GALOIS THEORY FOR NONCOMMUTATIVE RINGS AND NORMAL BASES(1)

BY
H. F. KREIMER

Introduction. The author [5] has formulated sufficient conditions on a ring B and a group G of automorphisms of B to derive a Galois theory of noncommutative rings which extends the Galois theory of commutative rings developed by Chase, Harrison, and Rosenberg [3]. This paper continues the study of that Galois theory, investigating the structure of the lattice of left ideals in B and the existence of normal bases for B.

1. *G*-**invariant ideals.** In subsequent use, ring will mean ring with identity element, subring of a ring will mean subring which contains the identity element of the ring, and the identity element of a ring will be denoted by 1. The following definitions are listed here for convenient reference.

(1.1) 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, 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 $2 \leqq i \leqq m$.

(1.2) Definition. Let G be a group of automorphisms of a ring B and let $I(G) = \{b \in B \mid b\sigma = b,\ \sigma \in G\}$.

(i) A subring A of B is G-admissible if $I(G) \subseteq A$, the set S of restrictions of elements of G to A is a finite strongly independent set of homomorphisms of A into B, and $I(G)$ is a direct summand of the left $I(G)$-module A.

(ii) B is a K-ring with respect to G if any finite subset of B is contained in a G-admissible subring of B.

(1.3) Definition. Let G be a group of automorphisms of a ring B. A subset T of B is G-invariant if $b\sigma \in T$ whenever $b \in T$ and $\sigma \in G$.

If G is a group of automorphisms of a ring B and P is a G-invariant two-sided ideal in B, $P \neq B$, then each automorphism in G induces an automorphism of the residue class ring B/P and the correspondence to each automorphism in G of the induced automorphism in B/P is a representation of G as a group of automorphisms of B/P.

(1.4) Theorem. *Let B be a K-ring with respect to a group G of automorphisms of B, and let P be a G-invariant two-sided ideal in B, $P \neq B$. The canonical representation of G as a group of automorphisms of B/P is faithful, B/P is a K-ring with*

Presented to the Society, January 25, 1967; received by the editors April 25, 1966.

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

respect to G, and $(I(G)+P)/P$ is the subring of elements of B/P which are invariant under G.

Proof. Let A be a G-admissible subring of B; let S be the set of restrictions of elements of G to A; and, for $\phi \in S$, let $\bar{\phi}$ be the induced homomorphism of $(A+P)/P$ into B/P. If ϕ_i, $1 \leqq i \leqq m$, are the distinct elements of S for some positive integer m, indexed arbitrarily, there exist a positive integer n and elements $x_j \in A$ and $y_j \in B$, $1 \leqq j \leqq n$, such that $\sum_{j=1}^{n} (x_j\phi_1)\cdot y_j = 1$ and $\sum_{j=1}^{n}(x_j\phi_i)\cdot y_j = 0$ for $2 \leqq i \leqq m$. Reducing these equations modulo P, it is evident that the $\bar{\phi}_i$, $1 \leqq i \leqq m$, are distinct and strongly independent homomorphisms of $(A+P)/P$ into B/P. Suppose $a \in A$ and $a - a\sigma \in P$ for $\sigma \in G$. There exists $c \in A$ such that $\sum_{\phi \in S} c\phi = 1$ [5, Lemma 3.2], and $a - \sum_{\phi \in S} (ac)\phi = \sum_{\phi \in S} (a - a\phi)(c\phi) \in P$. But $\sum_{\phi \in S} (ac)\phi \in I(G)$. Since any finite subset of B is contained in a G-admissible subring of B, it follows that distinct elements of G induce distinct automorphisms of B/P and $(I(G)+P)/P$ is the subring of elements of B/P which are invariant under G.

Considering again the given G-admissible subring A of B, $I(G) \subseteq A$ and, therefore, $(I(G)+P)/P$ is a subring of $(A+P)/P$. The set $\bar{S}$ of restrictions to $(A+P)/P$ of the automorphisms of B/P induced by elements of G is just the set of homomorphisms of $(A+P)/P$ into B/P induced by elements of S, and this set is finite and has been shown to be strongly independent. If $c \in A$ is such that $\sum_{\phi \in S} c\phi = 1$, then $(c+P) \in (A+P)/P$ and $\sum_{\bar{\phi} \in \bar{S}} (c+P)\bar{\phi} = 1 + P$. It follows from [5, Lemma 2.8], that $(A+P)/P$ is a G-admissible subring of B/P. If F is a finite subset of B/P, select a finite subset of B which contains a representative element from each residue class which is an element of F and suppose A is a G-admissible subring of B which contains this finite subset of B. $(A+P)/P$ is a G-admissible subring of B/P which contains F. Consequently B/P is a K-ring with respect to G.

Let G be a group of automorphisms of a ring B and let $\mathrm{Hom}_{I(G)}(B, B)$ be the ring of right $I(G)$-module endomorphisms of B. B is a right $\mathrm{Hom}_{I(G)}(B, B)$-module. For $b \in B$, let b_L denote the mapping $x \to bx$ of B into itself. $\sigma \in \mathrm{Hom}_{I(G)}(B, B)$ for $\sigma \in G$ and $b_L \in \mathrm{Hom}_{I(G)}(B, B)$ for $b \in B$.

(1.5) Proposition. *Let B be a K-ring with respect to a finite group G of automorphisms of B. If M is a right $\mathrm{Hom}_{I(G)}(B, B)$-module and $M_0 = \{x \in M \mid x\sigma = x, \sigma \in G\}$, then M_0 is a left $I(G)$-module such that the right $\mathrm{Hom}_{I(G)}(B, B)$-module homomorphism of $B \otimes_{I(G)} M_0$ into M which maps $b \otimes x$ onto xb_L for $b \in B$ and $x \in M_0$ is an isomorphism onto M.*

Proof. B is a G-admissible subring of itself by [5, Corollary 3.7]. Regard B as a right $I(G)$-module and let $\Omega = \mathrm{Hom}_{I(G)}(B, B)$. B is a finitely generated, projective right $I(G)$-module by [5, Proposition 3.5]. By [5, Lemma 3.2], there exists $c \in B$ such that $\sum_{\sigma \in G} c\sigma = 1$. Therefore $\sum_{\sigma \in G} \sigma$ is a right $I(G)$-module epimorphism of B onto $I(G)$ and the evaluation map of $B \otimes_{\Omega} \mathrm{Hom}_{I(G)}(B, I(G))$ into $I(G)$ is an $I(G)-I(G)$ bimodule epimorphism. By [1, Proposition A.6], the right Ω-module homomorphism of $B \otimes_{I(G)} \mathrm{Hom}_\Omega(B, M)$ into M which maps $b \otimes f$ onto $bf = (1b_L)f = (1f)b_L$ for $b \in B$ and $f \in \mathrm{Hom}_\Omega(B, M)$ is an isomorphism. But the ring Ω is generated by its elements $\sigma \in G$ and b_L, $b \in B$, [5, Propositions 1.2 and 3.5]; and the mapping $f \to 1f$, $f \in \mathrm{Hom}_\Omega(B, M)$, is a one-to-one correspondence of the set $\mathrm{Hom}_\Omega(B, M)$ onto the set M_0. The proposition results from identifying M_0 with $\mathrm{Hom}_\Omega(B, M)$ by this one-to-one correspondence.

A direct proof of this proposition can also be given by adapting to the present considerations the appropriate part of the proof of [3, Theorem 1.3].

(1.6) THEOREM. *Let B be a K-ring with respect to a group G of automorphisms of B. The mapping $P \to P \cap I(G)$ is an isomorphism of the lattice of G-invariant left ideals in B onto the lattice of left ideals in $I(G)$, and the inverse of this isomorphism is the mapping $Q \to B \cdot Q$. Moreover, for any left ideal Q in $I(G)$, the left B-module homomorphism of $B \otimes_{I(G)} Q$ into $B \cdot Q$ which maps $b \otimes c$ onto bc for $b \in B$ and $c \in Q$ is an isomorphism.*

Proof. Let P be a G-invariant left ideal in B. Clearly $P \cap I(G)$ is a left ideal in $I(G)$ and $B \cdot (P \cap I(G)) \subseteq P$. Suppose A is G-invariant, G-admissible subring of B. $A = I(H)$ for some subgroup H of finite index in G [5, Lemma 3.4 and Proposition 3.5], and H must be an invariant subgroup of G. By [5, Proposition 3.9], A is a K-ring with respect to the group G' of automorphisms of A which are restrictions of elements of G. G' is a finite group, $I(G') = I(G)$, and A is a G'-admissible subring of itself by [5, Corollary 3.7]. $P \cap A$ is a G'-invariant left ideal in A, and the ring $\mathrm{Hom}_{I(G)}(A, A)$ of right $I(G)$-module endomorphisms of A is generated by its elements $\tau \in G'$ and a_L, $a \in A$ [5, Propositions 1.2 and 3.5]. Therefore $P \cap A$ is a right $\mathrm{Hom}_{I(G)}(A, A)$-module. Letting $M = P \cap A$ and applying Proposition 1.5, $M_0 = P \cap I(G)$ and the right $\mathrm{Hom}_{I(G)}(A, A)$-module homomorphism π' of $A \otimes_{I(G)} (P \cap I(G))$ into $P \cap A$ which maps $a \otimes x$ onto $xa_L = ax$ for $a \in A$ and $x \in P \cap I(G)$ is an isomorphism. Letting i be the injection map of A into B and π be the left B-module homomorphism of $B \otimes_{I(G)} (P \cap I(G))$ into $B \cdot (P \cap I(G))$ which maps $b \otimes c$ onto bc for $b \in B$ and $c \in P \cap I(G)$, it is easily verified that π is an epimorphism and the diagram

$$\begin{array}{ccc} A \otimes_{I(G)} (P \cap I(G)) & \xrightarrow{i \otimes 1} & B \otimes_{I(G)} (P \cap I(G)) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ P \cap A & \subseteq & B \cdot (P \cap I(G)) \end{array}$$

is commutative. Since any finite subset of B is contained in a G-invariant, G-admissible subring of B [5, Proposition 3.9], it follows that $P = B \cdot (P \cap I(G))$ and that π is an isomorphism.

Let Q be a left ideal in $I(G)$. It is easily verified that $B \cdot Q$ is a G-invariant left ideal in B and $Q \subseteq (B \cdot Q) \cap I(G)$. Suppose $c \in (B \cdot Q) \cap I(G)$, say $c = \sum_{j=1}^{n} b_j \cdot c_j$ where n is a positive integer and $b_j \in B$, $c_j \in Q$ for $1 \leqq j \leqq n$. If A is a G-admissible subring of B which contains the finite set $\{b_j \mid 1 \leqq j \leqq n\}$ and S is the set of restrictions of elements of G to A, there exists $d \in A$ such that $\sum_{\phi \in S} d\phi = 1$ [5, Lemma 3.2].

$$c = \sum_{\phi \in S} (dc)\phi = \sum_{j=1}^{n} \left(\sum_{\phi \in S} (db_j)\phi \right) \cdot c_j$$

and

$$\sum_{\phi \in S} (db_j)\phi \in I(G), \quad 1 \leqq j \leqq n.$$

Therefore $c \in Q$ and $Q = B \cdot Q \cap I(G)$. It is now established that the mapping $P \to P \cap I(G)$ of the lattice of G-invariant left ideals in B into the lattice of left ideals in $I(G)$ and the mapping $Q \to B \cdot Q$ of the lattice of left ideals in $I(G)$ into the lattice of G-invariant left ideals in B are inverses to each other. Since both mappings preserve order, they are lattice isomorphisms.

Several consequences of Theorem 1.6 may be worth observing. Let B be a K-ring with respect to a group G of automorphisms of B. If B is a left Artinian, respectively Noetherian, ring then $I(G)$ is a left Artinian, respectively Noetherian, ring. Indeed, if the lattice of left ideals in B satisfies the minimum, respectively maximum, condition, then the sublattice of G-invariant left ideals in B also satisfies this condition, and the lattice of left ideals in $I(G)$ must satisfy the same condition by Theorem 1.6. If B is a (commutative) local ring and P is the unique maximal ideal in B, then P is a G-invariant ideal in B and it is an all element or identity element in the lattice of G-invariant ideals in B. Therefore, by Theorem 1.6, $P \cap I(G)$ is a maximal ideal in $I(G)$, it is unique, and $I(G)$ is a local ring. Moreover, the canonical representation of G as a group of automorphisms of B/P is faithful, and $(I(G)+P)/P$ is the subring of elements of B/P which are invariant under G by Theorem 1.4. There is a canonical ring isomorphism of $I(G)/(P \cap I(G))$ onto $(I(G)+P)/P$, and G is isomorphic to a dense subgroup of the group of all automorphisms of the residue class field B/P over the residue class field $I(G)/(P \cap I(G))$ with respect to the finite topology. In particular, if G is finite, then B/P is a finite dimensional field extension of $I(G)/(P \cap I(G))$ and G is isomorphic to the Galois group of B/P over $I(G)/(P \cap I(G))$.

(1.7) Lemma. *Let R be a two-sided ideal contained in the radical of a ring A, let M be a finitely generated right A-module, and let N be a finitely generated, projective right A-module. If f is an A-module homomorphism of M into N such that $f \otimes 1$ is an isomorphism of $M \otimes_A (A/R)$ onto $N \otimes_A (A/R)$, then f is an isomorphism of M onto N.*

Proof. If $f \otimes 1$ is an epimorphism, then f is an epimorphism by [2, §6, No. 3, Corollary 4 to Proposition 6]. Since N is a projective right A-module, the exact sequence

$$0 \longrightarrow \ker f \longrightarrow M \xrightarrow{f} N \longrightarrow 0$$

splits, and the derived sequence

$$0 \longrightarrow (\ker f) \otimes_A (A/R) \longrightarrow M \otimes_A (A/R) \xrightarrow{f \otimes 1} N \otimes_A (A/R) \longrightarrow 0$$

is exact. If $f \otimes 1$ is an isomorphism, then $(\ker f) \otimes_A (A/R) = 0$. But $\ker f$ is a finitely generated right A-module, since it is a direct summand of the finitely generated right A-module M. Therefore $\ker f = 0$ by [2, §6, No. 3, Corollary 3 to Proposition 6], and f is an isomorphism.

(1.8) Proposition. *Let B be a K-ring with respect to a finite group G of automorphisms of B, and let m be the order of G. If $I(G)$ is a semilocal subring of the center of B, then B is a free $I(G)$-module of rank m.*

Proof. If $I(G)$ is a semilocal subring of the center of B, there are only finitely many maximal ideals in $I(G)$. Denote the distinct maximal ideals in $I(G)$ by Q_γ, γ ranging over some finite indexing set Γ, and let $R = \bigcap_{\gamma \in \Gamma} Q_\gamma$. There is a canonical $I(G)$-module isomorphism of $I(G)/R$ onto the direct sum $\sum_{\gamma \in \Gamma} I(G)/Q_\gamma$, which determines an $I(G)$-module isomorphism of $M \otimes_{I(G)} (I(G)/R)$ onto the direct sum $\sum_{\gamma \in \Gamma} M \otimes_{I(G)} (I(G)/Q_\gamma)$ for any $I(G)$-module M. Let $\gamma \in \Gamma$. By Theorem 1.6, $B \cdot Q_\gamma$ is a G-invariant ideal in B and $B \cdot Q_\gamma \cap I(G) = Q_\gamma$. Moreover $B \cdot Q_\gamma$ is a two-sided ideal in B and the $I(G)$-modules $B/B \cdot Q_\gamma$ and $B \otimes_{I(G)} (I(G)/Q_\gamma)$, derived from the $I(G)$-module B, are isomorphic. Letting $\bar{B}$ denote the residue class ring $B/B \cdot Q_\gamma$ and C denote the subring $(I(G) + B \cdot Q_\gamma)/B \cdot Q_\gamma$ of $\bar{B}$, the canonical representation of G as a group of automorphisms of $\bar{B}$ is faithful, $\bar{B}$ is a K-ring with respect to G, and C is the subring of elements of $\bar{B}$ which are invariant under G. C is canonically isomorphic to $I(G)/(B \cdot Q_\gamma \cap I(G)) = I(G)/Q_\gamma$ both as a ring and as an $I(G)$-module. Since Q_γ is a maximal ideal in $I(G)$, C is a field. $\bar{B}$ is a G-admissible subring of itself by [5, Corollary 3.7]; and $\bar{B}$, which is an algebra over C, must be finite dimensional over C by [5, Proposition 3.5]. If n is the dimension of $\bar{B}$ over C, then n^2 is the dimension of the algebra $\mathrm{Hom}_c(\bar{B}, \bar{B})$ over C. But $\mathrm{Hom}_c(\bar{B}, \bar{B})$ is a free left $\bar{B}$-module on the set G of m elements by [5, Propositions 1.2 and 3.5]; consequently, the dimension of $\mathrm{Hom}_c(\bar{B}, \bar{B})$ over C is $m \cdot n$. Therefore $m = n$ and the $I(G)$-module $\bar{B} \cong B \otimes_{I(G)} (I(G)/Q_\gamma)$ is isomorphic to a direct sum of m copies of the $I(G)$-module $C \cong I(G)/Q_\gamma$. Thus, if $I(G)^m$ is a free $I(G)$-module on a set of m elements, the $I(G)$-modules $B \otimes_{I(G)} (I(G)/Q_\gamma)$ and $I(G)^m \otimes_{I(G)} (I(G)/Q_\gamma)$ are isomorphic for $\gamma \in \Gamma$. Consequently, the $I(G)$-modules $B \otimes_{I(G)} (I(G)/R)$ and $I(G)^m \otimes_{I(G)} (I(G)/R)$ are isomorphic. Let f be a homomorphism of the free $I(G)$-module $I(G)^m$ into B such that $f \otimes 1$ is an isomorphism of $I(G)^m \otimes_{I(G)} (I(G)/R)$ onto $B \otimes_{I(G)} (I(G)/R)$. R is the radical of $I(G)$ and f is an isomorphism by Lemma 1.7. Therefore B is a free $I(G)$-module of rank m.

2. **Normal bases.** Let G be a group of automorphisms of a ring B, let Z denote the ring of integers, and let $Z(G)$ denote the group ring of G. With the usual definition of multiplication for the tensor product of algebras, $Z(G) \otimes_Z I(G)$ is a ring. B is a right $I(G)$, $\mathrm{Hom}_{I(G)}(B, B)$-module, the action of G on B determines a ring homomorphism of $Z(G)$ into $\mathrm{Hom}_{I(G)}(B, B)$, and thereby B becomes a right $Z(G) \otimes_Z I(G)$-module.

(2.1) DEFINITION. B has a normal basis with respect to a group G of automorphisms of B if there exists a right $Z(G) \otimes_Z I(G)$-module isomorphism of $Z(G) \otimes_Z I(G)$ onto B.

$Z(G) \otimes_Z I(G)$ is a free right $I(G)$-module on the set G. If B has a normal basis with respect to G and $b \in B$ is the image of the identity element of $Z(G) \otimes_Z I(G)$ under a right $Z(G) \otimes_Z I(G)$ isomorphism of $Z(G) \otimes_Z I(G)$ onto B, then B is a free right $I(G)$-module and $\{b\sigma \mid \sigma \in G\}$ is a set of free generators for the right $I(G)$-module B. Conversely, if B is a free right $I(G)$-module and there exists $b \in B$ such that $\{b\sigma \mid \sigma \in G\}$ is a set of free generators for the right $I(G)$-module B, then the mapping $\sigma \to b\sigma$, $\sigma \in G$, determines a unique right $I(G)$-module isomorphism of $Z(G) \otimes_Z I(G)$ onto B and this isomorphism is a right $Z(G) \otimes_Z I(G)$-module isomorphism.

Even when B is a simple Artinian ring and a K-ring with respect to a finite group G of automorphisms of B, B may fail to have a normal basis with respect to G.

(2.2) EXAMPLE. Let Δ be a division ring of characteristic different from two and let Δ_3 be the ring of 3×3 matrices over Δ. Let I and 0 denote the identity and zero matrices, respectively, in Δ_3; and let E_{ij} denote the element of Δ_3 with entry 1 in the ith row and jth column and entry 0 elsewhere, for $1 \leqq i, j \leqq 3$. Let σ be the inner automorphism of Δ_3 determined by $E_{11}+E_{22}-E_{33}$. If $a_{ij} \in \Delta$ for $1 \leqq i$, $j \leqq 3$, then

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\sigma = \begin{pmatrix} a_{11} & a_{12} & -a_{13} \\ a_{21} & a_{22} & -a_{23} \\ -a_{31} & -a_{32} & a_{33} \end{pmatrix}$$

and σ generates a subgroup G of order two in the group of all automorphisms of Δ_3.

$I(G)=(\Delta E_{11}+\Delta E_{12}+\Delta E_{21}+\Delta E_{22})+\Delta E_{33}$. Let $X_1=I$, $X_2=E_{13}+E_{31}$, $X_3=E_{23}$, $Y_1=\frac{1}{2}I$, $Y_2=\frac{1}{2}(E_{13}+E_{31})$, and $Y_3=\frac{1}{2}E_{32}$. Then $X_1Y_1+X_2Y_2+X_3Y_3=I$ and $(X_1\sigma)Y_1+(X_2\sigma)Y_2+(X_3\sigma)Y_3=0$. From these equations it follows readily that G is a strongly independent set of automorphisms of Δ_3. Moreover, as a left $I(G)$-module, $\Delta_3=I(G) \oplus (\Delta E_{13}+\Delta E_{23}+\Delta E_{31}+\Delta E_{32})$. Therefore Δ_3 is a K-ring with respect to G [5, Corollary 3.7]. $I(G)=(\Delta E_{11}+\Delta E_{12}) \oplus (\Delta E_{21}+\Delta E_{22}) \oplus \Delta E_{33}$ is a decomposition of $I(G)$ as a direct sum of minimal right ideals, while $\Delta_3 =(\Delta E_{11}+\Delta E_{12}) \oplus (\Delta E_{21}+\Delta E_{22}) \oplus (\Delta E_{31}+\Delta E_{32}) \oplus \Delta E_{13} \oplus \Delta E_{23} \oplus \Delta E_{33}$ is a decomposition of the right $I(G)$-module Δ_3 as a direct sum of irreducible submodules. Evidently, Δ_3 is not a free right $I(G)$-module nor can Δ_3 be generated as a right $I(G)$-module by fewer than three elements. Therefore Δ_3 does not have a normal basis with respect to G.

If G is a group of automorphisms of a ring B, then B and $Z(G) \otimes_Z I(G)$ are in fact $I(G)-Z(G) \otimes_Z I(G)$ bimodules. Consequently, $B \otimes_{I(G)} B$ and $B \otimes_{I(G)} (Z(G) \otimes_Z I(G))$ are right $Z(G) \otimes_Z I(G)$-modules.

(2.3) LEMMA. *If B is a K-ring with respect to a finite group G of automorphisms of B, then there is a right $Z(G) \otimes_Z I(G)$-isomorphism of $B \otimes_{I(G)} (Z(G) \otimes_Z I(G))$ onto $B \otimes_{I(G)} B$.*

Proof. B is a G-admissible subring of itself [5, Corollary 3.7]. $\mathrm{Hom}_{I(G)}(B, B)$ is a free left B-module, G is a basis for this free left B-module, and there is a canonical B-B bimodule isomorphism of $B \otimes_{I(G)} B$ onto $\mathrm{Hom}_B(\mathrm{Hom}_{I(G)}(B, B), B)$ by [5, Propositions 1.2 and 3.5]. Under the canonical B-B bimodule isomorphism of $B \otimes_{I(G)} B$ onto $\mathrm{Hom}_B(\mathrm{Hom}_{I(G)}(B, B), B)$, $a \otimes b$ corresponds to the mapping $f \to (af)\cdot b$ for $a, b \in B$ and $f \in \mathrm{Hom}_{I(G)}(B, B)$. If $\{\sigma^* \mid \sigma \in G\}$ is the basis for $B \otimes_{I(G)} B$ dual to G, then in the right $Z(G) \otimes_Z I(G)$-module $B \otimes_{I(G)} B$, $\sigma^* \cdot \tau = (\sigma\tau)^*$ for $\sigma, \tau \in G$. From the equation $b\sigma^* = \sigma^*(b\sigma)$, $b \in B$ and $\sigma \in G$, it follows that $B \otimes_{I(G)} B$ is not only a free right B-module on the set $\{\sigma^* \mid \sigma \in G\}$ but also a free left B-module on this same set. There is a canonical right $Z(G) \otimes_Z I(G)$-module isomorphism of $B \otimes_{I(G)} (Z(G) \otimes_Z I(G))$ onto $B \otimes_Z Z(G)$, and $B \otimes_Z Z(G)$ is a free left B-module on the set G. The mapping $\sigma \to \sigma^*$, $\sigma \in G$, determines a unique left B-module isomorphism of $B \otimes_Z Z(G)$ onto $B \otimes_{I(G)} B$, which is readily verified to be a right $Z(G) \otimes_Z I(G)$-module isomorphism. Thus there is a right $Z(G) \otimes_Z I(G)$-module isomorphism of $B \otimes_{I(G)} (Z(G) \otimes_Z I(G))$ onto $B \otimes_{I(G)} B$.

(2.4) THEOREM. *Let B be a K-ring with respect to a finite group G of automorphisms of B, and let m be the order of G. If $I(G)$ is a semiprimary ring and the right $I(G)$-module B can be generated by a subset of m elements, then B has a normal basis with respect to G.*

Proof. If $I(G)$ is a semiprimary ring and R is the radical of $I(G)$, then $I(G)/R$ is a semisimple Artinian ring. Let $I(G)^m$ be a free right $I(G)$-module on a set of m elements. If the right $I(G)$-module B can be generated by a subset of m elements, there exist a right $I(G)$-module epimorphism f of $I(G)^m$ onto B and an exact sequence

$$0 \longrightarrow \ker f \longrightarrow I(G)^m \xrightarrow{f} B \longrightarrow 0.$$

Since B is a G-admissible subring of itself [5, Corollary 3.7], B is a finitely generated, projective right $I(G)$-module by [5, Proposition 3.5]. Therefore the derived sequence

$$0 \longrightarrow (\ker f) \otimes_{I(G)} B \longrightarrow I(G)^m \otimes_{I(G)} B \xrightarrow{f \otimes 1} B \otimes_{I(G)} B \longrightarrow 0$$

is an exact sequence of right $I(G)$-modules and $I(G)^m \otimes_{I(G)} B$ and $B \otimes_{I(G)} B$ are finitely generated, projective right $I(G)$-modules. $I(G)^m \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ are completely reducible right $I(G)$-modules and $f \otimes 1 \otimes 1$ is a right $I(G)$-module epimorphism of $I(G)^m \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ onto $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$. But $I(G)^m \otimes_{I(G)} B$ is a free right B-module on a set of m elements as is also $B \otimes_{I(G)} B$; and, consequently, the right $I(G)$-modules $I(G)^m \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ are isomorphic and have the same number of irreducible components, that number being finite since

$I(G)^m \otimes_{I(G)} B$ and $B \otimes_{I(G)} B$ are finitely generated right $I(G)$-modules. Therefore $f \otimes 1 \otimes 1$ must be an isomorphism, $f \otimes 1$ is an isomorphism by Lemma 1.7, and $(\ker f) \otimes_{I(G)} B = 0$. Since B is a G-admissible subring of itself, $I(G)$ is a direct summand of the left $I(G)$-module B, $\ker f = 0$, and f is an isomorphism. Thus B is a free right $I(G)$-module of rank m.

By Lemma 2.3, $B \otimes_{I(G)} (Z(G) \otimes_Z I(G)) \cong Z(G) \otimes_Z B$ and $B \otimes_{I(G)} B$ are isomorphic right $Z(G) \otimes_Z I(G)$-modules. Then $Z(G) \otimes_Z B \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ are isomorphic right $Z(G) \otimes_Z I(G)$-modules. Since B is a free right $I(G)$-module of rank m; then, as right $Z(G) \otimes_Z I(G)$-modules, $Z(G) \otimes_Z B \otimes_{I(G)} (I(G)/R)$ is isomorphic to a direct sum of m copies of $Z(G) \otimes_Z I(G) \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ is isomorphic to a direct sum of m copies of $B \otimes_{I(G)} (I(G)/R)$. But $Z(G) \otimes_Z B \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ are finitely generated, completely reducible right $I(G)$-modules and therefore satisfy the maximum and minimum conditions for submodules. Thus the right $Z(G) \otimes_Z I(G)$-modules $Z(G) \otimes_Z B \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} B \otimes_{I(G)} (I(G)/R)$ must satisfy the maximum and minimum conditions for submodules. It is a direct consequence of the Krull-Schmidt theorem that $Z(G) \otimes_Z I(G) \otimes_{I(G)} (I(G)/R)$ and $B \otimes_{I(G)} (I(G)/R)$ must be isomorphic right $Z(G) \otimes_Z I(G)$-modules. Let g be a right $Z(G) \otimes_Z I(G)$-module homomorphism of $Z(G) \otimes_Z I(G)$ into B such that $g \otimes 1$ is an isomorphism of $Z(G) \otimes_Z I(G) \otimes_{I(G)} (I(G)/R)$ onto $B \otimes_{I(G)} (I(G)/R)$. $Z(G) \otimes_Z I(G)$ and B are finitely generated, projective right $I(G)$-modules and g is a right $I(G)$-module homomorphism. g is an isomorphism by Lemma 1.7. Thus B has a normal basis with respect to G.

(2.5) Corollary. *If B is a K-ring with respect to a finite group G of automorphisms of B and $I(G)$ is a semilocal subring of the center of B, then B has a normal basis with respect to G.*

Proof. If $I(G)$ is a semilocal subring of the center of B, then $I(G)$ is a semiprimary ring. The corollary is an immediate consequence of Proposition 1.8 and Theorem 2.4.

References

1. M. Auslander and D. Buchsbaum, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24.

2. N. Bourbaki, *Éléments de mathématique. Fascicule* XXIII. *Algèbre*, Chapitre 8, *Modules et anneaux semi-simples*, Actualités Sci. Indust. No. 1261, Hermann, Paris, 1958.

3. 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.

4. N. Jacobson, *Structure of rings*, Colloq. Publ., Vol. 37, Amer. Math. Soc., Providence, R. I., 1964.

5. H. F. Kreimer, *A Galois theory for noncommutative rings*, Trans. Amer. Math. Soc. **127** (1967), 29–41.

Florida State University,
Tallahassee, Florida