NOTES ON GALOIS ALGEBRAS

George Szeto and Lianyong Xue

Bradley University, USA

Abstract. Let B be a ring with 1, C the center of B, and G an automorphism group of B of order n for some integer n. Assume B is a Galois algebra over R with Galois group G. For a nonzero idempotent $e \in R$, if the rank of Be over Ce is defined and equal to the order of $H|_{Be}$ where $H = \{g \in G \mid g(c) = c$ for each $c \in C\}$, then Be is a central Galois algebra with Galois group $H|_{Be}$. This generalizes the F. R. DeMeyer and T. Kanzaki theorems for Galois algebras. Moreover, a structure theorem for a Galois algebra is given in terms of the concept of the rank of a projective module.

1. Introduction

Galois theory for rings has been intensively investigated since 1960. Recently, several types of Galois extensions of noncommutative rings were studied ([5],[7],[8],[9]). Let B be a Galois algebra over a commutative ring R with Galois group G. F. R. DeMeyer (see [2]) and T. Kanzaki (see [4]) gave different conditions under which B is a central Galois algebra as follows:

(1) (see [2, Lemma 4]) Assume B is a Galois R-algebra with Galois group G. If C (= the center of B) contains no idempotents except 0 and 1, then $C = B^H$ where $H = \{g \in G \mid g(c) = c$ for each $c \in C\}$.

(2) (see [4, Proposition 3]) Let B be a Galois algebra over R with Galois group G, C the center of B, and $H = \{g \in G \mid g(c) = c$ for each $c \in C\}$. Then B is a central Galois algebra over C with Galois group H if and only if $J_g = \{0\}$ for each $g \notin H$ where $J_g = \{b \in B \mid bx = g(x)b$ for all $x \in B\}$ for each $g \in G$.

The purpose of the present paper is to generalize the above two theorems of DeMeyer and Kanzaki. We shall show that, for a Galois algebra B over R and a nonzero idempotent $e \in R$, the rank of Be over Ce is defined and equal to the order of $H|_{Be}$ if and only if Be is a central Galois algebra over Ce with Galois group $H|_{Be}$. Moreover, we shall give a structure theorem for a Galois algebra B in terms of the rank of a projective module as given in the theorem. The present paper was written during the visit of Professor S. Ikehata to Bradley University in winter, 1999, and supported by a Caterpillar Fellowship at Bradley University. We would like to thank Professor Ikehata for many useful discussions and Caterpillar Inc. for the support. This paper was also revised under the suggestions of the referee. We would like to thank the referee for the valuable suggestions.

2. Definitions and Notations

Throughout this paper, B will represent a ring with 1, G an automorphism group of B of order n for some integer n, C the center of B, B^G the set of elements in B fixed under each element in G, and $B * G$ a skew group ring of group G over B. We denote $J_g = \{b \in B \,|\, bx = g(x)b$ 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 call B a separable extension of A if there exist $\{a_i, b_i$ in B, $i = 1, 2, ..., m$ 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 $\{a_i, b_i$ in B, $i = 1, 2, ..., m\}$ for some integer m such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Such a set $\{a_i, b_i\}$ is called a G-Galois system for B. 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. Let P be a projective module over a commutative ring R. Then for a prime ideal p of R, $P_p (= P \otimes_R R_p)$ is a free module over $R_p (=$ the local ring of R at $p)$, and the rank of P_p over R_p is the number of copies of R_p in P_p; $\mathrm{rank}_R(P) = m$ if $\mathrm{rank}_{R_p}(P_p) = m$ for some integer m for all prime ideals p of R.

3. A Generalization

Let B be a Galois algebra over R with Galois group G and C the center of B. In this section, we shall give a condition under which B is a composition of a central Galois algebra and a commutative Galois algebra. This generalizes the theorems of DeMeyer and Kanzaki. At first, we recall the rank function of a finitely generated projective module P over a commutative ring R. Let $\mathrm{Spec}(R)$ be the set of prime ideals of R with the Zariski topology and Z the set of integers with the discrete topology. It is well known that

$rk_R(P) : \mathrm{Spec}(R) \longrightarrow Z$ by $rk_R(P)(p) = \mathrm{rank}_{R_p}(P_p)$ is a continuous function and there exist orthogonal idempotents $\{e_i \,|\, i = 1, 2, ..., m$ for some integer $m\}$ in R such that $P = \oplus \sum_{i=1}^{m} Pe_i$ and $\mathrm{rank}_{Re_i}(Pe_i) = k_i$ is defined for each i, and $k_i \neq k_j$ for $i \neq j$.

THEOREM 3.1. *Let B be a Galois algebra over R with Galois group G, C the center of B, and $H = \{g \in G \mid g(c) = c$ for each $c \in C\}$. Then, $\mathrm{rank}_C(B)$ is defined and equal to $|H|$, the order of H if and only if B is a central Galois algebra with Galois group H.*

PROOF. Since B is a Galois algebra over R with Galois group G, $B = \oplus \sum_{g \in G} J_g = (\oplus \sum_{h \in H} J_h) \oplus (\oplus \sum_{g \notin H} J_g)$ (see [4, Theorem 1]). But H is a C-automorphism group of B, so J_h is a finitely generated and projective C-module of rank 1 and $J_h J_{h^{-1}} = J_1 = C$ for each $h \in H$ (see [6]). By hypothesis, $\mathrm{rank}_C(B) = |H|$, so $B = \oplus \sum_{h \in H} J_h$ (and so $J_g = \{0\}$ for each $g \notin H$). Therefore, B is a central Galois algebra over C with Galois group H (see [3, Theorem 1]). Conversely, assume B is a central Galois algebra with Galois group H. Then $B = \oplus \sum_{h \in H} J_h$ and J_h is a finitely generated and projective C-module of rank 1 for each $h \in H$. Thus, $\mathrm{rank}_C(B) = |H|$. ☐

Next we show that Theorem 3.1 generalizes DeMeyer's theorem and is equivalent to Kanzaki's theorem.

COROLLARY 3.2 (F. R. DeMeyer). *Let B be a Galois algebra over R with Galois group G and $H = \{g \in G \mid g(c) = c$ for each $c \in C\}$. If C is indecomposable, then B is a central Galois algebra with Galois group H.*

PROOF. Since B is a Galois algebra over R with Galois group G, $B = \oplus \sum_{g \in G} J_g = (\oplus \sum_{h \in H} J_h) \oplus (\oplus \sum_{g \notin H} J_g)$ where $J_g J_{g^{-1}} = e_g C$ for some idempotents e_g in C (see [4, Theorem 2]). Since C is indecomposable, $J_g J_{g^{-1}} = \{0\}$ or C for each $g \in G$. We claim that $J_g J_{g^{-1}} = \{0\}$ for each $g \notin H$. Suppose that $J_g J_{g^{-1}} = C$. Then $1 \in J_g J_{g^{-1}}$. Hence $1 = \sum_{i=1}^{m} x_i y_i$ for some $x_i \in J_g$ and $y_i \in J_{g^{-1}}$. Since $g \notin H$, there exists $c \in C$ such that $g(c) = c' \neq c$. But, then $c' = 1c' = \sum_{i=1}^{m} x_i y_i c' = \sum_{i=1}^{m} x_i g^{-1}(c') y_i = \sum_{i=1}^{m} x_i c y_i = c \sum_{i=1}^{m} x_i y_i = c1 = c$. This is a contradiction. Thus, $J_g J_{g^{-1}} = \{0\}$ for each $g \notin H$. Next, we claim that $J_g = \{0\}$ for each $g \notin H$. Since B is a Galois algebra over R, B is an Azumaya C-algebra. Noting that BJ_g is an ideal of B and $I_g = BJ_g \cap C$ is an ideal of C, we have that $BJ_g = BI_g$ (see [1, Corollary 3.7, page 54]). Also, by Proposition 2 in

[4], $I_g^2 = I_g$ for all $g \in G$. Hence, for each $g \notin H$,

$$
\begin{aligned}
J_g \subset BJ_g &= BI_g = BI_g^2 = (BI_g)(BI_g) = (BJ_g)(BJ_g) \\
&= BJ_gJ_g = BI_gJ_{g^2} = BJ_gJ_{g^2} = BI_gJ_{g^3} \\
&= BJ_gJ_{g^3} = BI_gJ_{g^4} = \cdots\cdots \\
&= BJ_gJ_{g^{l-1}} \quad \text{(where l is the order of g)} \\
&= BJ_gJ_{g^{-1}} = \{0\}.
\end{aligned}
$$

This shows that $J_g = \{0\}$ for each $g \notin H$. Thus, $B = (\oplus \sum_{h \in H} J_h)$. Since $\operatorname{rank}_C(J_h) = 1$, $\operatorname{rank}_C(B) = |H|$. Hence, by Theorem 3.1, B is a central Galois algebra with Galois group H. $\square$

REMARK. It is well known that for a Galois algebra B over R, if B is a central Galois algebra over C with Galois group H, then C is a Galois algebra over R with Galois group G/H. Thus, Theorem 3.1 shows that a Galois algebra B is a composition of a central Galois algebra with Galois group H and a commutative Galois algebra C with Galois group G/H when $\operatorname{rank}_C(B) = |H|$.

THEOREM 3.3. *Let B be a Galois algebra over R with Galois group G and $H = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$. Then, $\operatorname{rank}_C(B) = |H|$ if and only if $J_g = \{0\}$ for each $g \notin H$.*

PROOF. Since B is a Galois algebra over R with Galois group G, $B = \oplus \sum_{g \in G} J_g = (\oplus \sum_{h \in H} J_h) \oplus (\oplus \sum_{g \notin H} J_g)$ as C-module (see [4, Theorem 1]). For each $h \in H$, J_h is a finitely generated and projective C-module of rank 1 (see [6]). Thus, $\operatorname{rank}_C(B) = |H|$ if and only if $J_g = \{0\}$ for each $g \notin H$. $\square$

To generalize the Kanzaki's theorem, we put Theorem 3.1 in a "local" form at a nonzero idempotent in R.

THEOREM 3.4. *Let B be a Galois algebra over R with Galois group G, e a nonzero idempotent in R, and $H = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$. Then, Be is a central Galois algebra over Ce with Galois group $H|_{Be}$ if and only if $\operatorname{rank}_{Ce}(Be)$ is defined and equal to $|H|_{Be}|$, the order of $H|_{Be}$.*

PROOF. We first claim that Be is a Galois algebra over Re with Galois group $G|_{Be} \cong G$. In fact, by hypothesis, B is a Galois algebra over R with Galois group G, so there exists a G-Galois system for B $\{a_j, b_j$ in B, $j = 1, 2, ..., t\}$ for some integer t such that $\sum_{j=1}^{t} a_j g(b_j) = \delta_{1,g}$ for each $g \in G$. Hence $\sum_{j=1}^{t} (a_j e) g(b_j e) = e \sum_{j=1}^{t} a_j g(b_j) = e\delta_{1,g}$ for each $g \in G$. Therefore, $\{a_j e, b_j e$ in Be, $j = 1, 2, ..., t\}$ is a G-Galois system for Be and $e = \sum_{j=1}^{t} (a_j e)(g(b_j e) - b_j e)$ for each $g \neq 1$ in G. But $e \neq 0$, so $g|_{Be} \neq 1$ whenever $g \neq 1$ in G. Thus, Be is a Galois algebra over Re with Galois group $G|_{Be} \cong G$. Thus, Theorem 3.4 holds by Theorem 3.1 for Be. $\square$

COROLLARY 3.5 (T. Kanzaki). *Let B be a Galois algebra over R with Galois group G and $H = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$. Then, $J_g = \{0\}$ for each $g \notin H$ if and only if B is a central Galois algebra with Galois group H.*

PROOF. This is a consequence of Theorem 3.3 and Theorem 3.4 for $e = 1$.
□

4. A STRUCTURE THEOREM

In this section, we shall show that any Galois algebra is a direct sum of Galois algebras each with Galois group isomorphic with and induced by G and a well defined rank over its center.

THEOREM 4.1. *Let B be a Galois algebra over R with Galois group G. Then there are orthogonal idempotents $\{e_i \mid i = 1, 2, ..., m \text{ for some integer } m\}$ in C^G such that $B = \oplus \sum_{i=1}^{m} Be_i$ where Be_i is a Galois algebra over Re_i with Galois group $G|_{Be_i} \cong G$ and $\text{rank}_{Ce_i}(Be_i) = k_i$ for distinct integers k_i, $i = 1, 2, ..., m$.*

PROOF. Since B is a Galois algebra over R, B is separable over R. Hence B is an Azumaya C-algebra (see [1, Theorem 3.8, page 55]), and so it is a finitely generated and projective C-module. Therefore, there exist orthogonal non-zero idempotents e_i in C, $i = 1, 2, ..., m$ for some integer m such that $B = \oplus \sum_{i=1}^{m} Be_i$ and $\text{rank}_{Ce_i}(Be_i) = k_i$ for some integer k_i, and $k_i \neq k_j$ for $i \neq j$. This implies that $g(Be_i) = Be_i$ for g preserves the rank of Be_i over Ce_i for each $g \in G$. Thus, for each $e_i \in C^G (= R)$, Be_i is a Galois algebra over Re_i with Galois group $G|_{Be_i} \cong G$ by the proof of Theorem 3.4. This completes the proof. □

Theorem 4.1 is another general form of Theorem 3.1 different from Theorem 3.4. We can use Theorem 3.1 to identify which direct summand of B is a composition of a central Galois algebra and a commutative Galois algebra.

COROLLARY 4.2. *Let B and e_i's be as given in Theorem 4.1, and $H_i = \{g \in G|_{Be_i} \mid g(ce_i) = ce_i \text{ for each } ce_i \in Ce_i\}$. Then Be_i is a central Galois algebra with Galois group H_i if and only if $\text{rank}_{Ce_i}(Be_i) = |H_i|$, the order of H_i.*

We conclude the present paper with two examples of a Galois algebra B: (1) B is a composition of a central Galois algebra and a commutative Galois algebra, (2) B is not so as given in (1), but has a direct summand which is so as given in (1).

EXAMPLE 4.3. Let $R[i, j, k]$ be the real quaternion algebra over R, $B = R[i, j, k] \oplus R[i, j, k]$, and $G = \{1, g_i, g_j, g_k, g_0, g_0 g_i, g_0 g_j, g_0 g_k\}$ where $g_i(a_1, a_2) = (ia_1 i^{-1}, ia_2 i^{-1})$, $g_j(a_1, a_2) = (ja_1 j^{-1}, ja_2 j^{-1})$, $g_k(a_1, a_2) = (ka_1 k^{-1}, ka_2 k^{-1})$, and $g_0(a_1, a_2) = (a_2, a_1)$ for all (a_1, a_2) in B. Then,

(1) B is a Galois extension with a G-Galois system:

$$\{a_1 = (1,0),\ a_2 = (i,0),\ a_3 = (j,0),\ a_4 = (k,0),$$
$$a_5 = (0,1),\ a_6 = (0,i),\ a_7 = (0,j),\ a_8 = (0,k);$$
$$b_1 = \frac{1}{4}(1,0),\ b_2 = -\frac{1}{4}(i,0),\ b_3 = -\frac{1}{4}(j,0),\ b_4 = -\frac{1}{4}(k,0),$$
$$b_5 = \frac{1}{4}(0,1),\ b_6 = -\frac{1}{4}(0,i),\ b_7 = -\frac{1}{4}(0,j),\ b_8 = -\frac{1}{4}(0,k)\}.$$

(2) $B^G = \{(r,r)\,|\,r \in R\} \cong R$.

(3) $C = R \oplus R$.

(4) By (1), (2), and (3), B is a Galois algebra over R with Galois group G, but not a central Galois algebra with Galois group G.

(5) $H = \{g \in G \mid g(c) = c \text{ for each } c \in C\} = \{1,\ g_i,\ g_j,\ g_k\}$.

(6) B is a central Galois algebra with Galois group H and C is a Galois algebra over R with Galois group $G/H \cong \{1,\ g_0\}$.

EXAMPLE 4.4. Let $R[i,j,k]$ be the real quaternion algebra over R, D the field of complex numbers, $B = R[i,j,k] \oplus R[i,j,k] \oplus (D \otimes_R D) \oplus (D \otimes_R D)$, and
$G = \{1,\ g_i,\ g_j,\ g_k,\ g_0,\ g_0 g_i,\ g_0 g_j,\ g_0 g_k\}$ where

$$g_i(a_1, a_2, d_1 \otimes d_2, d_3 \otimes d_4) = (ia_1 i^{-1}, ia_2 i^{-1}, \bar{d}_1 \otimes d_2, \bar{d}_3 \otimes d_4)$$
$$g_j(a_1, a_2, d_1 \otimes d_2, d_3 \otimes d_4) = (ja_1 j^{-1}, ja_2 j^{-1}, d_1 \otimes \bar{d}_2, d_3 \otimes \bar{d}_4)$$
$$g_k(a_1, a_2, d_1 \otimes d_2, d_3 \otimes d_4) = (ka_1 k^{-1}, ka_2 k^{-1}, \bar{d}_1 \otimes \bar{d}_2, \bar{d}_3 \otimes \bar{d}_4)$$
$$g_0(a_1, a_2, d_1 \otimes d_2, d_3 \otimes d_4) = (a_2, a_1, d_3 \otimes d_4, d_1 \otimes d_2)$$

for all $(a_1, a_2, d_1 \otimes d_2, d_3 \otimes d_4)$ in B, where $\bar{d}$ is the conjugate of the complex number d. Then,

(1) B is a Galois extension with a G-Galois system:

$$\{x_1 = (1,0,0,0),\ x_2 = (i,0,0,0),\ x_3 = (j,0,0,0),\ x_4 = (k,0,0,0),$$
$$x_5 = (0,1,0,0),\ x_5 = (0,i,0,0),\ x_7 = (0,j,0,0),\ x_8 = (0,k,0,0),$$
$$x_9 = (0,0,1 \otimes 1,0),\ x_{10} = (0,0,\sqrt{-1} \otimes 1,0),$$
$$x_{11} = (0,0,1 \otimes \sqrt{-1},0),\ x_{12} = (0,0,\sqrt{-1} \otimes \sqrt{-1},0),$$
$$x_{13} = (0,0,0,1 \otimes 1),\ x_{14} = (0,0,0,\sqrt{-1} \otimes 1),$$
$$x_{15} = (0,0,0,1 \otimes \sqrt{-1}),\ x_{16} = (0,0,0,\sqrt{-1} \otimes \sqrt{-1});$$
$$y_l = \frac{1}{4}x_l \text{ for } l = 1,5,9,12,13,16,$$
$$y_l = -\frac{1}{4}x_l \text{ for } l = 2,3,4,6,7,8,10,11,14,15\}.$$

(2) $B^G = \{(r,r,r',r')\,|\,r \in R,\ r' \in R \otimes_R R\} \cong R \oplus R$.

(3) $C = R \oplus R \oplus (D \otimes_R D) \oplus (D \otimes_R D)$.

(4) By (1), (2), and (3), B is a Galois algebra over $R \oplus R$ with Galois group G, but not a central Galois algebra with Galois group G.

(5) $H = \{g \in G \mid g(c) = c \text{ for each } c \in C\} = \{1\}$, and so B is not a central Galois algebra with Galois group H.

(6) Let $e_1 = (1,1,0,0)$ and $e_2 = (0,0,1,1)$. Then $B = Be_1 \oplus Be_2$ where $Be_1 = R[i,j,k] \oplus R[i,j,k]$ is a Galois algebra with Galois group $G|_{Be_1} \cong G$, and Be_1 is a composition of a central Galois algebra and a commutative Galois algebra as given in Example 1.

References

[1] F.R. DeMeyer and E. Ingraham, Separable algebras over commutative rings, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

[2] F.R. DeMeyer, *Some Notes on the General Galois Theory of Rings*, Osaka J. Math. **2** (1965) 117–127.

[3] M. Harada, *Supplementary Results on Galois Extension*, Osaka J. Math. **2** (1965), 343–350.

[4] T. Kanzaki, *On Galois Algebra Over A Commutative Ring*, Osaka J. Math. **2** (1965), 309–317.

[5] S. Ikehata and G. Szeto, On H-skew polynomial rings and Galois extensions, Rings, Extension and Cohomology (Evanston, IL, 1993), 113-121, Lecture Notes in Pure and Appl. Math., 159, Dekker, New York, 1994.

[6] A. Rosenberg and D. Zelinsky, *Automorphisms of Separable Algebras*, Pacific J. Math. **11** (1961), 1109–1117.

[7] K. Sugano, *On a Special Type of Galois Extensions*, Hokkaido J. Math. **9** (1980) 123–128.

[8] S. Szeto and L. Xue, *On Three types of Galois Extensions of Rings*, Southeast Asian Bulletin of Mathematics **23** (1999) 1–6.

[9] S. Szeto and L. Xue, *On Characterizations of a Center Galois Extension*, International Journal of Mathematics and Mathematical Sciences **23** (2000), 753–758.

Department of Mathematics
Bradley University
Peoria, Illinois 61625, USA

E-mail: `szeto@hilltop.bradley.edu`

E-mail: `lxue@hilltop.bradley.edu`