ON ALGEBRAS ARISING FROM THE ELEMENTS OF A GALOIS GROUP FOR A GALOIS ALGEBRA

GORO AZUMAYA
Department of Mathematics, Indiana University
Bloomington, IN 47405, USA

GEORGE SZETO
Department of Mathematics, Bradley University
Peoria, Illinois 61625, USA

LIANYONG XUE
Department of Mathematics, Bradley University
Peoria, Illinois 61625, USA

ABSTRACT. Let B be a ring with 1 and C the center of B. It is shown that if B is a Galois algebra over R with a finite Galois group G, $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ for each $g \in G$, and e_g an idempotent in C such that $BJ_g = Be_g$, then the algebra $B(g)$ generated by $\{J_h \,|\, h \in G$ and $e_h = e_g\}$ for an $g \in G$ is a separable algebra over Re_g and a central weakly Galois algebra with Galois group $K(g)$ generated by $\{h \in G \,|\, e_h = e_g\}$. Moreover, $\{B(g) \,|\, g \in G\}$ and $\{K(g) \,|\, g \in G\}$ are in a one-to-one correspondence, and three characterizations of a Galois extension are also given.

1. INTRODUCTION

The Boolean algebra of the idempotents in a commutative Galois algebra plays an important role ([2],[9]). For a noncommutative Galois algebra B over a commutative ring R with a finite Galois group G and center C, and $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ for each $g \in G$, it was shown that $BJ_g = Be_g$ for some central idempotent e_g $(\in C)$ for any $g \in G$ ([5]). We note that the central idempotent e_g is uniquely determined by g in G. To see this, let e be a central idempotent of B. Then the mapping $b \longmapsto be$ $(b \in B)$ defines a ring epimorphism $B \longrightarrow Be$ because $(b+b')e = be + b'e$ and $(bb')e = (be)(b'e)$ for every b, $b' \in B$. Thus, as the image of 1, e is the identity of the subring Be. Therefore if f is another central idempotent of B such that $Be = Bf$, then f is also the identity of Be,

AMS 2000 Subject Classification. 16S35, 16W20.
Keywords and Phrases. Separable algebras, Galois algebras, central Galois algebras, weakly Galois algebras, Azumaya Galois extensions.

and so we know that $e = f$. Hence, in particular, if f is a central idempotent such that $BJ_g = Bf$, i.e., $Be_g = Bf$, then it follows that $f = e_g$. Let B_a be the Boolean algebra generated by $\{0, e_g \,|\, g \in G\}$. Then a structure theorem for B was given by using B_a ([6]) and the subalgebra $\oplus \sum_{g \in K(1)} J_g$ was investigated where $K(1) = \{h \in G \,|\, e_h = 1\}$ ([8]). We note that B is a central Galois algebra with Galois group G if and only if $K(1) = G$. Let $S(g) = \{h \in G \,|\, e_h = e_g\}$ for each $g \in G$. Then $S(1) = K(1)$, but $S(g)$ is not a subgroup of G for any $e_g \neq 1$ ([7]). Denote the subgroup generated by the elements in $S(g)$ by $K(g)$. The purpose of the present paper is to investigate a more general class of algebras $B(g)$ generated by $\{J_h \,|\, h \in S(g)\}$ for an $g \in G$. The major results are (1) $B(g) = \oplus \sum_{k \in K(g)} e_g J_k$, (2) $B(g)$ is a separable algebra over Re_g, (3) $B(g)$ is a central weakly Galois algebra with Galois group $K(g)$ where a weakly Galois algebra is in the sense of [9], and (4) there exists a one-to-one correspondence between the set of algebras $\{B(g) \,|\, g \in G\}$ and the set of subgroups $\{K(g) \,|\, g \in G\}$. Thus $B = \sum_{g \in G} B(g)$ such that $B(g)$ is a central weakly Galois algebra with Galois group $K(g)$ for each $g \in G$. Three remarkable characterizations of a Galois extension in section 5 were given by the first author. This paper was written under the support of a Caterpillar Fellowship at Bradley University. The authors would like to thank Caterpillar Inc. for the support.

2. BASIC NOTATIONS AND DEFINITIONS

Throughout this paper, B will represent a ring with 1 and G a finite automorphism group of B. We keep the definitions of a Galois extension, a Galois algebra, a central Galois algebra, a separable extension, and an Azumaya algebra as defined in ([6]).

From now on, let B be a Galois algebra over a commutative ring R with a finite Galois group G, C the center of B, $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ for each $g \in G$, e_g a central idempotent in C such that $BJ_g = Be_g$ ([5]), $S(g) = \{h \in G \,|\, e_h = e_g\}$ for each $g \in G$, $K(g)$ the subgroup of G generated by $\{h \,|\, h \in S(g)\}$, $B(g)$ the algebra contained in B generated by $\{J_h \,|\, h \in S(g)\}$ for each $g \in G$, and $J_g^{(A)} = \{a \in A \,|\, ax = g(x)a$ for all $x \in A\}$ for a subring A of B. A weakly Galois extension A with Galois group G is a finitely generated projective right module A over A^G such that $A_l G = \mathrm{Hom}_{A^G}(A, A)$ where

$A_l = \{a_l$, the left multiplication map by $a \in A\}$ and $(a_l g)(x) = ag(x)$ for each $a_l \in A_l$ and $x \in A$ ([9]). We call A a weakly Galois algebra with Galois group G if A is a weakly Galois extension with Galois group G such that A^G is contained in the center of A and that A is a central weakly Galois algebra with Galois group G if A is a weakly Galois extension with Galois group G such that A^G is the center of A. An Azumaya Galois extension A with Galois group G is a Galois extension A of A^G which is a C^G-Azumaya algebra where C is the center of A ([1]). We call A an Azumaya weakly Galois extension with Galois group G if it is a weakly Galois extension of A^G which is a C^G-Azumaya algebra where C is the center of A.

3. THE SEPARABLE ALGEBRA $B(g)$

Let $g \in G$ and $B(g)$ the algebra generated by $\{J_h \mid h \in S(g)\}$. Keeping the notations in section 2, we shall show that $B(g) = \oplus \sum_{k \in K(g)} e_g J_k$ and that $B(g)$ is a separable algebra over Re_g. We begin with some lemmas.

LEMMA 3.1.

Let $G(g) = \{h \in G \mid h(e_g) = e_g\}$. Then $K(g)$ is a normal subgroup of $G(g)$.

PROOF. Clearly, $G(g)$ is a subgroup of G. Next, let $k \in S(g)$. Then $e_k = e_g$; and so $k(e_g) = k(e_k) = e_{kkk^{-1}} = e_k = e_g$. Hence $k \in G(g)$. Thus $S(g) \subset G(g)$. But $K(g)$ is the subgroup generated by the elements in $S(g)$ by the definition of $K(g)$, so $K(g)$ is a subgroup of $G(g)$. Next we show $K(g)$ is a normal subgroup of $G(g)$. For any $h \in G(g)$ and $k \in S(g)$, we have that $e_{hkh^{-1}} = h(e_k) = h(e_g) = e_g$, so $hkh^{-1} \in S(g)$. Clearly, $k^{-1} \in S(g)$ if $k \in S(g)$. Hence for any $k \in K(g)$, $k = k_1 k_2 \cdots k_m$ for some integer m and some $k_i \in S(g)$, $i = 1, 2, \cdots, m$. Thus, for any $h \in G(g)$, $hkh^{-1} = h(k_1 k_2 \cdots k_m)h^{-1} = (hk_1h^{-1})(hk_2h^{-1}) \cdots (hk_mh^{-1}) \in K(g)$. Therefore $hK(g)h^{-1} \subset K(g)$ for any $h \in G(g)$. This proves that $K(g)$ is a normal subgroup of $G(g)$.

LEMMA 3.2.

Be_g is a separable algebra over Re_g.

PROOF. Since B is a Galois algebra over R, B is a separable algebra over R. Hence Be_g is a separable algebra over Re_g ([3], Proposition 1.11, page 46).

LEMMA 3.3.

For each $h \in G(g)$, $J_h^{(Be_g)} = e_g J_h$.

PROOF. See Lemma 3.3 in [6].

THEOREM 3.4.

$B(g) = \oplus \sum_{k \in K(g)} e_g J_k$.

PROOF. Since $B(g)$ is generated by $\{J_h \mid h \in S(g)\}$,

$B(g) = \{\sum(\Pi J_h),$ a finite sum of finite products of J_h for some $h \in S(g)\}$.

By Proposition 2 in [5], $J_h J_{h'} = e_h J_{hh'} = e_g J_{hh'}$ for any $h, h' \in S(g)$, so $\Pi J_h = e_g J_{\Pi h}$ for some $h \in S(g)$. Hence $B(g) = \sum_{k \in K(g)} e_g J_k$. But B is a Galois algebra over R with Galois group G, so $B = \oplus \sum_{g \in G} J_g$ ([5], Theorem 1). Noting that J_h is a C-module, we have that $e_g J_h \subset J_h$ for each $h \in K(g)$. Thus, the sum is direct, that is, $B(g) = \oplus \sum_{k \in K(g)} e_g J_k$.

THEOREM 3.5.

For each $k \in K(g)$, $e_k e_g = e_g$.

PROOF. We want to prove that

$$(*) \qquad e_{g_1} e_{g_2} \cdots e_{g_n} = e_{g_2} \cdots e_{g_n} e_{g_1 g_2 \cdots g_n}$$

for any integer $n \geq 2$ and any elements $g_1, g_2, \cdots, g_n$ of G. Consider now the case for $n = 2$. We know by Proposition 2 in [5] that $J_{g_1} J_{g_2} = e_{g_2} J_{g_1 g_2}$, and so $e_{g_1} e_{g_2} B = e_{g_1} B J_{g_2} = B J_{g_1} J_{g_2} = B e_{g_2} J_{g_1 g_2} = e_{g_2} B J_{g_1 g_2} = e_{g_2} e_{g_1 g_2} B$. Since $e_{g_1} e_{g_2}$ and $e_{g_2} e_{g_1 g_2}$ are central idempotents, we have

$$(1) \qquad e_{g_1} e_{g_2} = e_{g_2} e_{g_1 g_2} \text{ for any } g_1, g_2 \in G.$$

Now assume that $(*)$ is true for an $n (\geq 2)$ and any $g_1, g_2, \cdots, g_n \in G$. Let g_{n+1} be any element of G. Then by applying (1) to $g_1 g_2 \cdots g_n$ and g_{n+1} instead of g_1 and g_2

respectively, we have

$$e_{g_1 g_2 \cdots g_n} e_{g_{n+1}} = e_{g_{n+1}} e_{g_1 g_2 \cdots g_n g_{n+1}}. \tag{2}$$

Thus we conclude

$$\begin{aligned} e_{g_1} e_{g_2} \cdots e_{g_n} e_{g_{n+1}} &= (e_{g_1} e_{g_2} \cdots e_{g_n}) e_{g_{n+1}} \\ &= (e_{g_2} \cdots e_{g_n} e_{g_1 g_2 \cdots g_n}) e_{g_{n+1}} \text{ by the assumption } (*) \\ &= (e_{g_2} \cdots e_{g_n})(e_{g_1 g_2 \cdots g_n} e_{g_{n+1}}) \\ &= (e_{g_2} \cdots e_{g_n})(e_{g_{n+1}} e_{g_1 g_2 \cdots g_n g_{n+1}}) \text{ by } (2) \\ &= e_{g_2} \cdots e_{g_n} e_{g_{n+1}} e_{g_1 g_2 \cdots g_n g_{n+1}}. \end{aligned}$$

This shows by induction that $(*)$ holds for any $n \geq 2$ and any $g_1,\ g_2,\ \cdots,\ g_n \in G$.

Now assume that $h_1,\ h_2,\ \cdots,\ h_n \in S(g)$ for some integer n, so $e_g = e_{h_1} = e_{h_2} = \cdots = e_{h_n}$. Then $e_g = e_g e_{h_1 h_2 \cdots h_n}$ by the above result $(*)$. Let L be the set of those elements of G which are finite products of elements in $S(g)$. Then clearly L is closed under multiplication. Since $e_h = e_{h^{-1}}$ for any $h \in G$ ([5], Proposition 2-(3)), $e_g = e_h = e_{h^{-1}}$ for any $h \in S(g)$; and so $h^{-1} \in S(g)$. It follows that if $h = h_1 h_2 \cdots h_n \in L$ where $h_1,\ h_2,\ \cdots,\ h_n \in S(g)$ for some integer n, then $h^{-1} = h_n^{-1} \cdots h_1^{-1} \in L$. Thus L is a subgroup generated by the elements in $S(g)$; that is, $L = K(g)$. Therefore, for any element $k \in K(g)$, $k = h_1 h_2 \cdots h_n$ where $h_1,\ h_2,\ \cdots,\ h_n \in S(g)$ for some integer n, we have that $e_g = e_g e_k$. This completes the proof.

Next is the main theorem in this section.

THEOREM 3.6.

$B(g)$ is a separable algebra over Re_g.

PROOF. Since B is a Galois algebra over R with Galois group G, there exists a $c \in C$ such that $\mathrm{Tr}_G(c) = 1$ by the proof of proposition 5 in [5]. Let $\{K(g)g_i \,|\, g_i \in G,\ i = 1, 2, \cdots, m$ for some integer $m\}$ be the set of the right cosets of $K(g)$ in G and $d = \sum_{i=1}^m g_i(c)$. Then $\mathrm{Tr}_{K(g)}(d) = \sum_{k \in K(g)} k(d) = \sum_{k \in K(g)} \sum_{i=1}^m k g_i(c) = \mathrm{Tr}_G(c) = 1.$

Hence $\mathrm{Tr}_{K(g)}(de_gx) = e_gx$ for each $e_gx \in (e_gB)^{K(g)}$. Thus the map $\mathrm{Tr}_{K(g)}(d\_) : e_gB \longrightarrow (e_gB)^{K(g)}$ is a split bimodule homomorphism over $(e_gB)^{K(g)}$. This implies that $(e_gB)^{K(g)}$ is a direct summand of e_gB as a bimodule over $(e_gB)^{K(g)}$. On the other hand, e_gB is a Galois extension of $(e_gB)^{G(g)}$ with Galois group $G(g)$ by Lemma 3.7 in [6], so e_gB is a Galois extension of $(e_gB)^{K(g)}$ with Galois group $K(g)$ for $K(g)$ is a subgroup of $G(g)$ by Lemma 3.1. Hence e_gB is a finitely generated and projective left (or right) module over $(e_gB)^{K(g)}$. Thus $(e_gB)^{K(g)}$ is a separable algebra over Re_g by the proof of Theorem 3.8 on page 55 in [3] because Be_g is a separable algebra over Re_g by Lemma 3.2. Next, we claim that $Ce_g \subset (e_gB)^{K(g)}$. In fact, for any $ce_g \in Ce_g$, $k \in K(g)$, and $x \in J_k$, we have that $(ce_g)x = x(ce_g) = k(ce_g)x$, so $(ce_g - k(ce_g))x = 0$. Hence $(ce_g - k(ce_g))J_k = \{0\}$. But $J_kJ_{k^{-1}} = e_kC$ ([5], Proposition 2), so $(ce_g - k(ce_g))e_kC = \{0\}$. By Lemma 3.5, $e_ge_k = e_g$, so $(ce_g - k(ce_g))C = \{0\}$. Thus $ce_g - k(ce_g) = 0$, that is, $k(ce_g) = ce_g$. This implies that $Ce_g \subset (e_gB)^{K(g)}$. Therefore Ce_g is contained in the center of $(e_gB)^{K(g)}$ for Ce_g is contained in the center of B. Consequently $(e_gB)^{K(g)}$ is separable over Ce_g ([3], Proposition 1.12, page 46). Moreover, since Be_g is separable over Re_g, Be_g is an Azumaya algebra over Ce_g and Ce_g is separable over Re_g ([3], Theorem 3.8, page 55). Hence $V_{Be_g}((e_gB)^{K(g)})$ is separable over Ce_g by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57); and so it is separable over Re_g by the transitivity of separable algebras. But, by Proposition 1 in [5], $V_{Be_g}((e_gB)^{K(g)}) = \oplus\sum_{k\in K(g)} J_k^{(Be_g)}$, so $V_{Be_g}((e_gB)^{K(g)}) = \oplus\sum_{k\in K(g)} e_gJ_k$ by Lemma 3.3. Therefore $B(g)$ $(= \oplus\sum_{k\in K(g)} e_gJ_k$ by Theorem 3.4) is a separable algebra over Re_g.

4. THE CENTRAL WEAKLY GALOIS ALGEBRA $B(g)$

We recall that an algebra A over a commutative ring R with a finite automorphism group G is called a weakly Galois extension with Galois group G if A is a finitely generated projective right A^G-module such that $A_lG = \mathrm{Hom}_{A^G}(A, A)$ where $A_l = \{a_l$, the left multiplication map by $a \in A\}$. We shall show that $B(g)$ is a central weakly Galois algebra with Galois group $U(g)$ where $U(g) = K(g)/L$ and $L = \{k \in K(g)\,|\,k(a) = a$ for all

$a \in B(g)\}$. For each $k \in K(g)$, $\overline{k}$ is denoted as the coset $kL \in U(g)$ and $\overline{k}(b) = k(b)$ for $b \in B(g)$.

LEMMA 4.1.

$(B(g))^{K(g)} = Z$, the center of $B(g)$.

PROOF. Let x be any element in $(B(g))^{K(g)}$ and b any element in $B(g)$. Then $b = \sum_{k\in K(g)} e_g b_k$ where $b_k \in J_k$ for each $k \in K(g)$ by Theorem 3.4. Hence

$$bx = \sum_{k\in K(g)} e_g b_k x = \sum_{k\in K(g)} e_g k(x) b_k = \sum_{k\in K(g)} e_g x b_k = x \sum_{k\in K(g)} e_g b_k = xb.$$

Thus $x \in Z$. Therefore $(B(g))^{K(g)} \subset Z$. Conversely, for any $z \in Z$, $k \in K(g)$, and $x \in J_k$, we have that $zx = xz = k(z)x$, so $(k(z) - z)x = 0$ for any $x \in J_k$. Hence $(k(z) - z)J_k = \{0\}$. Noting that $J_k J_{k^{-1}} = e_k C$, we have that $(k(z) - z)e_k C = \{0\}$. By Lemma 3.5, $e_g C = e_g e_k C \subset e_k C$. Hence $(k(z) - z)e_g C = \{0\}$, so $(k(z) - z)e_g = 0$, that is, $k(ze_g) = ze_g$. But z is in the center of $B(g)$ and $B(g) = \oplus \sum_{k\in K(g)} e_g J_k$, so $ze_g = z$. Thus $k(z) = z$ for any $z \in Z$ and $k \in K(g)$; and so $Z \subset (B(g))^{K(g)}$.

THEOREM 4.2.

$B(g)$ is a central weakly Galois algebra with Galois group $U(g)$, that is, $B(g)$ is a weakly Galois algebra over its center Z with Galois group $U(g)$.

PROOF. By Lemma 4.1, it suffices to show that $B(g)$ is a weakly Galois algebra with Galois group $U(g)$. In fact, by Theorem 3.6, $B(g)$ is separable over Re_g, so $B(g)$ is an Azumaya algebra over Z. Hence $B(g)$ is a finitely generated projective module over Z $(= (B(g))^{U(g)})$, and the map $f : B(g)\otimes_Z (B(g))^o \longrightarrow \mathrm{Hom}_Z(B(g), B(g))$ is an isomorphism ([3], Theorem 3.4, page 52) where $(B(g))^o$ is the opposite algebra of $B(g)$, $f(a\otimes b)(x) = axb$ for each $a\otimes b \in B(g)\otimes_Z (B(g))^o$ and each $x \in B(g)$. By denoting the left multiplication map with $a \in B(g)$ by a_l and the right multiplication map with $b \in B(g)$ by b_r, $f(a \otimes b)(x) = axb = (a_l b_r)(x)$. Since $B(g) = \oplus \sum_{k\in K(g)} e_g J_k$, $B(g) \otimes_Z (B(g))^o \cong \sum_{k\in K(g)} (B(g))_l (J_k)_r$. Observing that $(J_k)_r = (J_k)_l \overline{k}^{\,-1}$ where $\overline{k} = kL \in U(g) = K(g)/L$, we have that $B(g) \otimes_Z$

$(B(g))^o \cong \sum_{k\in K(g)}(B(g))_l(J_k)_r = \sum_{k\in K(g)}(B(g))_l(J_k)_l\overline{k}^{\,-1} = \sum_{k\in K(g)}(B(g)J_k)_l\overline{k}^{\,-1}$. Moreover, since $B(g) = \oplus\sum_{h\in K(g)} e_gJ_h$ and $e_ge_h = e_g$ for each $h \in K(g)$, $B(g)J_k = \oplus\sum_{h\in K(g)} e_gJ_hJ_k = \oplus\sum_{h\in K(g)} e_ge_hJ_{hk} = \oplus\sum_{h\in K(g)} e_gJ_{hk} = B(g)$ for each $k \in K(g)$. Therefore $B(g)\otimes_Z (B(g))^o \cong \sum_{k\in K(g)}(B(g)J_k)_l\overline{k}^{\,-1} = \sum_{k\in K(g)}(B(g))_l\overline{k}^{\,-1}$
$= (B(g))_lU(g)$. Consequently $(B(g))_lU(g) \cong \mathrm{Hom}_Z(B(g), B(g))$. This completes the proof.

COROLLARY 4.3.

By keeping the notations of Theorem 4.2, $B = \sum_{g\in G} B(g)$, a sum of central weakly Galois algebras.

PROOF. Since B is a Galois algebra with Galois group G, $B = \oplus\sum_{g\in G} J_g$ ([5], Theorem 1). But $B(g)$ is generated by $\{J_h \,|\, h \in S(g)\}$ which contains J_g, so $J_g \subset B(g)$ for each $g \in G$. Thus $B = \sum_{g\in G} B(g)$ such that $B(g)$ is a central weakly Galois algebra by Theorem 4.2.

We recall that a Galois extension A with Galois group G is called an Azumaya Galois extension if A^G is an Azumaya algebra over C^G where C is the center of A. We define a weakly Galois extension A with Galois group G a weakly Azumaya Galois extension if A^G is an Azumaya algebra over C^G. As a consequence of Theorem 4.2, $B(g)(B(g))^{K(g)}$ can be shown to be a weakly Azumaya Galois extension with Galois group $U(g)$.

COROLLARY 4.4.

$\big(B(g)\big)(e_gB)^{K(g)}$ is a weakly Azumaya Galois extension of $(e_gB)^{K(g)}$ with Galois group $U(g) = K(g)/L$.

PROOF. By Theorem 4.2, $(B(g))_lU(g) \cong \mathrm{Hom}_Z(B(g), B(g))$, so

$$\begin{aligned}\big((B(g))(e_gB)^{K(g)}\big)_lU(g) &\cong \mathrm{Hom}_Z(B(g), B(g))(e_gB)^{K(g)}\\ &\cong \mathrm{Hom}_Z(B(g), B(g)) \otimes_Z (e_gB)^{K(g)}\\ &\cong \mathrm{Hom}_{(e_gB)^{K(g)}}(B(g)\otimes_Z (e_gB)^{K(g)}, B(g)\otimes_Z (e_gB)^{K(g)}).\end{aligned}$$

Moreover, by the proof of Theorem 3.6, $B(g)$ and $(e_gB)^{K(g)}$ are Azumaya algebras over Z, so it is easy to see that $\big(B(g)\big)(e_gB)^{K(g)} \cong B(g)\otimes_Z(e_gB)^{K(g)}$ which is a finitely generated projective module over $(e_gB)^{K(g)}$. Thus $\big(B(g)\big)(e_gB)^{K(g)}$ is a weakly Azumaya Galois extension of $(e_gB)^{K(g)}$ with Galois group $U(g)=K(g)/L$.

Next we characterize a Galois extension $B(g)$ with Galois group $U(g)$.

THEOREM 4.5.

The following statements are equivalent:

(1) $B(g)$ is a central Galois algebra with Galois group $U(g)$.

(2) $B(g)$ is a Galois extension with Galois group $U(g)$.

(3) $J_{\overline{k}}^{(B(g))} = \oplus\sum_{l\in L} e_gJ_{kl}$ for each $\overline{k}\in U(g)$.

PROOF. (1) $\Longrightarrow$ (2) is clear.

(2) $\Longrightarrow$ (1) is a consequence of Lemma 4.1.

(1) $\Longrightarrow$ (3) Let $B(g)$ be a central Galois algebra with Galois group $U(g)$. Then $B(g)=\oplus\sum_{\overline{k}\in U(g)} J_{\overline{k}}^{(B(g))}$ ([5], Theorem 1). Next it is easy to check that $\oplus\sum_{l\in L} e_gJ_{kl}\subset J_{\overline{k}}^{(B(g))}$ for each $k\in K(g)$. But $B(g)=\oplus\sum_{k\in K(g)} e_gJ_k$ by Theorem 3.4, so $\oplus\sum_{k\in K(g)} e_gJ_k = \oplus\sum_{\overline{k}\in U(g)} J_{\overline{k}}^{(B(g))}$ (by Lemma 3.3) such that $\oplus\sum_{l\in L} e_gJ_{kl}\subset J_{\overline{k}}^{(B(g))}$. Thus $J_{\overline{k}}^{(B(g))} = \oplus\sum_{l\in L} e_gJ_{kl}$ for each $\overline{k}\in U(g)$.

(3) $\Longrightarrow$ (1) Since $J_{\overline{k}}^{(B(g))} = \oplus\sum_{l\in L} e_gJ_{kl}$ for each $\overline{k}\in U(g)$,

$$B(g)=\oplus\sum_{k\in K(g)} e_gJ_k=\oplus\sum_{\overline{k}\in U(g)} J_{\overline{k}}^{(B(g))}.$$

Moreover, by Lemma 4.1, $(B(g))^{K(g)}=Z$, so $U(g)$ is an Z-automorphism group of $B(g)$. But then it is well known that $J_{\overline{k}}^{(B(g))}J_{\overline{k}^{-1}}^{(B(g))}=Z$ for each $\overline{k}\in U(g)$. Thus $B(g)$ is a central Galois algebra with Galois group $U(g)$ ([4], Theorem 1) for $B(g)$ is an Azumaya algebra over Z by Theorem 3.6.

5. A ONE-TO-ONE CORRESPONDENCE

In this section we shall establish a one-to-one correspondence between the set of algebras $\{B(g) \mid g \in G\}$ and the set of subgroups $\{K(g) \mid g \in G\}$, and give three remarkable characterizations of a Galois extension due to the first author.

LEMMA 5.1.

Let $\alpha : e_g \longrightarrow K(g)$. Then α is a bijection between $\{e_g \mid g \in G\}$ and $\{K(g) \mid g \in G\}$.

PROOF. Assume that $K(g) = K(h)$ for some $g, h \in G$. Since $h \in K(h)$, $h \in K(g)$. Hence $e_g = e_g e_h$ by Lemma 3.5. Similarly, $e_h = e_g e_h$. Thus $e_g = e_h$; and so α is one-to-one. Clearly, α is onto. Therefore α is a bijection.

LEMMA 5.2.

Let $\beta : e_g \longrightarrow B(g)$. Then β is a bijection between $\{e_g \mid g \in G\}$ and $\{B(g) \mid g \in G\}$.

PROOF. Assume that $B(g) = B(h)$ for some $g, h \in G$. If $B(g) = B(h) = \{0\}$, then $e_g = 0 = e_h$. If $B(g) = B(h) \neq \{0\}$, noting that $e_g \in e_g C = e_g J_1 \subset \oplus \sum_{k \in K(g)} e_g J_k = B(g)$ by Theorem 3.4, we have that e_g is the identity of $B(g)$ and e_h is the identity of $B(h)$. Hence $e_g = e_h$. Thus β is one-to-one. Clearly, β is onto. Therefore β is a bijection.

Lemma 5.1 and Lemma 5.2 imply a one-to-one correspondence between $\{B(g) \mid g \in G\}$ and $\{K(g) \mid g \in G\}$.

THEOREM 5.3.

Let $\phi : K(g) \longrightarrow B(g)$. Then ϕ is a bijection between $\{K(g) \mid g \in G\}$ and $\{B(g) \mid g \in G\}$.

PROOF. By Lemma 5.1 and Lemma 5.2, $\phi = \beta\alpha^{-1}$ is a bijection.

We conclude the present paper with two interesting equivalent conditions for a Galois extension of a ring and a characterization of a Galois extension of a field. Let L be a ring with a finite automorphism group G, $K = L^G$, and R the endomorphism ring of the right K-module L. Then L can be regarded as a two-sided R-K-module. For each $a \in L$, denote by $\overline{a}$ the mapping $x \longrightarrow ax$ $(x \in L)$. Then $\overline{a}$ is an endomorphism of L_K, i.e., $\overline{a} \in R$, and the mapping $a \longrightarrow \overline{a}$ an isomorphism from L into R. Let $\overline{L}$ be the image of L by this isomorphism. Let σ be any element in G. Then σ is in R, because $(ax)^\sigma = a^\sigma x^\sigma = a^\sigma x$ for every $a \in L$ and $x \in K$. Moreover, we have $(\sigma\overline{a})b = \sigma(ab) = (ab)^\sigma = a^\sigma b^\sigma = (\overline{a^\sigma}\sigma)b$ for any $a, b \in L$, which shows that $\sigma\overline{a} = \overline{a^\sigma}\sigma$ for any $a \in L$ and in particular $\sigma\overline{L} = \overline{L}\sigma$. Now L is called a Galois extension of K relative to G if the right K-module L is finitely generated and projective and $R = \sum_{\sigma \in G} \oplus \sigma\overline{L}$. Thus, without using the crossed product of L and G with trivial factor set, a Galois extension is characterized.

THEOREM A.

The following are equivalent:

A. L is a Galois extension of K relative to G.

B. There exist $x_1, \cdots, x_n$; $y_1, \cdots, y_n$ in L such that

$$\sum_{i=1}^{n} x_i y_i^\sigma = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$$

PROOF. First we prove that A implies B: Assume A. Then L_K is finitely generated and projective, which means the existence of finite number of $x_i \in L$ and homomorphism $\phi_i : L_K \longrightarrow K_K$ $(i = 1, 2, \ldots, n)$ such that $\sum_{i=1}^n x_i \phi_i(x) = x$ for all $x \in L$. Since $K \subset L$, each ϕ_i is an endomorphism of L_K, i.e., $\phi_i \in R$. Then the above equality can be written as $(\sum_{i=1}^n \overline{x}_i \phi_i)x = x$ for all $x \in L$. But this means the following equality: $\sum_{i=1}^n \overline{x}_i \phi_i = 1$. Since $R = \sum_{\sigma \in G} \sigma\overline{L}$ by assumption A, each ϕ_i can be expressed as $\phi_i = \sum_{\sigma \in G} \sigma\overline{y}_{i,\sigma}$ with $y_{i,\sigma} \in L$ $(1 \leq i \leq n,\ \sigma \in G)$. On the other hand, since $\phi_i x \in K$ for every $x \in L$, it follows that $\phi_i x = \tau(\phi_i x) = (\tau\phi_i)x$ for every $\tau \in G$ and $x \in L$ and hence $\phi_i = \tau\phi_i = \sum_{\sigma \in G} \tau\sigma\overline{y}_{i,\sigma}$ for every $\tau \in G$. Since R is a direct sum of $\sigma\overline{L}$ $(\sigma \in G)$, this implies that $y_{i,\tau\sigma} = y_{i,\sigma}$ for every σ, τ in G and hence $y_{i,\sigma}$ is independent of σ and depends only on i. Therefore we can write $y_i = y_{i,\sigma}$ for every σ, so that we have $\phi_i = (\sum_{\sigma \in G} \sigma)\overline{y}_i$. It follows then $1 = \sum_{i=1}^n \overline{x}_i \phi_i = \sum_{i=1}^n \overline{x}_i (\sum_{\sigma \in G} \sigma)\overline{y}_i = \sum_{\sigma \in G}(\sum_{i=1}^n \overline{x}_i \overline{y_i^\sigma})\sigma$. From this we can conclude that $1 = \sum_{i=1}^n x_i y_i$ and $0 = \sum_{i=1}^n x_i y_i^\sigma$ if $\sigma \neq 1$.

Next we assume B. Let $\phi_i = (\sum_{\sigma\in G}\sigma)\overline{y}_i$ for each i $(1 \le i \le n)$. Then ϕ_i is in R and satisfies $\sum_{i=1}^n \overline{x}_i\phi_i = \sum_{i=1}^n \overline{x}_i(\sum_{\sigma\in G}\sigma)\overline{y}_i = \sum_{\sigma\in G}(\sum_{i=1}^n \overline{x}_i\overline{y_i^\sigma})\sigma = 1$. This implies that $\sum_{i=1}^n x_i\phi_i(x) = \sum_{i=1}^n x_i(\phi_i x) = (\sum_{i=1}^n \overline{x}_i\phi_i)x = x$ for every $x \in L$. Moreover, $\phi_i(x) = (\sum_{\sigma\in G}\sigma)(y_i x)$ for every $x \in L$ and so for any $\tau \in G$ we have $\phi_i(x)^\tau = \tau(\sum_{\sigma\in G}\sigma)(y_i x) = (\sum_{\sigma\in G}\tau\sigma)(y_i x) = (\sum_{\sigma\in G}\sigma)(y_i x)$ whence $\phi_i(x)^\tau = \phi_i(x)$ for every $x \in L$ and $\tau \in G$. Thus we know that $\phi_i(x)$ is in $L^G = K$ for every $x \in L$, i.e., ϕ_i is a homomorphism $L_K \longrightarrow K_K$ and therefore L_K is finitely generated and projective.

Let α be any endomorphism of L_K, i.e., $\alpha \in R$. Then we have $(\sum_{i=1}^n \overline{\alpha x_i}\phi_i)x = \sum_{i=1}^n \overline{\alpha x_i}\phi_i(x) = \sum_{i=1}^n (\alpha x_i)\phi_i(x)$. But $\phi_i(x) \in K$, we have

$$\sum_{i=1}^n (\alpha x_i)\phi_i(x) = \sum_{i=1}^n \alpha(x_i\phi_i(x)) = \alpha\sum_{i=1}^n x_i\phi_i(x) = \alpha x.$$

Thus we have $\sum_{i=1}^n \overline{\alpha x_i}\phi_i = \alpha$. Since $\phi_i \in \sum_{\sigma\in G}\sigma\overline{L}$, this means that $\alpha \in \sum_{\sigma\in G}\sigma\overline{L}$. Therefore we know that $R = \sum_{\sigma\in G}\sigma\overline{L}$. Let $\sum_{\sigma\in G}\overline{a}_\sigma\sigma$ be any linear combination of $\sigma \in G$ with $a_\sigma \in L$. Then for each $\tau \in G$ we have $\sum_{i=1}^n(\sum_{\sigma\in G}\overline{a}_\sigma\sigma x_i)y_i^\tau = \sum_{i=1}^n(\sum_{\sigma\in G}a_\sigma x_i^\sigma)y_i^\tau$ $= \sum_{\sigma\in G}a_\sigma\sum_{i=1}^n x_i^\sigma y_i^\tau = \sum_{\sigma\in G}a_\sigma(\sum_{i=1}^n x_i y_i^{\tau\sigma^{-1}})^\sigma = a_\tau$ because

$$\sum_{i=1}^n x_i y_i^{\tau\sigma^{-1}} = \begin{cases} 1, & \text{if } \sigma = \tau \\ 0, & \text{if } \sigma \neq \tau. \end{cases}$$

Therefore if $\sum_{\sigma\in G}\overline{a}_\sigma\sigma = 0$, then it follows $a_\tau = 0$ for every $\tau \in G$, which shows that R is a direct sum of $\overline{L}\sigma = \sigma\overline{L}$, i.e., $R = \sum_{\sigma\in G}\oplus\sigma\overline{L}$. Thus L is a Galois extension of K relative to G.

Next, consider L as a left K-module and let S be the endomorphism ring of ${}_KL$. Then L can be regarded as a two-sided K-S-module. For each $a \in L$, denote by $\underline{a}$ the mapping $x \longrightarrow xa$ $(x \in L)$. Then $\underline{a}$ is an endomorphism of ${}_KL$, i.e., $\underline{a} \in S$, and the mapping $a \longrightarrow \underline{a}$ an isomorphism from L into S. Let $\underline{L}$ be the image of L by this isomorphism, so that $\underline{L}$ $(\cong L)$ is a subring of S and $\underline{a}\sigma = \sigma\underline{a^\sigma}$ for each $\sigma \in G$ and $a \in L$. Now L is called a left Galois extension of K relative to G if L as a left K-module is finitely generated and projective and $S = \sum_{\sigma\in G}\oplus\sigma\underline{L}$. Then it can be shown that a left Galois extension and a Galois extension are the same.

THEOREM B.

The following are equivalent:

A. L is a Galois extension of K relative to G.

A_l. L is a left Galois extension of K relative to G.

PROOF. First we prove that A_l implies A: Assume A_l. Then ${}_K L$ is finitely generated and projective, i.e., there exist finite number of $y_i \in L$ and homomorphism $\psi_i : {}_K L \longrightarrow {}_K K$ $(i = 1, 2, \ldots, n)$ such that $\sum_{i=1}^n \psi_i(x) y_i = x$ for all $x \in L$. But since $K \subset L$, each ψ_i is an endomorphism of ${}_K L$, i.e., $\psi_i \in S$. Then we have $x \sum_{i=1}^n \psi_i \underline{y}_i = \sum_{i=1}^n \psi_i(x) y_i = x$ for all $x \in L$, which shows that $\sum_{i=1}^n \psi_i \underline{y}_i = 1$. On the other hand, each ψ_i is in $S = \sum_{\sigma \in G} \sigma \underline{L}$ and therefore it is expressed as $\psi_i = \sum_{\sigma \in G} \underline{x}_{i,\sigma} \sigma$ with $x_{i,\sigma} \in L$ $(1 \leq i \leq n,\ \sigma \in G)$. Since $x\psi_i = \psi_i(x) \in K$ for every i and $x \in L$, we have that $x(\psi_i \tau) = \psi_i(x)\tau = \psi_i(x) = x\psi_i$ for every i, $\tau \in G$ and $x \in L$, and thus $\psi_i \tau = \psi_i$ for every i and $\tau \in G$. But since $\psi_i \tau = \sum_{\sigma \in G} \underline{x}_{i,\sigma} \sigma\tau$ for every $\tau \in G$ and S is a direct sum of $\sigma \underline{L}$ $(\sigma \in G)$, we know that $x_{i,\tau\sigma} = x_{i,\sigma}$ for every i and σ, τ in G and therefore $x_{i,\sigma}$ is independent of $\sigma \in G$, which means that if we put $x_i = x_{i,1}$ then $x_i = x_{i,\sigma}$ for every $\sigma \in G$. Thus we have $\psi_i = \underline{x}_i \sum_{\sigma \in G} \sigma$ and therefore

$$1 = \sum_{i=1}^n \psi_i \underline{y}_i = \sum_{i=1}^n \underline{x}_i \Big(\sum_{\sigma \in G} \sigma\Big) \underline{y}_i = \sum_{\sigma \in G} \sigma \sum_{i=1}^n (\underline{x_i^\sigma y_i}) = \sum_{\sigma \in G} \sigma \underline{\sum_{i=1}^n x_i^\sigma y_i}.$$

Since S is a direct sum of $\sigma \underline{L}$ $(\sigma \in G)$, it follows that $\sum_{i=1}^n x_i^\sigma y_i = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1 \end{cases}$ and therefore $\sum_{i=1}^n x_i y_i^\sigma = (\sum_{i=1}^n x_i^{\sigma^{-1}} y_i)^\sigma = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$ Thus the condition B of Theorem A holds. Therefore by Theorem A we have the condition A.

Next we want to prove that A implies A_l: Assume A. Then by Theorem A, there exist $x_1, \cdots, x_n$; $y_1, \cdots, y_n$ in L such that

$$\sum_{i=1}^n x_i y_i^\sigma = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$$

Then we have

$$\sum_{i=1}^n x_i^\sigma y_i = \Big(\sum_{i=1}^n x_i y_i^{\sigma^{-1}}\Big)^\sigma = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$$

Let $\psi_i = \underline{x}_i \sum_{\sigma\in G} \sigma$ for each i $(1 \le i \le n)$. Then ψ_i is in S and satisfies $\sum_{i=1}^n \psi_i \underline{y}_i = \sum_{i=1}^n \underline{x}_i (\sum_{\sigma\in G} \sigma) \underline{y}_i = \sum_{\sigma\in G} \sigma \sum_{i=1}^n \underline{x}_i^\sigma \underline{y}_i = 1$. Therefore we have

$$\sum_{i=1}^n \psi_i(x) y_i = \sum_{i=1}^n (x\psi_i) y_i = x \sum_{i=1}^n \psi_i \underline{y}_i = x \quad \text{for every } x \in L.$$

Furthermore, $\psi_i(x)^\tau = (x\psi_i)^\tau = (x\underline{x}_i \sum_{\sigma\in G} \sigma)^\tau = x(\underline{x}_i \sum_{\sigma\in G} \sigma\tau) = x\underline{x}_i \sum_{\sigma\in G} \sigma = x\psi_i = \psi_i(x)$ for every $x \in L$ and $\tau \in G$ and this implies that $\psi_i(x)$ is in $L^G = K$ for every $x \in L$ and thus ψ_i is a homomorphism ${}_K L \longrightarrow {}_K K$. This shows that ${}_K L$ is finitely generated and projective.

The rest part of the proof is similar to the proof for the implication $B \Longrightarrow A$ of Theorem A. Namely, let β be any endomorphism of ${}_K L$, i.e., $\beta \in S$. Then we have $x(\sum_{i=1}^n \psi_i \underline{y_i \beta}) = \sum_{i=1}^n \psi_i(x)(y_i\beta) = (\sum_{i=1}^n \psi_i(x) y_i)\beta = x\beta$ for every $x \in L$, and thus we know that $\sum_{i=1}^n \psi_i \underline{y_i \beta} = \beta$. Since $\psi_i \in \sum_{\sigma\in G} \sigma\underline{L}$, it follows that $\beta \in \sum_{\sigma\in G} \sigma\underline{L}$, which shows that $S = \sum_{\sigma\in G} \sigma\underline{L}$. Next let $\sum_{\sigma\in G} \sigma\underline{a}_\sigma$ be any linear combination of $\sigma \in G$ with coefficients $\underline{a}_\sigma \in \underline{L}$. Then we have, for each $\tau \in G$, $\sum_{i=1}^n x_i^\tau (y_i (\sum_{\sigma\in G} \sigma\underline{a}_\sigma)) = \sum_{i=1}^n x_i^\tau \sum_{\sigma\in G} y_i^\sigma a_\sigma = \sum_{\sigma\in G} (\sum_{i=1}^n x_i^\tau y_i^\sigma) a_\sigma = \sum_{\sigma\in G} (\sum_{i=1}^n x_i^{\tau\sigma^{-1}} y_i)^\sigma a_\sigma = a_\tau$ because $\sum_{i=1}^n x_i^{\tau\sigma^{-1}} y_i = 1$ if $\sigma = \tau$ and $= 0$ if $\sigma \ne \tau$. Therefore it follows that $\sum_{\sigma\in G} \sigma\underline{a}_\sigma = 0$, then $a_\sigma = 0$ for every $\sigma \in G$. Thus we know that S is a direct sum of $\sigma\underline{L}$ $(\sigma \in G)$, i.e., $S = \sum_{\sigma\in G} \oplus \sigma\underline{L}$. This completes the proof of our theorem.

THEOREM C.

Let L be a (commutative) field and G a finite group of automorphism of L and let $K = L^G$. Then K is a subfield of L and $[L : K] = n$, where n is the order of G, and moreover L is a Galois extension of K relative to G.

PROOF. I. First we prove that $[L : K] = n$. Let a be any element of L and let $G(a) = \{\sigma \in G \,|\, a^\sigma = a\}$. Then $G(a)$ is a subgroup of G. Let $n(a) = (G : G(a))$. Then $n(a) \big| n$ whence $n(a) \le n$. Let σ, τ be in G. Then $a^\sigma = a^\tau$ if and only if $a^{\sigma\tau^{-1}} = a$, i.e., $\sigma\tau^{-1} \in G(a)$, i.e., $G(a)\sigma = G(a)\tau$. Let $\sigma_1, \sigma_2, \ldots, \sigma_{n(a)}$ be in G such that $G(a)\sigma_1, G(a)\sigma_2, \ldots, G(a)\sigma_{n(a)}$ are all distinct right cosets of G mod $G(a)$. Then for each

$\sigma \in G$ $G(a)\sigma_1\sigma$, $G(a)\sigma_2\sigma$, $\ldots$, $G(a)\sigma_{n(a)}\sigma$ are all distinct right cosets of G mod $G(a)$. Consider now a polynomial $f(x) = (x - a^{\sigma_1})(x - a^{\sigma_2})\cdots(x - a^{\sigma_{n(a)}})$ over L. Then for each $\sigma \in G$ we have $f(x)^\sigma = (x - a^{\sigma_1\sigma})(x - a^{\sigma_2\sigma})\cdots(x - a^{\sigma_{n(a)}\sigma}) = f(x)$. Therefore $f(x)$ is a polynomial over K and of degree $n(a)$. Let $G(a)\sigma_e = G(a)$, i.e., $\sigma_e \in G(a)$. Then $a^{\sigma_e} = a$. This implies that $f(a) = 0$. Let $g(x)$ be a polynomial over K such that $g(a) = 0$. Then we have $g(a^{\sigma_1}) = g(a)^{\sigma_1} = 0$. Therefore $g(x) = (x - a^{\sigma_1})g_1(x)$ with a polynomial $g_1(x)$ over L. Next we have $(a^{\sigma_2} - a^{\sigma_1})g_1(a^{\sigma_2}) = g(a^{\sigma_2}) = g(a)^{\sigma_2} = 0$. But $a^{\sigma_1} \neq a^{\sigma_2}$, i.e., $a^{\sigma_2} - a^{\sigma_1} \neq 0$, we have that $g_1(a^{\sigma_2}) = 0$ and therefore $g_1(x) = (x-a^{\sigma_2})g_2(x)$ with a polynomial $g_2(x)$ over L. Thus we have $g(x) = (x-a^{\sigma_1})(x-a^{\sigma_2})g_2(x)$. Similarly, by considering $\sigma_2, \ldots, \sigma_{n(a)}$, we have a polynomial $g_{n(a)}(x)$ over L such that $g(x) = (x - a^{\sigma_1})(x - a^{\sigma_2})\cdots(x - a^{\sigma_{n(a)}})g_{n(a)}(x) = f(x)g_{n(a)}(x)$. Thus $f(x)$ is a minimal polynomial of a over k, which shows that $[K(a) : K] = n(a)$ and a is separable over K for every $a \in L$.

Now since $n(a) \leq n$ for every $a \in L$, we can choose $u \in L$ such that $n(u)$ is maximal, i.e., $n(a) \leq n(u)$ for every $a \in L$. Let a be any element of L, and consider $K(a, u)$. Then $K(a, u)$ is a finite whence separable extension of K, and therefore as is well known there exists a $b \in L$ such that $K(b) = K(a, u)$. It follows that $K(u) \subset K(b)$ whence $n(u) \leq n(b)$. But the maximality of $n(u)$ implies that $n(u) = n(b)$ whence $K(u) = K(b)$. Thus we know that $a \in K(u)$ for every $a \in L$, which means that $L = K(u)$ and so $[L : K] = n(u)$. Let now σ be any element of $G(u)$. Then $u^\sigma = u$ whence $a^\sigma = a$ for every $a \in L$, i.e., σ is the identity automorphism. Thus we know that $n(u) = n$ and so $[L : K] = n$.

By using this we shall prove

II. L is a Galois extension of K relative to G: First L is a finite extension of K, L_K is finitely generated. Next since K is a field, every K-module and in particular L_K is projective. Let R be the endomorphism ring of L_K and we regard L as a left R-module. For each $l \in L$, we denote by $\bar{l}$ the mapping $x \longmapsto lx$ $(x \in L)$. Then $\bar{l}$ is an endomorphism of L_K, and the mapping $l \longmapsto \bar{l}$ is a ring isomorphism of L into R. We denote by $\overline{L}$ the image of L by this isomorphism. Similarly we denote by $\overline{K}$ the image of the subfield

K of L. Now let α be any endomorphism of L_K, i.e., $\alpha \in R$. Let a and l be any elements of K and L respectively. Then by using the commutativity of the field L we have $(\overline{a}\alpha)l = \overline{a}(\alpha l) = a(\alpha l) = (\alpha l)a = \alpha(la) = \alpha(al) = \alpha(\overline{a}l) = (\alpha\overline{a})l$, which shows that $\overline{a}\alpha = \alpha\overline{a}$, i.e., $\overline{a}$ is whence $\overline{K}$ is in the center of R.

Let $(\, l_1 \quad l_2 \quad \ldots \quad l_n \,)$ be any vector of length n with l_i $(i = 1, 2, \ldots, n)$ in L and α an endomorphism of L_K. Then we define

$$\alpha\,(\, l_1 \quad l_2 \quad \ldots \quad l_n \,) = (\, \alpha l_1 \quad \alpha l_2 \quad \ldots \quad \alpha l_n \,).$$

Let β be another endomorphism of L_K. Then we can see that

$$\begin{aligned} \alpha\beta\,(\, l_1 \quad l_2 \quad \ldots \quad l_n \,) &= (\, \alpha\beta l_1 \quad \alpha\beta l_2 \quad \ldots \quad \alpha\beta l_n \,) \\ &= \alpha\,(\, \beta l_1 \quad \beta l_2 \quad \ldots \quad \beta l_n \,) \\ &= \alpha(\beta\,(\, l_1 \quad l_2 \quad \ldots \quad l_n \,)). \end{aligned}$$

Let u_1, u_2, …, u_n be a linearly independent basis of L_K. Let α be an endomorphism of L_K. Then for each j, αu_j is expressed as $\alpha u_j = \sum u_i a_{ij}$ with $a_{ij} \in K$. Then if we put A as the $n \times n$ matrix whose (i, j)-component is a_{ij}, we have $(\, \alpha u_1 \quad \alpha u_2 \quad \ldots \quad \alpha u_n \,) = (\, u_1 \quad u_2 \quad \ldots \quad u_n \,)\, A$. Since u_1, u_2, …, u_n are linearly independent over K, A is uniquely determined by α. Thus by associating α with A we have a mapping φ from R into the set $[K]_n$ of all $n \times n$ matrices over K. Let conversely A be an $n \times n$ matrix over K. Let l be any element of L. Then $l = (\, u_1 \quad u_2 \quad \ldots \quad u_n \,) \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ with a unique vector $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ in K. Then by associating l with $(\, u_1 \quad u_2 \quad \ldots \quad u_n \,)\, A \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ we have an endomorphism α. Since $u_1 = (\, u_1 \quad u_2 \quad \ldots \quad u_n \,) \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $u_2 = (\, u_1 \quad u_2 \quad \ldots \quad u_n \,) \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, …, $u_n = (\, u_1 \quad u_2 \quad \ldots \quad u_n \,) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$, we know that

$$(\,\alpha u_1 \quad \alpha u_2 \quad \ldots \quad \alpha u_n\,) = (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,A \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$
$$= (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,A.$$

This shows that φ is a mapping from R onto $[K]_n$. Let α, β be in R and let $\varphi(\alpha) = A$, $\varphi(\beta) = B$, i.e., $\alpha\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) = (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,A$, $\beta\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) = (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,B$. Assume $\varphi(\alpha) = \varphi(\beta)$, i.e., $A = B$. Then it follows that

$$\alpha\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) = \beta\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,.$$

Since u_1, u_2, $\ldots$, u_n are basis of L_K, this implies that $\alpha = \beta$. Thus we know that φ is a one-to-one mapping from R onto $[K]_n$. Let again α, β be in R and let $\varphi(\alpha) = A$, $\varphi(\beta) = B$. Then

$$\begin{aligned}(\alpha+\beta)\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) &= \alpha\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) + \beta\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) \\ &= (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,A + (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,B \\ &= (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,(A+B).\end{aligned}$$

Thus $\varphi(\alpha+\beta) = A + B$. Furthermore,

$$\begin{aligned}(\alpha\beta)\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) &= \alpha(\beta\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,)) = \alpha\big(\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,B\big) \\ &= \alpha\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,B = (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,AB,\end{aligned}$$

which shows that $\varphi(\alpha\beta) = AB$. Therefore φ is a ring isomorphism from R onto $[K]_n$. Let a be any element of K. Then

$$\begin{aligned}\overline{a}\,(\,u_1 \quad u_2 \quad \ldots \quad u_n\,) &= (\,au_1 \quad au_2 \quad \ldots \quad au_n\,) = (\,u_1a \quad u_2a \quad \ldots \quad u_na\,) \\ &= (\,u_1 \quad u_2 \quad \ldots \quad u_n\,)\,aE\end{aligned}$$

where E is the identity matrix, i.e., the $n \times n$ matrix whose (i,i)-components $(1 \leq i \leq n)$ are 1 and other components are all 0. Thus we know that $\varphi(\overline{a}) = aE$ whence $\varphi(\overline{K}) = KE$. Let for each pair (i,j) with $1 \leq i,j \leq n$ E_{ij} be the $n \times n$ matrix whose (i,j)-component is 1 and other components are all 0. Then each $A \in [K]_n$ whose (i,j)-component is a_{ij}

($\in K$) can be expressed as $A = \sum a_{ij}E_{ij}$. This implies that E_{ij} $(1 \leq i, j \leq n)$ are linearly independent basis of $[K]_n$ over K. Thus the dimension of $[K]_n$ over K is n^2. Since $aA = aEA$ for every $a \in K$ and $A \in [K]_n$, this implies that $\big[[K]_n : KE\big] = n^2$. Therefore we know that $[R : \overline{K}] = n^2$.

Let σ be any element of G. Then σ is in R, because $(lk)^\sigma = l^\sigma k^\sigma = l^\sigma k$ for every $l \in L$ and $k \in K$. Moreover, we have $(\sigma\bar{l})l' = \sigma(ll') = (ll')^\sigma = l^\sigma l'^\sigma = (\overline{l^\sigma}\sigma)l'$ for every $l, l' \in L$, which shows that $\sigma\bar{l} = \overline{l^\sigma}\sigma$ for any $l \in L$ and in particular $\sigma\overline{L} = \overline{L}\sigma$. Therefore $\overline{L}\sigma$ can be regarded as a two-sided $\overline{L}$-module ${}_{\overline{L}}\overline{L}\sigma_{\overline{L}}$. Let τ be another element of G such that $\overline{L}\sigma$ and $\overline{L}\tau$ are isomorphic as two-sided $\overline{L}$-modules. Let μ be the isomorphism and $\mu(\sigma) = \bar{a}\tau$ with $a \in L$ ($a \neq 0$ because $\sigma \neq 0$). Then for every $l \in L$ $\mu(\sigma\bar{l}) = \bar{a}\tau\bar{l} = \bar{a}\overline{l^\tau}\tau$. But since $\sigma\bar{l} = \overline{l^\sigma}\sigma$, we also have $\mu(\sigma\bar{l}) = \overline{l^\sigma}\bar{a}\tau$. It follows then that $al^\tau = l^\sigma a$ whence $l^\tau = l^\sigma$ for every $l \in L$, i.e., $\sigma = \tau$.

Now, since L is a field, the left $\overline{L}$-module ${}_{\overline{L}}\overline{L}$ is simple and therefore the two-sided $\overline{L}$-module ${}_{\overline{L}}\overline{L}\sigma_{\overline{L}}$ is simple for every $\sigma \in G$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all distinct elements of G. Then if $i \neq j$, the corresponding ${}_{\overline{L}}(\overline{L}\sigma_i)_{\overline{L}}$ and ${}_{\overline{L}}(\overline{L}\sigma_j)_{\overline{L}}$ are not isomorphic. Consider now $S = \overline{L}\sigma_1 + \overline{L}\sigma_2 + \cdots + \overline{L}\sigma_n$. Then S is a two-sided $\overline{L}$-submodule of R. We want to show that $S = \overline{L}\sigma_1 \oplus \overline{L}\sigma_2 \oplus \cdots \oplus \overline{L}\sigma_n$. For the proof, consider first $\overline{L}\sigma_1 \cap \overline{L}\sigma_2$. If $\overline{L}\sigma_1 \cap \overline{L}\sigma_2 \neq 0$, then this is a non-zero submodule of $\overline{L}\sigma_1$ and $\overline{L}\sigma_2$. But since both ${}_{\overline{L}}(\overline{L}\sigma_1)_{\overline{L}}$ and ${}_{\overline{L}}(\overline{L}\sigma_2)_{\overline{L}}$ are simple, it follows that $\overline{L}\sigma_1 \cap \overline{L}\sigma_2$ is equal to $\overline{L}\sigma_1$ and to $\overline{L}\sigma_2$ whence $\overline{L}\sigma_1 = \overline{L}\sigma_2$. But this contradicts to that $\sigma_1 \neq \sigma_2$. Thus we have that $\overline{L}\sigma_1 \cap \overline{L}\sigma_2 = 0$ whence $\overline{L}\sigma_1 + \overline{L}\sigma_2 = \overline{L}\sigma_1 \oplus \overline{L}\sigma_2$. Consider next $S_r = \overline{L}\sigma_1 + \overline{L}\sigma_2 + \cdots + \overline{L}\sigma_r$ with $1 < r < n$ and assume that $S_r = \overline{L}\sigma_1 \oplus \overline{L}\sigma_2 \oplus \cdots \oplus \overline{L}\sigma_r$. Let P_i $(i = 1, 2, \ldots, r)$ be the projection from S_r to $\overline{L}\sigma_i$. Now suppose $S_r \cap \overline{L}\sigma_{r+1} \neq 0$. Then since this is a non-zero submodule of the simple two-sided module $\overline{L}\sigma_{r+1}$, this coincides with $\overline{L}\sigma_{r+1}$, i.e., $\overline{L}\sigma_{r+1} \subset S_r$. Then there must be a P_i such that P_i maps $\overline{L}\sigma_{r+1}$ isomorphically onto $\overline{L}\sigma_i$. Then this contradicts to that $\sigma_i \neq \sigma_{r+1}$. Thus $S_r \cap \overline{L}\sigma_{r+1} = 0$ whence $S_r + \overline{L}\sigma_{r+1} = S_r \oplus \overline{L}\sigma_{r+1}$. By applying this for $r = 2, \ldots, n-1$ we know that $S = \overline{L}\sigma_1 \oplus \overline{L}\sigma_2 \oplus \cdots \oplus \overline{L}\sigma_n$.

Since we have proved that $[L : K] = n$ in I and ${}_{\overline{L}}\overline{L}\sigma_i \cong_{\overline{L}} \overline{L}$ for every i $(1 \leq i \leq n)$, it follows that $[\overline{L}\sigma_i : \overline{K}] = n$ and therefore $[S : \overline{K}] = n^2$. But since S is a $\overline{K}$-submodule of R and we proved that $[R : \overline{K}] = n^2$, we can conclude that $R = S = \sum_{\sigma \in G} \overline{L}\sigma$, which shows that L is a Galois extension of K relative to G.

REFERENCES

1. R. Alfaro and G. Szeto, *On Galois extensions of an Azumaya algebra,* Comm. in Algebra, 25(6), (1997), 1873-1882.
2. F.R. DeMeyer, *Galois theory in separable algebras over commutative rings,* Illinois J. Math., 10(1966), 287-295.
3. F.R. DeMeyer and E. Ingraham, *Separable algebras over commutative rings,* Vol. 181, Springer-Verlag, Berlin,1971.
4. M. Harada, *Supplementary results on Galois extension,* Osaka J. Math., 2(1965), 343-350.
5. T. Kanzaki, *On Galois algebra over a commutative ring,* Osaka J. Math., 2(1965), 309-317.
6. G. Szeto and L. Xue, *The structure of Galois algebras,* Journal of Algebra, 237(1)(2001), 238-246.
7. G. Szeto and L. Xue, *The Boolean algebra and central Galois algebras,* International Journal of Mathematics and Mathematical Sciences, 28(4)(2001), 237-242.
8. G. Szeto and L. Xue, *The Galois algebras and the Azumaya Galois extensions,* International Journal of Mathematics and Mathematical Sciences, 31(1) (2002), 37-42.
9. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents,* Nagoya Math. J. 35(1969), 83–98.