Internat. J. Math. & Math. Sci.
Vol. 7 No. 1 (1984) 103-108

ON AUTOMORPHISM GROUP OF FREE QUADRATIC EXTENSIONS OVER A RING

GEORGE SZETO

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

(Received March 8, 1983 and in Revised Form November 11, 1983)

ABSTRACT. Let R be a ring with 1, ρ an automorphism of R of order 2. Then a normal extension of the free quadratic extension $R[x,\rho]$ with a basis $\{1,x\}$ over R with an R-automorphism group G is characterized in terms of the element $(x-(x)\alpha)$ for α in G. It is also shown by a different method from the one given by Nagahara that the order of G of a Galois extension $R[x,\rho]$ over R with Galois group G is a unit in R. When 2 is not a zero divisor, more properties of $R[x,\rho]$ are derived.

KEY WORDS AND PHRASES. Free quadratic extensions, normal extensions, Galois extensions.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. 16A74, 16A72.

1. INTRODUCTION.

Let C be a commutative ring with 1 and with a finite automorphism group G. Then it is well known that C is Galois over C^G (= $\{r$ in C / $(r)\alpha = r$ for each α in $G\}$) with Galois group G if and only if the ideal generated by $\{(r-(r)\alpha)$ / r in C and α in $G\}$ is C ([1], or [2], Proposition 1.2, P. 81). The sufficiency of such a characterization of Galois extensions for non-commutative rings does not hold. However, for free quadratic extensions $R[x,\rho]$ (see definition below) with respect to an automorphism ρ of R (not necessarily commutative), the above characterization becomes that $R[x,\rho]$ is Galois over R with Galois group G if and only if $G = \{1,\alpha / \alpha^2 = 1\}$ and $(x-(x)\alpha)$ is a unit in $R[x,\rho]$ ([3], Lemma 2.3). In fact, the element $(x-(x)\alpha)$ will play an important role in the study of $R[x,\rho]$. The purposes of the present paper are to characterize a normal extension $R[x,\rho]$ over R with an R-automorphism group G in terms of the elements $(x-(x)\alpha)$ for α in G, and to show by a different method from the one given by Nagahara ([3], Lemma 2.3) that 2 is a unit in R if $R[x,\rho]$ is Galois over R. More properties of $R[x,\rho]$ are derived from the informations of $(x-(x)\alpha)$ when 2 is not a zero divisor. At the end, examples are given to demonstrate our results.

2. PRELIMINARIES.

Throughout, let R be a ring with 1, and ρ an automorphism of R of order 2. Then a free quadratic extension $R[x,\rho]$ with respect to ρ is a ring with a free basis $\{1,x\}$ over R such that $rx = x(r\rho)$, $x^2 = b$ which is an element in $U(C^\rho)$ (= the set of units in the center C such that $(b)\rho = b$) ([4], [5], [6] , and [3]). An R-automorphism α of $R[x,\rho]$ is a ring automorphism such that $(r+xt)\alpha = r+((x)\alpha)t$ for r and t in R. A ring T is called a normal extension of a subring S with respect to an automorphism group G of T if $T^G = S$, where $T^G = \{t \text{ in } T / (t)\alpha = t \text{ for each } \alpha \text{ in } G\}$. A ring T is called a Galois extension over S with a finite Galois group G if it is normal over S and if there are elements $\{a_i, b_i \text{ in } T / i = 1, \ldots, n \text{ for some integer } n\}$ such that $\sum a_i b_i = 1$ and $\sum a_i (b_i)\alpha = 0$ for each $\alpha \neq 1$ in G ([7], or [2], P. 81).

3. NORMAL AND GALOIS EXTENSIONS.

In this section, we shall characterize a normal extension $R[x,\rho]$ in terms of the elements $\{(x-(x)\alpha) / \alpha \text{ in } G\}$, where G is an R-automorphism group of $R[x,\rho]$. When G is of order 2, it is known. Hence we have a different method from Nagahara ([3], Lemma 2.3) to show that 2 is a unit in R if $R[x,\rho]$ is Galois over R with Galois group G. We begin with several lemmas.

LEMMA 3.1. The R-linear map α such that $(x)\alpha = p+xq$ for some p, q in R is an R-automorphism of $R[x,\rho]$ if and only if (1) $rp = p(r\rho)$ for each r in R, and $(p\rho) = -p$, (2) q is in U(C), the set of units in the center C, and (3) $p^2+b(q\rho)q = b$ where $x^2 = b$ in $U(C^\rho)$.

PROOF. Since $r(x\alpha) = (rx)\alpha = (x(r\rho))\alpha = (x\alpha)(r\rho)$, conditions (1) and (2) hold immediately. Using that $(x\alpha)^2 = (x^2)\alpha = b$, we have condition (3). The converse is straightforward.

Let α be an R-automorphism of $R[x,\rho]$, and $A^r(x-(x)\alpha)$ the right annihilator of $(x-(x)\alpha)$ in R. Then we have:

LEMMA 3.2. $R[x,\rho]$ is normal over R with respect to an automorphism group G if and only if $\bigcap_\alpha A^r(x-(x)\alpha) = \{0\}$ for all α in G.

PROOF. Since $(x-(x)\alpha)r = xr-(xr)\alpha$ for r in R and α in G, $(x-(x)\alpha)r = 0$ if and only if $xr = (xr)\alpha$. But (xr) is in R if and only if $r = 0$, so the lemma follows.

LEMMA 3.3. Assume 2 is not a zero divisor in R. Let $(x)\alpha = p+xq$, for some α in G. Then $p^2 = 0$ and $(q)\rho = q^{-1}$.

PROOF. Since $(p)\rho = -p$ and $rp = p(r\rho)$ by condition (1) of Lemma 3.1, $p^2 = -p^2$ (for $r = p$). Hence $2p^2 = 0$. But 2 is not a zero divisor by hypothesis, so $p^2 = 0$. By condition (3) of Lemma 3.1, $p^2+b(q\rho)q = b$, so $(q\rho)q = 1$. Thus $(q\rho) = q^{-1}$.

Lemma 3.2 gives a different method from the one given by Nagahara ([3], Lemma 1.1) to show the normality of $R[x,\rho]$ over R with respect to an R-automorphism group G.

THEOREM 3.4. (T. Nagahara) If $(x-(x)\alpha)$ is not a zero divisor in $R[x,\rho]$, then $R[x,\rho]$ is a normal extension over R with respect to the cyclic R-automorphism group $\langle\alpha\rangle$.

PROOF. Assume $R[x,\rho]$ is not normal over R with respect to $\langle\alpha\rangle$. Then $A^r(p)\cap A^r(1-q) \neq \{0\}$ by Lemma 3.2. Let $u \neq 0$ be in the intersection. Then $(x-(x)\alpha)u = (-p+x(1-q))u = 0$. This contradicts to that $(x-(x)\alpha)$ is not a zero divisor. Thus $R[x,\rho]$ is normal.

The converse of Theorem 3.4 holds in case 2 is not a zero divisor.

THEOREM 3.5. Assume 2 is not a zero divisor in R. If $R[x,\rho]$ is a normal extension over R with respect to a cyclic R-automorphism group $\langle\alpha\rangle$, then $(x-(x)\alpha)$ is not a zero divisor in $R[x,\rho]$.

PROOF. Let $(x)\alpha = p+xq$ for some p, q in R. Then $A^r(x-(x)\alpha) = A^r(p)\cap A^r(1-q)$. Now let $R[x,\rho]$ be a normal extension over R with respect to $\langle\alpha\rangle$. Then

$A^r(p) \cap A^r(1-q) = \{0\}$ by Lemma 3.2. For $u+xv$ in $R[x,\rho]$ such that $(x-(x)\alpha)(u+xv) = 0$, we have that $-pu+b((1-q)\rho)v = 0$ and $pv+(1-q)u = 0$ ... (*). By multiplying p in equation (*), Lemma 3.3 implies that $p((1-q)\rho)v = 0$ and $p(1-q)u = 0$ ... (**) (for b is in $U(C^\rho)$). By Lemma 3.3 again, $(q)\rho = q^{-1}$ which is in U(C), so $p(1-q)v = 0$ and $p(1-q)u = 0$ from equations (**). Hence pv and pu are in $A^r(1-q)$. But $p^2 = 0$, so pv and pu are also in $A^r(p)$. Thus pv and pu are in $A^r(p) \cap A^r(1-q)$ which is 0, and so pv and pu are 0. This implies that v and u are in $A^r(p)$. But then equations (*) become that $(1-q)\rho \cdot v = 0$ and $(1-q)u = 0$. Noting that $(q)\rho = q^{-1}$, we have that $(1-q)v = 0$ and $(1-q)u = 0$. Thus v and u are also in $A^r(1-q)$. Therefore, v and u are in $A^r(p) \cap A^r(1-q)$ which is 0; and so $v = 0$ and $u = 0$. Similarly, we can show that $(u+xv)(x-(x)\alpha) = 0$ implies that $v = 0$ and $u = 0$. Thus $(x-(x)\alpha)$ is not a zero divisor.

Next, we determine all R-automorphism groups of $R[x,\rho]$ of order 2 such that $R[x,\rho]$ is a normal extension over R.

THEOREM 3.6. Let $R[x,\rho]$ be a normal extension over R with respect to a cyclic automorphism group $\langle\alpha\rangle$. Then, the order of α is 2 if and only if $(x)\alpha = p-x$ such that $rp = p((r)\rho)$, $(p)\rho = -p$, and $p^2 = 0$.

PROOF. Let $(x)\alpha = p+xq$ for p, q in R satisfying three conditions of Lemma 3.1 and $\alpha^2 = 1$. Then $(x)\alpha^2 = (x\alpha)\alpha = x$. This implies that $p+pq = 0$ and $q^2 = 1$. Hence $p(1+q) = 0$ and $(1-q)(1+q) = 0$. But then $(1+q)$ is in $A^r(p) \cap A^r(1-q)$. By hypothesis, $R[x,\rho]$ is normal over R with respect to $\langle\alpha\rangle$, so $q = -1$ by Lemma 3.2. Also, by condition 3 of Lemma 3.1, $p^2+b((-1)\rho)(-1) = b$, so $p^2 = 0$. Thus, $(x)\alpha = p-x$ such that $rp = p(r\rho)$, $p\rho = -p$ (Lemma 3.1), and $p^2 = 0$. The converse is easy to verify.

We are going to show that 2 is a unit in R if $R[x,\rho]$ is Galois over R by a different method from Lemma 2.3 in [3].

COROLLARY 3.7. If $R[x,\rho]$ is Galois over R with Galois group G, then 2 is a unit in R.

PROOF. By Lemma 1.2 in [3], the Galois group G of $R[x,\rho]$ is of order 2 and $(x-(x)\alpha)$ is a unit, where $G = \langle\alpha\rangle$. But $R[x,\rho]$ is normal over R with respect to $\langle\alpha\rangle$. This implies that $2bv-pu = 1$ ... (1), and $2u+pv = 0$ ... (2). Multiplying p in (2), we have $2pu = 0$ (for $p^2 = 0$ by Theorem 3.6). But $p(pu) = 0$, so pu is in $A^r(2) \cap A^r(p)$ which is $\{0\}$ by Lemma 3.2. Thus $pu = 0$. Thus equation (1) becomes $2bv = 1$. Therefore, 2 is a unit in R.

The following are more properties of $A^r(x-(x)\alpha)$.

THEOREM 3.8. Assume 2 is not a zero divisor. Then (1) $A^r(x-(x)\alpha)$ is an invariant ideal I of R under ρ (that is, $(I)\rho = I$), and (2) $A^r(x-(x)\alpha) = A^l(x-(x)\alpha)$, the left annihilator of $(x-(x)\alpha)$ in R.

PROOF. (1) For r, s in I and t in R, clearly, $(r-s)$ and (rt) are in I. Since $(x-(x)\alpha)tr = (t\rho)(x-(x)\alpha)r = 0$, (tr) is in I. Hence I is an ideal of R. Also, let $(x)\alpha = p+xq$ for p, q satisfying 3 conditions in Lemma 3.1. Then $(x-(x)\alpha)r = 0$ if and only if $-pr = 0$ and $(1-q)r = 0$. Hence $(-pr)\rho = 0$ and $((1-q)r)\rho = 0$; that is, $p(r\rho) = 0$ and $(1-q)(r\rho) = 0$ (for $(p)\rho = -p$ and $(q)\rho = q^{-1}$ by Lemma 3.3). Thus $(r\rho)$ is in I.

(2) Let r be in I. Then $(r\rho)$ is in I by Part (1). Since $r(x-(x)\alpha) = (x-(x)\alpha)(r\rho) = 0$, r is in $A^l(x-(x)\alpha)$. Conversely, let r be in $A^l(x-(x)\alpha)$. Then $r(x-(x)\alpha) = (x-(x)\alpha)(r\rho) = 0$. Hence $(r\rho)$ is in I. Thus r $(= (r\rho)\rho)$ is in I.

4. EXAMPLES.

We conclude the paper with three examples to demonstrate the results in Section 3. 1. Let Z be the ring of integers, and ρ an automorphism of R $(= Z[\sqrt{3}])$ defined by $(n+m\sqrt{3})\rho = n-m\sqrt{3}$ in R. Then $R[i,\rho]$ is normal over R, where $i^2 = -1$, with respect to an R-automorphism group $\langle\alpha\rangle$ such that $(i)\alpha = -i$.

2. By replacing Z with Z/(4), Example 1 becomes a non-normal extension.

3. Let Q be the rational field. By replacing Z with Q, Example 1 becomes a Galois extension over R with Galois group $\langle\alpha\rangle$.

ACKNOWLEDGEMENT. This paper is written during the author's sabbatical leave at the University of Chicago. The author wishes to thank Professor I. Herstein for his excellent lectures on Galois theory. The author would also like to thank the referee for his valuable comments and suggestions.

REFERENCES

1. CHASE, S., HARRISON, D. AND ROSENBERG, A. Galois Theory and Galois Cohomology of Commutative Rings, Mem. Amer. Math. Soc. 52 (1965).

2. DeMEYER, F and INGRAHAM, E. Separable Algebras over Commutative Rings, Springer-Verlag-Berlin-Heidelberg-New York, 1971.

3. NAGAHARA, T. On Separable Polynomials of Degree 2 in Skew Polynomial Rings, Math. J. Okayama Univ., 19 (1976), 65-95.

4. PARIMULA, S.and SRIDHARAN, R. Projective Modules over Quaternion Algebras, J. Pure Appl. Algebra 9 (1977), 181-193.

5. SZETO, G. A Characterization of a Cyclic Galois Extension of Commutative Rings, J. Pure Appl. Algebra 16 (1980), 315-322.

6. SZETO, G. On Free Ring Extensions of Degree N, Internat. J. Math. and Math. Sci. 4 (1981), 703-709.

7. DeMEYER, F. Some Notes on the General Galois Theory of Rings, Osaka J. Math. 2 (1965), 117-127.