ b \in T\}$, and let S be the set of maps of T into B which are restrictions of elements of G. H is a subgroup of G and there is a one-to-one correspondence between S and the set of left cosets of G relative to H. Indeed, the restriction to T of the elements in any system of representatives of the left cosets of G relative to H is a one-to-one map of that system onto S. Moreover, T is mapped into itself by the elements of S if and only if H is an invariant subgroup of G. Now assume that B is a K-ring with respect to G, and let $a \in B$. There exists a G-admissible subring A of B such that $a \in A$. Since the set of homomorphisms of A into B which are restrictions of elements of G is finite, there are only finitely many images of a under the automorphisms in G. Consequently, if T is a finite subset of B, S must be finite and H is a subgroup of finite index in G. For a subgroup H of a group G, let $(G : H)$ denote the index of H in G.

(3.4) LEMMA. *Let B be a K-ring with respect to a group G of automorphisms of B, let A be a G-admissible subring of B, and let $H=\{\sigma \in G \mid a\sigma=a,\ a \in A\}$. H is a subgroup of finite index in G; and, if H_1 is a subgroup of G such that $H \subseteq H_1$, then $I(H_1)$ is a G-admissible subring of B, $H_1=\{\sigma \in G \mid b\sigma=b,\ b \in I(H_1)\}$, and B is a K-ring with respect to H_1.*

Proof. Let S be the set of restrictions of elements of G to A. Since A is G-admissible, S is a finite, strongly independent set of homomorphisms of A into B. In particular, $(G : H)$ must be finite. Let H_1 be a subgroup of G such that $H \subseteq H_1$. Clearly $I(G) \subseteq I(H_1)$. Since $(G : H)$ is finite, so are $(G : H_1)$ and $(H_1 : H)$. If $\{\sigma_p \in H_1 \mid 1 \leqq p \leqq (H_1 : H)\}$ is a system of representatives of the left cosets of H_1 relative to H and $\{\tau_q \in G \mid 1 \leqq q \leqq (G : H_1)\}$ is a system of representatives of the left cosets of G relative to H_1, then $\{\sigma_p\tau_q \mid 1 \leqq p \leqq (H_1 : H)$ and $1 \leqq q \leqq (G : H_1)\}$ is a system of representatives of the left cosets of G relative to H. Since S is strongly independent, there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} (x_j\sigma_1\tau_1)\cdot y_j=1$ and $\sum_{j=1}^{n} (x_j\sigma_p\tau_q)\cdot y_j=0$ for $2 \leqq p \leqq (H_1 : H)$ or $2 \leqq q \leqq (G : H_1)$. If $w_j=\sum_{p=1}^{p=(H_1:H)} (x_j\sigma_p)$; then $w_j \in I(H_1)$ for $1 \leqq j \leqq n$, $\sum_{j=1}^{n} (w_j\tau_1)\cdot y_j=1$, and $\sum_{j=1}^{n} (w_j\tau_q)\cdot y_j=0$ for $2 \leqq q \leqq (G : H_1)$. Certainly $H_1 \subseteq \{\sigma \in G \mid b\sigma=b,\ b \in I(H_1)\}$, and the set S_1 of restrictions of elements of G to $I(H_1)$ is no more than the set of restrictions of the automorphisms τ_q, $1 \leqq q \leqq (G : H_1)$, to $I(H_1)$. Therefore S_1 is finite and strongly independent by Proposition (2.3). $I(H_1)$ is G-admissible by Corollary (3.3).

If the set $\{\tau_q \mid 1 \leqq q \leqq (G : H_1)\}$ is chosen so that $\tau_1 \in H_1$, then $\sum_{j=1}^{n} w_jy_j = \sum_{j=1}^{n} (w_j\tau_1)\cdot y_j=1$ and $\sum_{j=1}^{n} (w_j\tau_q)\cdot y_j=0$ for $2 \leqq q \leqq (G : H_1)$. Therefore $\tau_q \notin \{\sigma \in G \mid b\sigma=b,\ b \in I(H_1)\}$ for $2 \leqq q \leqq (G : H_1)$ and $\{\sigma \in G \mid b\sigma=b,\ b \in I(H_1)\} = H_1$. Letting T_1 be a finite subset of $I(H_1)$ such that the automorphisms τ_q, $1 \leqq q \leqq (G : H_1)$, restrict to distinct maps of T_1 into B, $H_1=\{\sigma \in G \mid b\sigma=b,\ b \in T_1\}$.

Let F be a finite subset of B, let T_2 be the set of images of elements of $T_1 \cup F$ under the automorphisms in G, and let $H_2=\{\sigma \in G \mid b\sigma=b, b \in T_2\}$. T_2 is a finite set and there exists a G-admissible subring A' of B such that $T_2 \subseteq A'$. Since $T_1 \subseteq T_2 \subseteq A'$, $\{\sigma \in G \mid a\sigma=a, a \in A'\} \subseteq H_2 \subseteq H_1$ and $I(H_2)$ is a G-admissible subring of B. Also $I(H_1) \subseteq I(H_2)$ and $F \subseteq T_2 \subseteq I(H_2)$. Since the set of restrictions of elements of G to $I(H_2)$ is finite and strongly independent, so is the set of restrictions of elements of H_1 to $I(H_2)$. Since T_2 contains the images of its elements under the automorphisms in G, H_2 is an invariant subgroup of G and, consequently, $I(H_2)$ is mapped into itself by the automorphisms in G. Let $\{u_r \in H_1 \mid 1 \leqq r \leqq (H_1 : H_2)\}$ be a system of representatives of the left cosets of H_1 relative to H_2. Since H_2 is an invariant subgroup of H_1, $\{u_r^{-1} \mid 1 \leqq r \leqq (H_1 : H_2)\}$ is also a system of representatives of the left cosets of H_1 relative to H_2. $\{u_r^{-1}\tau_q \mid 1 \leqq q \leqq (G : H_1)$ and $1 \leqq r \leqq (H_1 : H_2)\}$ is a system of representatives of the left cosets of G relative to H_2, as is also $\{\tau_q^{-1}u_r \mid 1 \leqq q \leqq (G : H_1)$ and $1 \leqq r \leqq (H_1 : H_2)\}$, since H_2 is an invariant subgroup of G. By Lemma (3.2), there exists $b \in I(H_2)$ such that

$$\sum_{q=1}^{q=(G:H_1)} \sum_{r=1}^{r=(H_1:H_2)} (b\tau_q^{-1}u_r) = 1.$$

Letting

$$c = \sum_{q=1}^{q=(G:H_1)} (b\tau_q^{-1}), \quad c \in I(H_2)$$

and

$$\sum_{r=1}^{r=(H_1:H_2)} (cu_r) = 1.$$

It now follows from Lemma (2.8) that $I(H_2)$ is H_1-admissible. Since F may be any finite subset of B, B is a K-ring with respect to H_1.

(3.5) PROPOSITION. *Let B be a K-ring with respect to a group G of automorphisms of B, let A be a G-admissible subring of B, let S be the set of restrictions of elements of G to A, and let $H=\{\sigma \in G \mid a\sigma=a, a \in A\}$.*

(i) $A=I(H)$.

(ii) *The right $I(G)$-module A is finitely generated, projective, and contains $I(G)$ as a direct summand.*

(iii) $\mathrm{Hom}_{I(G)}(A, B)$ *is a direct sum of the B-A bimodules $R(J_\phi) \subseteq \mathrm{Hom}_Z(A, B)$, $\phi \in S$.*

(iv) *If $J_0=\bigcap_{\phi \in S} J_\phi$, there exist canonical A-B bimodule isomorphisms $A \otimes_{I(G)} B \cong K_0/J_0 \cong \mathrm{Hom}_B(\mathrm{Hom}_{I(G)}(A, B), B)$.*

Proof. H is a subgroup of finite index in G and B is a K-ring with respect to H by Lemma (3.4). Let $\{\tau_q \in G \mid 1 \leqq q \leqq (G : H)\}$ be a system of representatives of the left cosets of G relative to H with $\tau_1 \in H$. Since A is G-admissible, there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^n (x_j\tau_1)\cdot y_j = 1$ and $\sum_{j=1}^n (x_j\tau_q)\cdot y_j = 0$ for $2 \leqq q \leqq (G : H)$. Thus $\sum_{j=1}^n x_j y_j = 1$ and $\sum_{j=1}^n (x_j\sigma)\cdot y_j = 0$ for $\sigma \in G$ but $\sigma \notin H$. Let A_1 be an H-admissible subring of B such that

$\{y_j \mid 1 \leqq j \leqq n\} \subseteq A_1$, and let $H_1 = \{\sigma \in H \mid a\sigma = a,\ a \in A_1\}$. By Lemma (3.4), H_1 is a subgroup of finite index in H. If $\{\sigma_p \in H \mid 1 \leqq p \leqq (H : H_1)\}$ is a system of representatives of the left cosets of H relative to H_1, there exists $c \in A_1$ such that $\sum_{p=1}^{p=(H:H_1)} (c\sigma_p) = 1$ by Lemma (3.2). Letting $z_j = \sum_{p=1}^{p=(H:H_1)} (y_j c)\sigma_p$, $z_j \in I(H)$ for $1 \leqq j \leqq n$, and

$$\sum_{j=1}^{n} x_j \cdot z_j = \sum_{p=1}^{p=(H:H_1)} \left(\sum_{j=1}^{n} x_j y_j c\right)\sigma_p = 1$$

while

$$\sum_{j=1}^{n} (x_j\sigma) \cdot z_j = \sum_{p=1}^{p=(H:H_1)} \left(\sum_{j=1}^{n} (x_j \sigma\sigma_p^{-1}) \cdot y_j c\right)\sigma_p = 0$$

for $\sigma \in G$ but $\sigma \notin H$. Letting f_j be the restriction of $(z_j)_L \cdot \sum_{q=1}^{q=(G:H)} \tau_q$ to $I(H)$, f_j is a right $I(G)$-module homomorphism of $I(H)$ into $I(G)$ for $1 \leqq j \leqq n$, and

$$\sum_{j=1}^{n} x_j \cdot (bf_j) = \sum_{q=1}^{q=(G:H)} \left(\sum_{j=1}^{n} (x_j \tau_q^{-1}) \cdot z_j b\right)\tau_q = b\tau_1 = b$$

for $b \in I(H)$. But $\sum_{j=1}^{n} x_j \cdot (bf_j) \in A$ for $b \in I(H)$, and therefore $A = I(H)$. The representation $a = \sum_{j=1}^{n} x_j \cdot (af_j)$, $a \in A$, shows that A is a finitely generated, projective right $I(G)$-module. $I(G)$ is a direct summand of the right $I(G)$-module A by Lemma (3.2) and Lemma (2.8).

For $\phi \in S$, $R(J_\phi)$ is a B-A submodule of $\mathrm{Hom}_{I(G)}(A, B)$. Let ϕ_q be the restriction of τ_q to A for $1 \leqq q \leqq (G : H)$. If $\psi \in \mathrm{Hom}_{I(G)}(A, B)$, let

$$\omega = \sum_{q=1}^{q=(G:H)} \sum_{j=1}^{n} (z_j)_L \cdot \phi_q \cdot (x_j\psi)_L.$$

For $a \in A$, $a\omega = \sum_{j=1}^{n} \sum_{q=1}^{q=(G:H)} (x_j\psi) \cdot ((z_j a)\phi_q) = \sum_{j=1}^{n} (x_j\psi) \cdot (af_j) = a\psi$; therefore $\psi = \omega$, but $\sum_{j=1}^{n} (z_j)_L \cdot \phi_q \cdot (x_j\psi)_L \in R(J_{\phi_q})$ for $1 \leqq q \leqq (G : H)$. Therefore $\psi \in \sum_{\phi \in S} R(J_\phi)$ and $\sum_{\phi \in S} R(J_\phi) = \mathrm{Hom}_{I(G)}(A, B)$. Since S is a strongly independent set of homomorphisms of A into B, it is an independent set and $\{R(J_\phi) \mid \phi \in S\}$ is an independent set of B-A submodules of $\mathrm{Hom}_Z(A, B)$. Therefore $\mathrm{Hom}_{I(G)}(A, B)$ is a direct sum of the B-A bimodules $R(J_\phi)$, $\phi \in S$. Let J_1 be the A-B submodule of K_0 generated by the set $\{bg_0 - g_0 b \mid b \in I(G)\}$. $R(J_1) = \mathrm{Hom}_{I(G)}(A, B)$ and there is an A-B bimodule isomorphism of $A \otimes_{I(G)} B$ onto K_0/J_1 which maps $1 \otimes 1$ onto g. Since A is finitely generated, projective right $I(G)$-module, $K_0/J_1 \cong A \otimes_{I(G)} B$ is a finitely generated, projective B-module. Therefore the natural A-B bimodule homomorphism h of K_0/J_1 into $\mathrm{Hom}_B(R(J_1), B) = \mathrm{Hom}_B(\mathrm{Hom}_{I(G)}(A, B), B)$ is an isomorphism and J_1 is a closed A-B submodule of K_0. If $J_0 = \bigcap_{\phi \in S} J_\phi$, then J_0 is also a closed A-B submodule of K_0. Clearly $J_1 \subseteq J_0$, so $R(J_0) \subseteq R(J_1) = \mathrm{Hom}_{I(G)}(A, B)$. But $R(J_0) = R(\bigcap_{\phi \in S} J_\phi) \supseteq \sum_{\phi \in S} R(J_\phi) = \mathrm{Hom}_{I(G)}(A, B)$. Therefore $R(J_0) = R(J_1)$, $J_0 = J(R(J_0)) = J(R(J_1)) = J_1$, and the theorem follows.

(3.6) PROPOSITION. *If B is a K-ring with respect to a group G of automorphisms of B and H is a subgroup of finite index in G, then $I(H)$ is a G-admissible subring of B.*

Proof. Suppose $I(H)$ were not a G-admissible subring of B. Let F_1 be any finite subset of $I(H)$, let n be a positive integer, and suppose that a finite subset F_n of $I(H)$ has already been chosen. Letting $H_n=\{\sigma\in G \mid b\sigma=b,\ b\in F_n\}$, $H\subseteq H_n$ and $I(H_n)\subseteq I(H)$. There exists a G-admissible subring A of B such that $F_n\subseteq A$. $\{\sigma\in G \mid a\sigma=a,\ a\in A\}\subseteq H_n$ and $I(H_n)$ is a G-admissible subring of B by Lemma (3.4). Therefore $I(H_n)\neq I(H)$ and there exists $c\in I(H)$ such that $c\notin I(H_n)$. Let $F_{n+1}=F_n\cup\{c\}$ and $H_{n+1}=\{\sigma\in G \mid b\sigma=b,\ b\in F_{n+1}\}$. $H\subseteq H_{n+1}\subset H_n$; and a properly descending chain $\{H_n \mid n\geqq 1\}$ of subgroups of G, each of which contains H, is defined by induction. But then H cannot be of finite index in G.

(3.7) COROLLARY. *Let G be a finite group of automorphisms of a ring B. B is a K-ring with respect to G if, and only if, G is a strongly independent set of automorphisms of B and $I(G)$ is a direct summand of the left $I(G)$-module B.*

Proof. B is a G-admissible subring of itself if, and only if, G is a strongly independent set of automorphisms of B and $I(G)$ is a direct summand of the left $I(G)$-module B. If B is a G-admissible subring of itself, then B is certainly a K-ring with respect to G. Conversely, suppose B is a K-ring with respect to G. Since G is finite, the trivial subgroup $\{1\}$ of G has finite index in G and $B=I(\{1\})$ is a G-admissible subring of itself.

(3.8) THEOREM. *If B is a K-ring with respect to a finite group G of automorphisms of B, then the mapping $H\to I(H)$ is a bijection of the set of subgroups of G onto the set of G-admissible subrings of B.*

Proof. B is a G-admissible subring of itself by Corollary (3.7). If H is a subgroup of G, then $H\supseteq\{1\}=\{\sigma\in G \mid b\sigma=b,\ b\in B\}$. By Lemma (3.4), $I(H)$ is a G-admissible subring of B and $H=\{\sigma\in G \mid b\sigma=b,\ b\in I(H)\}$. Conversely, if A is a G-admissible subring of B and $H=\{\sigma\in G \mid a\sigma=a,\ a\in A\}$, then $A=I(H)$. The theorem is now immediate.

Let G be a group of automorphisms of a ring B. If H is an invariant subgroup of G, then $I(H)$ is mapped into itself by the automorphisms in G. If A is a subring of B which is mapped into itself by the automorphisms in G, then the restriction of elements of G to A is a homomorphism of G onto a group of automorphisms of A.

(3.9) PROPOSITION. *Let B be a K-ring with respect to a group G of automorphisms of B.*

(i) *If H is an invariant subgroup of G, then $I(H)$ is a K-ring with respect to the group G' of automorphisms of $I(H)$ which are restrictions of elements of G.*

(ii) *If F is a finite subset of B, then there exists a G-admissible subring A of B such that $F\subseteq A$, A is mapped into itself by the automorphisms in G, and A is a K-ring with respect to the group G' of automorphisms of A which are restrictions of elements of G.*

Proof. Let H be an invariant subgroup of G and let G' be the group of automorphisms of $I(H)$ which are restrictions of elements of G. Clearly $I(H)\supseteq I(G)=I(G')$. Let F be a finite subset of $I(H)$ and let $H_1=\{\sigma\in G \mid b\sigma=b,\ b\in F\}$. Then $H\subseteq H_1$

and $F \subseteq I(H_1) \subseteq I(H)$. Since F is finite, $(G : H_1)$ is finite and $I(H_1)$ is G-admissible by Proposition (3.6). Therefore $I(G')$ is contained as a direct summand in the left $I(G')$-module $I(H_1)$. The set S of restrictions of elements of G' to $I(H_1)$ is equal to the set of restrictions of elements of G to $I(H_1)$. If $\{\sigma_p \in G \mid 1 \leqq p \leqq (G : H_1)\}$ is a system of representatives of the left cosets of G relative to H_1, there exist a positive integer n and elements $x_j \in I(H_1)$ and $y_j \in B$, $1 \leqq j \leqq n$, such that

$$\sum_{j=1}^{n} (x_j\sigma_1)\cdot y_j = 1$$

and

$$\sum_{j=1}^{n} (x_j\sigma_p)\cdot y_j = 0$$

for $2 \leqq p \leqq (G : H_1)$. If $y_j' = y_j\sigma_1^{-1}$ for $1 \leqq j \leqq n$, then

$$\sum_{j=1}^{n} x_j y_j' = 1$$

and

$$\sum_{j=1}^{n} (x_j\sigma)\cdot y_j' = 0$$

for $\sigma \in G$ but $\sigma \notin H_1$. Repetition of the argument in the first part of the proof of Proposition (3.5) shows that there exist $z_j \in I(H_1) \subseteq I(H)$ for $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} x_j z_j = 1$ and $\sum_{j=1}^{n} (x_j\sigma)\cdot z_j = 0$ for $\sigma \in G$ but $\sigma \notin H_1$. Then $z_j\sigma_1 \in I(H)$ for $1 \leqq j \leqq n$, and $\sum_{j=1}^{n} (x_j\sigma_1)\cdot(z_j\sigma_1) = 1$ while $\sum_{j=1}^{n} (x_j\sigma_p)\cdot(z_j\sigma_1) = 0$ for $2 \leqq p \leqq (G : H_1)$. Consequently, S is a finite, strongly independent set of homomorphisms of $I(H_1)$ into $I(H)$ and $I(H_1)$ is a G'-admissible subring of $I(H)$. Since F may be any finite subset of $I(H)$, $I(H)$ is a K-ring with respect to G'.

If F is a finite subset of B, then $T = \{b\sigma \mid b \in F \text{ and } \sigma \in G\}$ is a finite set and $H = \{\sigma \in G \mid b\sigma = b, b \in T\}$ is an invariant subgroup of finite index in G. If $A = I(H)$, then $F \subseteq T \subseteq A$, A is mapped into itself by the automorphisms in G, and A is a K-ring with respect to the group G' of automorphisms of A which are restrictions of elements of G. Moreover, since $(G : H)$ is finite, A is G-admissible.

4. Infinite Galois theory.

(4.1) PROPOSITION. *Let B be a K-ring with respect to a group G of automorphisms of B, and let G^* be the closure of G in the set of maps of B into B with respect to the finite topology.*

(i) *$\sum_{\sigma \in G} R(J_\sigma)$ is a direct sum of the B-B bimodules $R(J_\sigma) \subseteq \mathrm{Hom}_Z(B, B)$ and $\sum_{\sigma \in G} R(J_\sigma)$ is a dense subring of $\mathrm{Hom}_{I(G)}(B, B)$ with respect to the finite topology.*

(ii) *G^* is a group of automorphisms of B which is compact with respect to the finite topology and B is a K-ring with respect to G^*.*

Proof. Suppose m is a positive integer and σ_i, $1 \leqq i \leqq m$, are distinct elements of G. Let T be a finite subset of B such that the automorphisms σ_i, $1 \leqq i \leqq m$, restrict to distinct maps of T into B; let A be a G-admissible subring of B which contains T; and let ϕ_i be the restriction of σ_i to A, $1 \leqq i \leqq m$. The homomorphisms ϕ_i, $1 \leqq i \leqq m$,

are distinct, and the set of restrictions of elements of G to A is strongly independent, hence independent. Therefore there does not exist a nontrivial relation $\sum_{i=1}^{m} \phi_i \circ (b_i)_L = 0$, $b_i \in B$, for $1 \leqq i \leqq m$. Then certainly there cannot exist a nontrivial relation $\sum_{i=1}^{m} \sigma_i \circ (b_i)_L = 0$, $b_i \in B$, for $1 \leqq i \leqq m$; and $\{R(J_{\sigma_i}) \mid 1 \leqq i \leqq m\}$ is an independent set of B-B submodules of $\mathrm{Hom}_Z(B, B)$. It follows that $\{R(J_\sigma) \mid \sigma \in G\}$ is an independent set of B-B submodules of $\mathrm{Hom}_Z(B, B)$ and $\sum_{\sigma \in G} R(J_\sigma)$ is a direct sum. For $\sigma \in G$, $R(J_\sigma)$ is a B-B submodule of $\mathrm{Hom}_{I(G)}(B, B)$; and $\sum_{\sigma \in G} R(J_\sigma)$ is a subring of $\mathrm{Hom}_{I(G)}(B, B)$ since G is a group of automorphisms of B. Let $\psi \in \mathrm{Hom}_{I(G)}(B, B)$, let F be a finite subset of B, and let A be a G-admissible subring of B which contains F. The restriction of ψ to A is an element of $\mathrm{Hom}_{I(G)}(A, B)$; and $\mathrm{Hom}_{I(G)}(A, B) = \sum_{\phi \in S} R(J_\phi)$, where S is the set of restrictions of elements of G to A, by part (iii) of Proposition (3.5). Therefore ψ and some element of $\sum_{\sigma \in G} R(J_\sigma)$ restrict to the same homomorphism of A into B and, hence, to the same map of F into B. Therefore $\sum_{\sigma \in G} R(J_\sigma)$ is a dense subring of $\mathrm{Hom}_{I(G)}(B, B)$.

By routine arguments using the finite topology, it can be verified that G^* is a semigroup of monomorphisms of the ring B into itself and $I(G) = \{b \in B \mid b\tau = b, \tau \in G^*\}$. Let $\tau \in G^*$. If $b \in B$, then the set T_1 of images of b under the automorphisms in G is finite, the restriction of τ to T_1 coincides with the restriction of some $\sigma \in G$ to T_1, and $(b\sigma^{-1})\tau = (b\sigma^{-1})\sigma = b$. Therefore τ is an automorphism of B. Let F be a finite subset of B and let $T_2 = \{b\tau^{-1} \mid b \in F\}$. The restriction of τ to T_2 coincides with the restriction of some $\sigma \in G$ to T_2 and the restriction of τ^{-1} to F coincides with the restriction of σ^{-1} to F. Therefore $\tau^{-1} \in G^*$, G^* is a group of automorphisms of B, and $I(G^*) = I(G)$. Let A be a G-admissible subring of B. A is a finitely generated right $I(G)$-module by part (ii) of Proposition (3.5), and the restriction of $\tau \in G^*$ to a finite set of generators of the right $I(G)$-module A coincides with the restriction of some $\sigma \in G$ to this set. Therefore the set of restrictions of elements of G^* to A is equal to the set of restrictions of elements of G to A, and A is G^*-admissible. Consequently, B is a K-ring with respect to G^*. For $b \in B$, $T_b = \{b\tau \mid \tau \in G^*\}$ is a finite set. Let T_b be topologized by the discrete topology and let $\prod_{b \in B} T_b$ be the product space. Since T_b is compact for each $b \in B$, $\prod_{b \in B} T_b$ is compact. But the mapping $\tau \to (b\tau)_{b \in B}$ is a homomorphism of G^* with the finite topology onto a closed subspace of $\prod_{b \in B} T_b$. Therefore G^* is compact.

(4.2) THEOREM. *Let B be a K-ring with respect to a group G of automorphisms of B, and assume that G is a closed subset of the set of maps of B into B with respect to the finite topology.*

(i) *For a subgroup H of G, $H = \{\sigma \in G \mid a\sigma = a, a \in A\}$ for some subring A of B if and only if H is a closed subgroup of G with respect to the finite topology.*

(ii) *For a subring A of B, $A = I(H)$ for some subgroup H of G if and only if A has the property that any finite subset of A is contained in a subring of A which is G-admissible.*

Proof. If A is a subring of B, then $H=\{\sigma \in G \mid a\sigma=a,\ a \in A\}$ is a closed subgroup of G by routine arguments using the finite topology. Suppose H is a closed subgroup of G and let $H_1=\{\sigma \in G \mid b\sigma=b,\ b \in I(H)\}$. Clearly $H \subseteq H_1$. If F is a finite subset of B, there exists a G-admissible subring A of B such that $F \subseteq A$, A is mapped into itself by the automorphisms in G, and A is a K-ring with respect to the group G' of automorphisms of A which are restrictions of elements of G, by part (ii) of Proposition (3.9). Let H' (resp. H_1') be the set of restrictions of elements of H (resp. H_1) to A. H' and H_1' are subgroups of G' and $I(H')=I(H) \cap A=I(H_1')$. Since A is G-admissible, G' is finite and $H'=H_1'$ by Theorem (3.8). Therefore the set of restrictions of elements of H to $F \subseteq A$ is equal to the set of restrictions of elements of H_1 to F. Consequently H is dense in H_1 with respect to the finite topology. Since H is closed, $H=H_1=\{\sigma \in G \mid b\sigma=b,\ b \in I(H)\}$.

If H is a subgroup of G and F is a finite subset of $I(H)$, let $H_1=\{\sigma \in G \mid b\sigma=b,\ b \in F\}$. $H \subseteq H_1$ and $F \subseteq I(H_1) \subseteq I(H)$. Since F is finite, $(G : H_1)$ is finite and $I(H_1)$ is G-admissible by Proposition (3.6). Conversely, suppose A is a subring of B with the property that any finite subset of A is contained in a subring of A which is G-admissible, and let $H=\{\sigma \in G \mid a\sigma=a,\ a \in A\}$. Let $\{A_i \mid i \in I\}$ be the set of subrings of A which are G-admissible, where I is some indexing set, and let $H_i=\{\sigma \in G \mid a\sigma=a,\ a \in A_i\}$ for $i \in I$. If $b \in B$ but $b \notin A$, let $U=\{\sigma \in G \mid b\sigma=b\}$. The set theoretic difference H_i-U is a closed subset of G for $i \in I$. If I_0 is a finite subset of I, $\bigcap_{i \in I_0}(H_i-U)$ is nonempty. Indeed each A_i, $i \in I$, is a finitely generated right $I(G)$-module. Let F_i be a finite set of generators for the right $I(G)$-module A_i, $i \in I_0$, and suppose A_1 is the subring of A which is G-admissible and contains the finite set $\bigcup_{i \in I_0} F_i$. Then $A_i \subseteq A_1$ and $H_1 \subseteq H_i$ for $i \in I_0$. Since $A_1=I(H_1)$, there exists $\sigma \in H_1$ such that $b\sigma \neq b$, and $\sigma \in \bigcap_{i \in I_0}(H_i-U)$. But G is compact by part (ii) of Proposition (4.1). Therefore $\bigcap_{i \in I}(H_i-U)$ is nonempty. If $\sigma \in \bigcap_{i \in I}(H_i-U)$ then $b\sigma \neq b$. But if $a \in A$, then $a \in A_i$ for some $i \in I$ and $a\sigma=a$. Therefore $\sigma \in H$ and $A=I(H)$.

REFERENCES

1. S. U. Chase, D. K. Harrison and Alex Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), pp. 15–33.

2. J. Dieudonné, *Linearly compact spaces and double vector space over s fields*, Amer. J. Math. **73** (1951), 13–19.

3. G. Hochschild, *Double vector spaces over division rings*, Amer. J. Math. **71** (1949), 443–460.

4. N. Jacobson, *An extension of Galois theory to non-normal and non-separable fields*, Amer. J. Math. **66** (1944), 1–29.

5. ———, *Structure of rings*, Colloq. Publ., Vol. 37, Amer. Math Soc., Providence, R. I., 1964.

6. O. Ore, *Galois connexions*, Trans. Amer. Math. Soc. **55** (1944), 493–513.

7. O. Zariski and P. Samuel, *Commutative algebra*, Vol. 1, Van Nostrand, Princeton, N. J., 1958.

FLORIDA STATE UNIVERSITY,
TALLAHASSEE, FLORIDA