

On Azumaya Algebras with a Finite Automorphism Group

George Szeto and Lianyong Xue

Department of Mathematics, Bradley University

Peoria, Illinois 61625 – U.S.A.

Email: szeto@hilltop.bradley.edu and lxue@hilltop.bradley.edu

ABSTRACT. Let B be a ring with 1, C the center of B , and G an finite automorphism group of B . It is shown that if B is an Azumaya algebra such that $B = \oplus \sum_{g \in G} J_g$ where $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$, then there exist orthogonal central idempotents $\{f_i \in C \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups H_i of G such that $B = (\oplus \sum_{i=1}^m Bf_i) \oplus D$ where Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, m$ and D is contained in C .

Key Words and Phrases. Separable extensions, Azumaya algebras, Galois extensions, Galois algebras, and central Galois extensions.

2000 Mathematics Subject Classification. Primary 16S35, 16W20

1. Introduction. Let A be an Azumaya algebra, G a finite algebra automorphism group of A , and $J_g = \{a \in A \mid ax = g(x)a \text{ for all } x \in A\}$ for each $g \in G$. In [6], it was shown that $J_g J_h = J_{gh}$ for all $g, h \in G$. In [2], let B be a separable algebra over a commutative ring R and G a finite algebra automorphism group of B . Assume that $B = \oplus \sum_{g \in G} J_g$ where J_g are similarly defined as for A . Then, B is a central Galois algebra with Galois group G if and only if for each $g \in G$, $J_g J_{g^{-1}} = C$, the center of B . Thus, any Azumaya algebra B with a finite algebra automorphism group G such that $B = \oplus \sum_{g \in G} J_g$ is a central Galois algebra with Galois group G . By changing the algebra automorphism group G to a ring automorphism group G , the purpose of the present paper

is to generalize the above fact. We shall show that if B is an Azumaya C -algebra with a finite ring automorphism group G such that $B = \oplus \sum_{g \in G} J_g$, then there exist orthogonal central idempotents $\{f_i \in C \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups H_i of G such that $B = (\oplus \sum_{i=1}^m Bf_i) \oplus Bf$ where Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m f_i$, and $Bf = Cf$. Since a Galois algebra B with Galois group G is an Azumaya algebra such that $B = \oplus \sum_{g \in G} J_g$, our result can be applied to Galois algebras. Moreover, if B is a separable extension of B^G such that $B = \oplus \sum_{g \in G} J_g$, then the direct summand Bf is a commutative Galois algebra with Galois group $G|_{Bf} \cong G$. An example is given to demonstrate the results and to illustrate that an Azumaya algebra B such that $B = \oplus \sum_{g \in G} J_g$ is not necessarily a Galois algebra with Galois group G . This paper was written under the support of a Caterpillar Fellowship at Bradley University. We would like to thank Caterpillar Inc. for the support.

2. Definitions and Notations. Throughout this paper, B will represent a ring with 1, C the center of B , G a ring automorphism group of B of order n for some integer n , and B^G the set of elements in B fixed under each element in G . We denote $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$ and $I_g = BJ_g \cap C$ for each $g \in G$.

Let A be a subring of a ring B with the same identity 1. We denote $V_B(A)$ the commutator subring of A in B . We follow the definitions of a Galois extension, a separable extension, and an Azumaya algebra as given in [1], [5], and [7]. B is called a separable extension of A if there exist $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, m \text{ for some integer } m\}$ such that $\sum a_i b_i = 1$, and $\sum b a_i \otimes b_i = \sum a_i \otimes b_i b$ for all b in B where \otimes is over A . An Azumaya algebra is a separable extension of its center. B is called a Galois extension of B^G with Galois group G if there exist elements $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. B is called a Galois algebra over R if B is a Galois extension of R which is contained in C , and B is called a central Galois extension if B is a Galois extension of C .

3. The Structure Theorem. In this section, we assume that B is an Azumaya C -algebra with a finite ring automorphism group G such that $B = \oplus \sum_{g \in G} J_g$. We shall show a structure theorem for such a B . We begin with some properties of the C -module J_g for $g \in G$ similar to those as for a Galois algebra ([3, Proposition 2]).

LEMMA 3.1. *For all $g, h \in G$,*

(1) $J_g J_h = I_g J_{gh} = I_h J_{gh}$ where $I_g = BJ_g \cap C$ and $I_h = BJ_h \cap C$.

(2) there is a unique idempotent $e_g \in C$ such that $BJ_g = Be_g$ and $J_g J_{g^{-1}} = e_g C$.

PROOF. (1) Since B is an Azumaya C -algebra and BJ_g is an ideal of B , $BJ_g = BI_g$ ([1, Proposition 1.11, page 46]). By hypothesis, $B = \oplus \sum_{g \in G} J_g$, so $BJ_h = \sum_{g \in G} J_g J_h$. Noting that $J_g J_h \subset J_{gh}$ and $B = \oplus \sum_{g \in G} J_{gh}$, we have that $BJ_h = \oplus \sum_{g \in G} J_g J_h$. Hence $\oplus \sum_{g \in G} J_g J_h = BJ_h = BI_h = \oplus \sum_{g \in G} J_{gh} I_h$. Thus, $J_g J_h = I_h J_{gh}$. Similarly, $J_g J_h = I_g J_{gh}$.

(2) By (1), $J_g J_h = I_g J_{gh}$ for all $g, h \in G$. By letting $h = 1$, we have $I_g J_g = J_g J_1 = J_g C = J_g$, and by letting $h = g^{-1}$, we have $J_g J_{g^{-1}} = I_g J_1 = I_g C = I_g$. Thus, $(I_g)^2 = I_g J_g J_{g^{-1}} = J_g J_{g^{-1}} = I_g$. Moreover, since $B = \oplus \sum_{g \in G} J_g$ is an Azumaya C -algebra, J_g is a finitely generated and projective C -module for each $g \in G$. Hence $BJ_g \cong B \otimes_C J_g$ is a finitely generated and projective ideal of B . This implies that $I_g (= BJ_g \cap C)$ is a finitely generated and projective ideal of C . But, $(I_g)^2 = I_g$, so $I_g = Ce_g$ for some idempotent $e_g \in C$ ([3, Lemma 2] or [4, Theorem 76]). Therefore, $BJ_g = BI_g = Be_g$ and $J_g J_{g^{-1}} = I_g = e_g C$. Since e_g is the identity of Be_g , it is unique.

By Lemma 3.1-(2), for each $g \in G$, there is a unique idempotent $e_g \in C$ such that $BJ_g = Be_g$. The Boolean algebra generated by the elements $\{e_g \mid g \in G \text{ and } BJ_g = Be_g\}$ is denoted by E .

LEMMA 3.2. *Let e be a nonzero element in E of form $e = \prod_{h \in H} e_h$ for some maximum subset H of G . Then H is a subgroup of G and $h(e) = e$ for each $h \in H$.*

PROOF. For any $g, h \in H$,

$$Be_g e_h = (BJ_g)(BJ_h) = B(J_g J_h) = B(I_g J_{gh}) = (BI_g)(BJ_{gh}) = Be_g e_{gh}.$$

Hence $e_g e_h = e_g e_{gh}$. Thus, $e_g e_h = e_g e_h^2 = e_g e_{gh} e_h$. Therefore, $e = e e_{gh}$. Thus, $gh \in H$ by the maximality of H . Since G is finite, that $gh \in H$ whenever $g, h \in H$ implies that H is a subgroup of G . Noting that, for a subgroup H , $gHg^{-1} = H$ for all $g \in H$, we have that

$$g(Be) = g(B(\prod_{h \in H} J_h)) = B(\prod_{h \in H} g(J_h)) = B(\prod_{h \in H} J_{ghg^{-1}}) = B(\prod_{h \in H} J_h) = Be$$

for each $g \in H$. Hence, $g(e) = e$ for each $g \in H$ because e is the identity of Be .

Next we show that $H|_{Be}$ is an algebra automorphism group.

LEMMA 3.3. *Let e and H be given in Lemma 3.2. Then h restricted to Ce is an identity for each $h \in H$.*

PROOF. For any $h \in H$ and $b \in J_h$, $bc = h(c)b$ for all $c \in C$, so $(c - h(c))b = 0$. Hence $(c - h(c))J_h = \{0\}$. Therefore $B(c - h(c))e_h = (c - h(c))Be_h = (c - h(c))BJ_h = B(c - h(c))J_h = \{0\}$. Thus, $(c - h(c))e_h = 0$. But $e = \prod_{h \in H} e_h$, so $(c - h(c))e = 0$. Moreover, $h(e) = e$ for each $h \in H$ by Lemma 3.2, so $0 = (c - h(c))e = (c - h(c))h(e) = ch(e) - h(c)h(e) = ce - h(ce)$, that is, $h(ce) = ce$ for all $c \in C$.

LEMMA 3.4. *Let $J_h^{(Bf)} = \{b \in Bf \mid bx = h(x)b \text{ for all } x \in Bf\}$ for any $f \in E$ and $h \in G$. If $h(f) = f$, then $J_h^{(Bf)} = fJ_h$.*

PROOF. It is clear that $fJ_h \subset J_h^{(Bf)}$. Conversely, for any $b \in J_h^{(Bf)}$, $b = fb$ and $bx = h(x)b$ for each $x \in Bf$. Hence for any $y \in B$, $by = (fb)y = b(yf) = h(yf)b = h(y)fb = h(y)b$. Therefore, $b \in J_h$, and so $b = fb \in fJ_h$. Thus, $J_h^{(Bf)} = fJ_h$.

Let e and H be given in Lemma 3.2. We have a structure theorem for the Azumaya Ce -algebra Be with an algebra automorphism group $H|_{Be} \cong H$ and for the Azumaya C -algebra B with a ring automorphism group G respectively.

THEOREM 3.5. *Let e and H be given in Lemma 3.2. Then Be is a central Galois algebra with Galois group $H|_{Be} \cong H$.*

PROOF. By Lemma 3.2, H is a subgroup of G and $h(e) = e$ for any $h \in H$. By Lemma 3.3, h restricted to Ce is an identity for each $h \in H$. Hence $H|_{Be}$ is a Ce -algebra automorphism group of Be . Since B is an Azumaya C -algebra, Be is an Azumaya Ce -algebra ([1, Proposition 1.11, page 46]). By Lemma 3.4, $J_h^{(Be)} = eJ_h$ for each $h \in H$, so $Be = \oplus \sum_{g \in G} J_g e = \oplus \sum_{g \in H} eJ_g \oplus \sum_{g \notin H} eJ_g$. Since H is a maximum subset of G such that $e = \prod_{h \in H} e_h$, $ee_g = 0$ for each $g \notin H$. This implies that $BeJ_g = Bee_g = \{0\}$. Therefore, $eJ_g = \{0\}$ for each $g \notin H$. Thus, $Be = \oplus \sum_{g \in H} eJ_g = \oplus \sum_{g \in H} J_g^{(Be)}$. Moreover, $J_h^{(Be)} J_{h^{-1}}^{(Be)} = (eJ_h)(eJ_{h^{-1}}) = eJ_h J_{h^{-1}} = ee_h C = Ce$ which is the center of Be by Lemma 3.1. Thus, Be is a central Galois algebra over Ce with Galois group $H|_{Be}$ ([2, Theorem 1]). Next, we claim that $H|_{Be} \cong H$. Since $e \neq 0$, $\{0\} \neq Be = Bee_h = BeJ_h = BJ_h^{(Be)}$ for each $h \in H$. Hence $J_h^{(Be)} \neq \{0\}$ for each $h \in H$. Now, if $h|_{Be} = 1$, then $\{0\} \neq Ce = J_h^{(Be)} = eJ_h \subset C \cap J_h = J_1 \cap J_h$. But $B = \oplus \sum_{g \in G} J_g$, so $J_1 = J_h$. Therefore $h = 1$. This implies that $h|_{Be} \neq 1$ whenever $h \neq 1$ in H . Thus, $H|_{Be} \cong H$.

THEOREM 3.6. *Let B be an Azumaya C -algebra with a finite ring automorphism group G such that $B = \oplus \sum_{g \in G} J_g$, then there exist orthogonal idempotents $\{f_i \in C \mid i =$*

$1, 2, \dots, m$ for some integer m and subgroups H_i of G such that $B = (\oplus \sum_{i=1}^m Bf_i) \oplus Cf$ where Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, m$ and $f = 1 - \sum_{i=1}^m f_i$.

PROOF. Let $\{f_i \in E | i = 1, 2, \dots, k\}$ be all distinct nonzero elements in E of form $f_i = \prod_{h \in H_i} e_h$ for some maximum subset (subgroup) H_i of G as given in Lemma 3.2. Then they are orthogonal. Hence $B = (\oplus \sum_{i=1}^k Bf_i) \oplus Bf$ where $f = 1 - \sum_{i=1}^k f_i$ such that Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, k$ by Theorem 3.5. Next, we claim that $Bf = Cf$. Since $\{f_i | i = 1, 2, \dots, k\}$ are all distinct nonzero elements in E of form $f_i = \prod_{h \in H_i} e_h$ for some maximum subset (subgroup) H_i of G , g permutes the set $\{f_i | i = 1, 2, \dots, k\}$ for each $g \in G$. Hence $g(f) = f$ for each $g \in G$. Hence, by Lemma 3.4, $J_g^{(Bf)} = fJ_g$ for each $g \in G$. Therefore, $Bf = \oplus \sum_{g \in G} J_g f = \oplus \sum_{g \in G} J_g^{(Bf)}$ is an Azumaya Cf -algebra with a finite ring automorphism group $G|_{Bf}$. If $J_g^{(Bf)} = \{0\}$ for each $g \neq 1$ in G , then $Bf = J_1^{(Bf)} = fJ_1 = Cf$, and so we are done. If $J_g^{(Bf)} \neq \{0\}$ for some $g \neq 1$ in G , we can repeat the above argument to have more direct summands of central Galois algebras. Since E is finite, we have only finitely many central orthogonal idempotents $\{f_i \in E | i = 1, 2, \dots, m \text{ for some integer } m\}$ such that $B = (\oplus \sum_{i=1}^m Bf_i) \oplus Bf$ where Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, m$ and $Bf = Cf$. This completes the proof.

Remark 1. Theorem 3.6 generalizes the following theorem of Harada ([2, Theorem 1]):

Let B be a separable R -algebra with automorphism group G . If $B = \oplus \sum_{g \in G} J_g$ and $J_g J_{g^{-1}} = C$ for each $g \in G$, then B is a central Galois algebra with Galois group G .

Remark 2. Any Galois algebra with Galois group G satisfies the conditions as given in Theorem 3.6. There are Azumaya C -algebras B such that $B = \oplus \sum_{g \in G} J_g$, but B

is not a Galois algebra with Galois group G (see the example at the end of the paper). However, for a Galois extension B of B^G with Galois group G , the condition that B is a Galois algebra with Galois group G and that $B = \bigoplus \sum_{g \in G} J_g$ are equivalent as given by the following proposition.

PROPOSITION 3.7. *For a Galois extension B of B^G with Galois group G , B is a Galois algebra with Galois group G if and only if $B = \bigoplus \sum_{g \in G} J_g$.*

PROOF. Since B is a Galois extension of B^G with Galois group G , $V_B(B^G) = \bigoplus \sum_{g \in G} J_g$ ([3, Proposition 1]). Hence $B = \bigoplus \sum_{g \in G} J_g$ if and only if $V_B(B^G) = B$, that is, $B^G \subset C$.

As an application of theorem 3.6, we obtain a structure theorem for a separable extension B of B^G such that $B = \bigoplus \sum_{g \in G} J_g$.

THEOREM 3.8. *Let B be a separable extension of B^G such that $B = \bigoplus \sum_{g \in G} J_g$, then there exist orthogonal idempotents $\{f_i \in C \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups H_i of G such that $B = (\bigoplus \sum_{i=1}^m B f_i) \oplus B f$ where $B f_i$ is a central Galois algebra with Galois group $H_i|_{B f_i} \cong H_i$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m f_i$, and $B f = C f$ is commutative Galois algebra with Galois group $G|_{B f} \cong G$ if $f \neq 0$.*

PROOF. For any $a \in B^G$ and $b = \sum_{g \in G} b_g \in B$ where $b_g \in J_g$, $b_g a = g(a) b_g = a b_g$ for each $g \in G$, so $ba = \sum_{g \in G} b_g a = a \sum_{g \in G} b_g = ab$ for any $b \in B$. Thus, $a \in C$ for any $a \in B^G$. Therefore, $B^G \subset C$. Noting that B is a separable algebra over B^G , we have that B is an Azumaya C -algebra. But $B = \bigoplus \sum_{g \in G} J_g$, so, by Theorem 3.6, there exist orthogonal idempotents $\{f_i \in C \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups H_i of G such that $B = (\bigoplus \sum_{i=1}^m B f_i) \oplus B f$ where $B f_i$ is a central Galois algebra with Galois group $H_i|_{B f_i} \cong H_i$ for each $i = 1, 2, \dots, m$, $B f = C f$, and $f = 1 - \sum_{i=1}^m f_i$. Thus, it suffices to

show that $Bf(= Cf)$ is commutative Galois algebra with Galois group $G|_{Bf} \cong G$ in case $f \neq 0$. In fact, since B^G is contained in C and B is separable over B^G , C is separable over B^G ([1, Theorem 3.8, page 55]), and so Cf is separable over $B^G f$ ([1, Proposition 1.11, page 46]). Moreover, since $f \in C^G$, $B^G f \subset (B^G f)^G \subset (Cf)^G$. Hence Cf is separable over $(Cf)^G$ ([1, Proposition 1.11, page 46]). Furthermore, $J_g^{(Cf)} = J_g^{(Bf)} = fJ_g$ for each $g \in G$ by Lemma 3.4, so $J_g^{(Cf)} \subset C \cap J_g = \{0\}$ for each $g \neq 1$ in G . This implies that $g|_{Cf} \neq \text{identity}$ whenever $g \neq 1$ in G (for $J_1^{(Cf)} = Cf$). Thus, $G|_{Bf} \cong G$ and $Bf(= Cf)$ is a commutative Galois algebra with Galois group $G|_{Bf} \cong G$ ([2, Proposition 2]). This completes the proof.

We conclude the present paper with an example to demonstrate the results in Theorem 3.6 and illustrate that an Azumaya C -algebra B such that $B = \bigoplus_{g \in G} J_g$, but not necessarily a Galois algebra with Galois group G .

EXAMPLE 3.9. Let $R[i, j, k]$ be the real quaternion algebra over the field of real numbers R , Z the integer ring, $D = (Z + \sqrt{-1}Z) \otimes_Z (Z + \sqrt{-1}Z)$, $B = R[i, j, k] \oplus D$, and $G = \{1, g_i, g_j, g_k\}$ where $g_i(a, d_1 \otimes d_2) = (iai^{-1}, \bar{d}_1 \otimes d_2)$, $g_j(a, d_1 \otimes d_2) = (jaj^{-1}, d_1 \otimes \bar{d}_2)$, and $g_k(a, d_1 \otimes d_2) = (kak^{-1}, \bar{d}_1 \otimes \bar{d}_2)$, for all $(a, d_1 \otimes d_2)$ in B , where \bar{d} is the conjugate of the complex number d . Then,

- (1) The center of B is $C = R \oplus D$.
- (2) B is an Azumaya C -algebra.
- (3) $J_1 = C = R \oplus D$, $J_{g_i} = R(i, 0)$, $J_{g_j} = R(j, 0)$, $J_{g_k} = R(k, 0)$. Hence $B = \bigoplus_{g \in G} J_g$
- (4) By (3), $J_g J_{g^{-1}} = C(1, 0)$ for each $g \neq 1$ in G . Hence, $f_1 = (1, 0)$ is the only nonzero element in E of form $f_1 = \prod_{h \in H_1} e_h$ for some maximum subset H_1 of G (here $H_1 = G$) and $f = 1 - f_1 = (0, 1 \otimes 1)$.

(5) $B = (\oplus \sum_{i=1}^m Bf_i) \oplus Cf$ where $m = 1$, Bf_i is a central Galois algebra with Galois group $H_i|_{Bf_i} \cong H_i$ for each $i = 1, 2, \dots, m$

(6) $B^G = R \oplus (Z \otimes Z) = R \oplus Z.$

(7) Since D is not separable over Z , B is not separable over $B^G (= R \oplus Z)$. Hence B is not a Galois algebra with Galois group G .

REFERENCES

- [1] F.R. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971, Lecture Notes in Mathematics.
- [2] M. Harada, *Supplementary Results on Galois Extension*, Osaka J. Math. **2**(1965), 343-350.
- [3] T. Kanzaki, *On Galois Algebra Over A Commutative Ring*, Osaka J. Math. **2**(1965), 309-317.
- [4] I. Kaplansky, *Commutative Rings*, Allyn and Bacon, Inc, Boston, 1970.
- [5] P. Nuss, *Extensions, Galoisiennes non commutatives normalité, cohomologie non abélienne*, Comm. in Algebra **28**(2000), no. 7, 3223-3251.
- [6] A. Rosenberg and D. Zelinsky, *Automorphisms of Separable Algebras*, Pacific J. Math. **11**(1961), 1109-1117.
- [7] G. Szeto and L. Xue, *On Characterizations of a Center Galois Extension*, International Journal of Mathematics and Mathematical Sciences, **23**(2000), no. 11, 753-758.