ON FREE RING EXTENSIONS OF DEGREE n

GEORGE SZETO

Mathematics Department
Bradley University
Peoria, Illinois 61625 U.S.A.

(Received June 25, 1980)

ABSTRACT. Nagahara and Kishimoto [1] studied free ring extensions $B(x)$ of degree n for some integer n over a ring B with 1, where $x^n = b$, $cx = x\rho(c)$ for all c and some b in B (ρ = automorphism of B), and $\{1, x, \dots, x^{n-1}\}$ is a basis. Parimala and Sridharan [2], and the author investigated a class of free ring extensions called generalized quaternion algebras in which $b = -1$ and ρ is of order 2. The purpose of the present paper is to generalize a characterization of a generalized quaternion algebra to a free ring extension of degree n in terms of the Azumaya algebra. Also, it is shown that a one-to-one correspondence between the set of invariant ideals of B under ρ and the set of ideals of $B(x)$ leads to a relation of the Galois extension B over an invariant subring under ρ to the center of B .

KEY WORDS AND PHRASES. Free ring extensions, separable algebras, Azumaya algebras, Galois extensions.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: 16A16, 13A20, 13B05.

1. INTRODUCTION.

Kishimoto [3], and Nagahara and Kishimoto [1] studied free ring extensions of

degree 2 and n for an integer $n > 2$: (1) $B(x)$ is a free ring extension over a ring B with 1 with a basis $\{1, x\}$ such that $x^2 = xa + b$ for some a and b in B , and $cx = x\rho(c)$ for each c in B , where ρ is a ring automorphism of B of order 2. (2) $B(x)$, a free ring extension of degree $n > 2$ is similarly defined with a basis $\{1, x, \dots, x^{n-1}\}$, and $x^n = b$ for some b in B and $cx = x\rho(c)$ for each c in B , where ρ is of order n . Some special free ring extensions called generalized quaternion algebras were investigated by Parimala and Sridharan [2] and the author Szeto ([4] - [5]). One of their results is a characterization of the Galois extension of B over a subring ([2], Proposition 1.1): Let $B(x)$ be a generalized quaternion algebra ($x^2 = -1$) over a commutative ring B with 2 a unit in B . Then B is Galois over A ($=\{a \text{ in } B/\rho(a) = a \text{ for an automorphism } \rho \text{ of order } 2\}$) if and only if $B \otimes_A B(x)$ is a matrix algebra of order 2. The above characterization was generalized to a free ring extension of degree n , $B(x)$ with $x^n = -1$ ([4], Theorems 3.4 and 3.5). The purpose of the present paper is to continue the above generalization to a free ring extension. Also, we shall show that there is a one-to-one correspondence between the set of invariant ideals of B under ρ and the set of ideals of $B(x)$. This correspondence will lead to a relation of the Galois extension B over the invariant subring A under ρ to the center Z of B over A .

2. PRELIMINARIES.

Throughout, we assume that B is a ring (not necessarily commutative) with 1, ρ an automorphism of B of order n for some positive integer n , $A = \{a \text{ in } B/\rho(a) = a\}$, and $B(x)$ a free ring extension over B with a basis $\{1, x, \dots, x^{n-1}\}$ such that $x^n = b$ and $ax = x\rho(a)$ for some b and all a in B (hence $\rho(b) = b$ ([1], p. 20)). Let T be a ring containing a subring R with 1. Then T is called a separable extension over R if there exist elements $\{u_i, v_i / i = 1, \dots, m \text{ for some integer } m\}$ such that $a(\sum u_i \otimes v_i) = (\sum u_i \otimes v_i)a$ for all a in T where $\otimes$ is over R and $\sum u_i v_i = 1$ ([6], [7]). Such an element $\sum u_i \otimes v_i$ is called a separable idempotent for T . If R is in the center of T , the separable extension T is called a separable R -algebra. In particular, if R is the center of T , the separable R -algebra T is called an Azumaya R -algebra ([6], [7]). A commutative ring extension S of R is called a

splitting ring for the Azumaya R -algebra T if $S\hat{\otimes}_R T \cong \text{Hom}_S(P, P)$ for a progenerator S -module P ([6], [7]). The ring extension T over R is called a Galois extension with a finite automorphism group G (Galois group) if (1) $R = \{a \in T / \alpha(a) = a \text{ for all } \alpha \in G\}$, and (2) there exist elements $\{u_i, v_i \in T / i = 1, \dots, m \text{ for some integer } m\}$ such that (1) $\sum u_i v_i = 1$, and (2) $\sum u_i \alpha(v_i) = 0$ for each $\alpha \neq \text{the identity of } G$ ([7], [8]).

3. A GENERAL PARIMALA-SRIDHARAN THEOREM.

In this section, we shall generalize the Parimala-Sridharan [2] theorem to a free ring extension $B(x)$ of degree n for an integer n such that $x^n = b$ and $ax = x\rho(a)$ for some b and all a in B where ρ is an automorphism of B of order n . We note that if $B(x)$ is separable over B then b is a unit ([1], Proposition 2.4). The converse holds if n is also a unit:

LEMMA 3.1. If n and b are units, then $B(x)$ is a separable extension over B .

PROOF. Since b is in A ([1], p. 20) and since $\rho^n = \text{the identity}$, it is straightforward to verify that the element $u = b^{-1} n^{-1} (\sum_{i=0}^{n-1} x^i \rho^i(x^{n-1-i}))$ satisfies the equations: $au = ua$ for all a in $B(x)$, and $b^{-1} n^{-1} (\sum x^i x^{n-1-i}) = 1$, where ρ is over B .

We remark here that there are separable extensions with n ($\neq 2$) not a unit ([4], Theorem 4.2). With the same proof as given for Proposition 1.2 in [7] we have a characterization for Galois extensions of non-commutative rings:

LEMMA 3.2. Let B be a ring extension of A with a finite automorphism group G such that $A = B^G$ ($=\{a \in B / \alpha(a) = a \text{ for each } \alpha \in G\}$). Then B is Galois over A if and only if the left ideal generated by $\{a - \alpha(a) / \text{for } a \in B\} = B$ for any $\alpha \neq \text{the identity of } G$.

THEOREM 3.3. Let n and b be units in B . If B is Galois over A which is contained in the center Z of B with a Galois group $\{1, \rho, \dots, \rho^{n-1}\}$ of order n , then the free ring extension $B(x)$ of degree n is an Azumaya A -algebra, where $x^n = b$ and $cx = x\rho(c)$ for each c in B .

PROOF. By Lemma 3.1, $B(x)$ is separable over B . Since B is Galois over A , B is separable over A . Hence $B(x)$ is separable over A ([4], the proof of Theorem 3.4).

So, it suffices to show that the center of $B(x)$ is A . Let $u = \sum_{i=0}^{n-1} a_i x^i$ be in the center. Then $xu = ux$. Noting that $\{1, x, \dots, x^{n-1}\}$ is a basis for $B(x)$ over B , we have that a_i are in A . Also, $au = ua$ for all a in B , so $a_i(a - \rho^i(a)) = 0$ for each $i \neq 0$. Hence the central elements a_i are in the left annihilators of the left ideal generated by $\{a - \rho^i(a) \mid a \in B\}$ for $i \neq 0$. By hypothesis, B is Galois over A , so $a_i = 0$ for each $i \neq 0$ by Lemma 3.2. Thus $u = a_0$ in A . Clearly, A is in the center of $B(x)$. Therefore, A = the center of $B(x)$.

By the Parimala-Sridharan theorem ([3], Proposition 1.1), let $B(x)$ be a generalized quaternion algebra ($x^2 = -1$) over a commutative ring B . Then, B is Galois over A ($= \{a \in B \mid \rho(a) = a \text{ for an automorphism } \rho \text{ of order } 2\}$) if and only if $B \otimes_A B(x)$ is a matrix algebra of order 2 over B . Hence, Theorem 3.3 generalizes the necessity of the Parimala-Sridharan theorem. For the sufficiency, we first give a one-to-one correspondence between the sets of ideals of B , of $B(x)$, of A , and the center Z of B . An ideal I of B is called a G-ideal if $\rho(I) = I$. Since $\rho(Z) = Z$, a G-ideal J of Z is similarly defined, where $G = \{1, \rho, \dots, \rho^{n-1}\}$.

THEOREM 3.4. Let $B(x)$ be an Azumaya A -algebra. Then there exists a one-to-one correspondence between (1) the set of G-ideals of B , (2) the set of ideals of $B(x)$, and (3) the set of ideals of A .

PROOF. At first, we want to give a structure of a G-ideal I of B . Since $\rho(I) = I$, $xIB(x) \subset \rho^{-1}(I)B(x) = IB(x)$. Hence $IB(x)$ is an ideal of $B(x)$. By hypothesis, $B(x)$ is an Azumaya A -algebra, so $IB(x) = I_0 B(x)$ where $I_0 = IB(x) \cap A$ ([7], Corollary 3.7, p. 54). Noting that $\{1, x, \dots, x^{n-1}\}$ is a basis for $B(x)$ over B , we have $I = I_0 B$ and $I_0 = I \cap A$. Next, it is easy to see that $J_0 B$ is a G-ideal of B for any ideal J_0 of A . Thus the set of G-ideals of B are in one-to-one correspondence with the set of ideals of A from the above representation $I_0 B$ of a G-ideal I of B . By hypothesis again, $B(x)$ is an Azumaya A -algebra, so the set of ideals of $B(x)$ and the set of ideals of A are in one-to-one correspondence under $I_0 B(x) \leftrightarrow I_0$ for an ideal I_0 of A . Thus the theorem is proved.

COROLLARY 3.5. Let n and b be units in B . Suppose B is Galois over A which is contained in Z . Then there exists a one-to-one correspondence between the set of G-ideals of Z and the set of ideals of $B(x)$.

PROOF. Since B is Galois over A , B is a separable A -algebra. Hence B is Azumaya over its center Z ([7], Theorem 3.8, p. 55). Thus the set of G -ideals of B and the set of G -ideals of Z are in one-to-one correspondence; and so Theorem 3.4 implies the corollary.

Now we show a generalization of the sufficiency of the Parimala-Sridharan theorem. The set $\{a \text{ in } B / \rho(a) = a\}$ is denoted by B^0 . Let G' be an automorphism group, $\{1, \dots, \rho^{m-1}\}$ obtained from $G (= \{1, \dots, \rho^{n-1}\})$ by taking m as the minimal integer such that $\rho^m = \text{the identity on } Z$. We denote the ideal generated by $\{a - \rho^i(a) / a \text{ in } Z\}$ by I_i for $i = 1, \dots, m-1$. It is easy to see that each I_i is a G -ideal such that $I_{m-1} \subset I_{m-2} \subset \dots \subset I_1$. We shall show that the chain of I_i 's characterizes the Galois extension of Z over A . That is:

THEOREM 3.6. If $B(x)$ is an Azumaya A -algebra such that $I_1 = I_2 = \dots = I_{m-1}$, then Z is Galois over A with a Galois group G' .

PROOF. In case $Z = A$, the theorem is trivial. Let $Z \neq A$. Then $m \neq 0$. Clearly, $A = B^G = B^0 = Z^0 = Z^{G'}$. Now we assume Z is not Galois over A . Then the ideal I_1 of Z is not Z ([7], Proposition 1.2, p. 80) since $I_1 = I_2 = \dots = I_{m-1}$ by hypothesis. Since I_1 is a G -ideal, $I_1 = IZ$ for some ideal I of A by Theorem 3.4. Hence $B(x)/I_1 B(x) \cong A/I \otimes_A B(x)$ is an Azumaya A/I -algebra ([7], Proposition 1.11, p. 46). But $\bar{a} = \rho(\bar{a})$ in $B(x)/I_1 B(x)$ for each a in Z , so $\bar{a}\bar{x} = \overline{\rho(a)x} = \bar{x}\bar{a}$. This implies that $\bar{Z}$ is contained in the center A/I of the Azumaya A/I -algebra $A/I \otimes_A B(x)$. This is impossible since Z is not contained in A . Thus Z is Galois over A .

COROLLARY 3.7. By keeping the notations of Theorem 3.6, if B is Galois over A with a Galois group $G (= \{1, \rho, \dots, \rho^{n-1}\})$ such that $I_1 = I_2 = \dots = I_{m-1}$, then Z is Galois over A with a Galois group G' , where b and n are units in B .

PROOF. Theorem 3.3 implies that $B(x)$ is an Azumaya A -algebra, so the corollary is a consequence of Theorem 3.6.

As given in Theorem 3.6, let $B(x)$ be an Azumaya A -algebra. If B is commutative, $B = Z$. Now assume B is not Galois over A . Then there is an I_i for some $i = 1, \dots, m-1$ such that $I_i \neq Z$. One can show as given in Theorem 3.6 that $A/I_i \otimes_A B(x)$ is an Azumaya algebra such that x^i is in the center A/I_i . Thus we have a contradiction. This proves that B is Galois over A . So, Theorem 3.6 generalizes Theorems 3.4 and

and 3.5 in [4].

4. SPLITTING RINGS.

In this section, we shall show that if $B(x)$ is an Azumaya A -algebra in which b and n are units, then $A(x)$ is a splitting ring for $B(x)$ such that $A(x)$ is a chain of Galois extensions of degree 2 (that is, $A(x) \supset A(x^2) \supset \dots \supset A(x^n) = A$, such that $A(x^i)$ is Galois over $A(x^{2i})$).

THEOREM 4.1. Let A be a commutative ring with 1, $x^n = b$ in A , and $ax = xa$ for each a in A . If b and n are units in A with n a power of 2 ($=2^m$ for some m), then $A(x)$ is a chain of Galois extensions of degree 2.

PROOF. We define a mapping $\alpha: A(x) \rightarrow A(x)$ by $\alpha(x) = -x$ and $\alpha(\sum a_i x^i) = \sum a_i (\alpha(x))^i$ for $i = 0, 1, \dots, n-1$. Then it is straightforward to check that α is an automorphism of $A(x)$ of order 2 such that $(A(x))^\alpha = A(x^2)$. Since $n (= 2^m = 2 \cdot 2^{m-1})$ and $b (= x^n = (x^2)^{2^{m-1}})$ are units in A , 2 and x^2 are units in $A(x^2)$. Now we claim that $A(x)$ is Galois over $A(x^2)$ with a Galois group $\{1, \alpha\}$. In fact, let $a_1 = (2x^2)^{-1}x$, $a_2 = 2^{-1}$, $b_1 = x$ and $b_2 = 1$. Then we have $a_1 b_1 + a_2 b_2 = 1$ and $a_1 \alpha(b_1) + a_2 \alpha(b_2) = 0$. Thus $A(x)$ is Galois over $A(x^2)$ of degree 2. Similarly, we can show that $A(x^2)$ is Galois over $A(x^4)$ with a Galois group $\{1, \beta\}$ with $\beta(x^2) = -x^2$ of order 2. Therefore, an induction argument concludes the existence of a chain of Galois extensions of degree 2.

For the class of free ring extensions $B(x)$ of degree n as given in [1], Section 2 such that c and $(1-c^i)$ are units in A where $c^n = 1$ and $i = 1, 2, \dots, n-1$, we have:

THEOREM 4.2. Let A be a commutative ring with 1, $x^n = b$ which is a unit in A , and $ax = xa$ for each a in A . If there is an c in A such that n and $(1-c^i)$ are units in A for $i = 1, \dots, n-1$ with $c^n = 1$, then $A(x)$ is Galois over A .

PROOF. We define a mapping $\alpha: A(x) \rightarrow A(x)$ by $\alpha(x) = cx$ and $\alpha(\sum a_i x^i) = \sum a_i (cx)^i$. Then one can check that $(A(x))^\alpha = A$ and that α is an automorphism of $A(x)$ of order n (for $1-c^i$ are units in A for $i = 1, 2, \dots, n-1$). Moreover, since $(1-c)$ is a unit in A , $(x-\alpha(x)) = x-cx = (1-c)x$ is also a unit (for x is also a unit). Therefore, $A(x)$ is Galois over A with a Galois group $\{1, \dots, \alpha^{n-1}\}$ ([7], Proposition 1.2, p. 80).

As given in Theorem 3.3, if B is Galois over A , $B(x)$ is an Azumaya A -algebra. We are going to show the existence of a splitting ring for the Azumaya A -algebra $B(x)$.

THEOREM 4.3. Let $B(x)$ be an Azumaya A -algebra with b and n as units in A . Then $A(x)$ is a splitting ring for $B(x)$. Moreover, if n is a power of 2, the splitting ring $A(x)$ is a chain of Galois extensions of degree 2, and if c and $(1-c)^{-1}$ are units in A where $c^n = 1$, then $A(x)$ is Galois over A .

PROOF. Since b and n are units in A , the element $u = (nb)^{-1} \left(\sum_{i=0}^{n-1} x^i \otimes x^{n-i} \right)$ satisfies the equations: $ua = au$ for each a in $A(x)$ and $(nb)^{-1} \left(\sum_{i=0}^{n-1} x^i \otimes x^{n-i} \right) = 1$. Hence $A(x)$ is a separable A -algebra. Moreover, one can show directly that $A(x)$ is a maximal subcommutative ring of $B(x)$ by showing that the commutant of $A(x)$ in $B(x)$ is $A(x)$. Thus $A(x)$ is a splitting ring for $B(x)$ ([7], Theorem 5.5, p. 64). The other results of the theorem are consequences of Theorems 4.1 and 4.2.

Theorem 4.1 is a generalization of Theorem 4.2 in [4] for quadratic free ring extensions, while Theorem 4.3 proves the existence of a splitting ring for $B(x)$, other than B when B is commutative ([2], Proposition 1.1 and [5], Theorem 3.2).

REFERENCES

1. NAGAHARA, T. and KISHIMOTO, K. On Free Cyclic Extensions of Rings, Math. J. Okayama Univ. (1978), 1-25.
2. PARIMALA, S. and SRIDHARAN, R. Projective Modules over Quaternion Algebras, J. Pure Appl. Algebra **9** (1977), 181-193.
3. KISHIMOTO, K. A Classification of Free Extensions of Rings, Math. J. Okayama Univ. **181** (1976), 139-148.
4. SZETO, G. On Generalized Quaternion Algebras, Internat. J. Math. Math. Sci. **2** (1980), 237-245.
5. SZETO, G. A Characterization of a Cyclic Galois Extension of Commutative Rings, J. Pure Appl. Algebra **16** (1980), 315-322.
6. AUSLANDER, M. and GOLDMAN, O. The Brauer Group of a Commutative Ring, Trans. Amer. Math. Soc. **97** (1960), 367-409.
7. DeMEYER, F. and INGRAHAM, E. Separable Algebras over Commutative Rings, Springer-Verlag- Berlin-Heidelberg-New York, 1971.
8. CHASE, S., HARRISON, D. and ROSENBERG, A. Galois Theory and Galois Cohomology of Commutative Rings, Mem. Amer. Math. Soc. **52** (1965).
9. MIYASHITA, Y. Finite Outer Galois Theory of Non-commutative Rings, J. Fac. Sci. Hokkaido Univ. Ser. I, **19** (1966), 114-134.