13. *Note on Cyclic Galois Extensions*

By Kozo SUGANO
Department of Mathematics, Hokkaido University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1981)

Introduction. As a generalization of central separable algebras, the notion of H-separable extension was introduced in [3]. Especially in the case where B is a commutative ring and A is a faithful B-algebra, A is an H-separable Galois extension of B if and only if A is central Galois extension of B. But in the case where B is non-commutative, there are some properties which hold in H-separable extensions of B but do not hold in central Galois extensions. Especially by Theorem 11 [2] there is no central cyclic Galois extension, while we could find some examples of H-separable cyclic Galois extensions in [11]. The aim of this paper is to show that if A is an H-separable Galois extension of B relative to a cyclic group $G=\langle\sigma\rangle$, then the centralizer of B in A is equal to the center of B (Theorem 1). We will also show that if A is an H-separable extension of B and the center of A is semi-local, then all elements of Aut $(A|B)$ are inner automorphisms (Theorem 2).

Definitions and symbols. Throughout this paper A will be a ring with the identity 1, B a subring of A which contains 1 of A and C and C' the centers of A and B, respectively. For any subset X of A, any ring automorphism σ of A and any A-A-module M, we will set respectively

$$V_A(X)=\{a\in A\,|\,ax=xa \text{ for all } x \text{ in } X\}$$
$$J_\sigma=\{a\in A\,|\,xa=a\sigma(x) \text{ for all } x \text{ in } A\}$$
$$M^A=\{m\in M\,|\,ma=am \text{ for all } a\in A\}.$$

Furthermore, by A_σ we denote an A-A-module such that $A_\sigma=A$ as left A-module and $ax=a\sigma(x)$ for $a\in A_\sigma$ and $x\in A$ as right A-module. Then we see $J_\sigma=(A_\sigma)^A$, $V_A(B)=A^B=(A_\sigma)^B$, $C=V_A(A)$ and $C'=V_B(B)$. Especially we will denote $D=V_A(B)$. A is an H-separable extension of B if and only if $A\otimes_B A$ is isomorphic to a direct summand of some $(A\oplus A\oplus\cdots\oplus A)$ (finite direct sum) as A-A-module. This condition is equivalent to the condition that for any A-A-module M $D\otimes_C M^A\cong M^B$ by $d\otimes m\to dm$ for $d\in D$ and $m\in M^A$ (see Theorem 1.2 [9]). Hence if A is an H-separable extension of B, $D=(A_\sigma)^B\cong D\otimes_C(A_\sigma)^A=D\otimes_C J_\sigma$. Thus J_σ is rank 1 C-projective, since D is C-finitely generated projective by Theorem 1.1 [3], and $DJ_\sigma=J_\sigma D=D$ for each $\sigma\in$ Aut $(A|B)$, where Aut $(A|B)$ denotes the group of all automorphisms of A which fix all elements of B. Furthermore, G will always stand for a finite group of ring automorphisms of A, and for any subgroup K of G we will set

$$A^K=\{a \in A \mid \sigma(a)=a \text{ for all } \sigma \text{ in } K\}.$$

A is a Galois extension of B relative to G if and only if $B=A^G$ and there exist x_i, y_i $(i=1, 2, \cdots, m)$ in A such that $\Sigma x_i\sigma(y_i)=\delta_{1\sigma}$ (Kronecker delta) for each $\sigma \in G$ (see [2] and [6]). Note that if A is a Galois extension of B relative to G, $D=\Sigma^{\oplus}_{\sigma\in G}J_\sigma$ by Proposition 1 [6].

Cyclic Galois extensions. The next lemma may already be known. But the author wishes to state here for completeness.

Lemma 1. *Let A be a Galois extension of B relative to G and R a subring of $C \cap B$. Then for any multiplicative subset S of R, A_S $(=A\otimes_R R_S)$ is a Galois extension of B_S $(=B\otimes_R R_S)$ relative to G.*

Proof. Let φ be the natural homomorphism of A to A_S and $\mathfrak{N}$ the kernel of φ, namely, $\varphi(x)=x\otimes 1$ for $x \in A$ and $\mathfrak{N}=\{a \in A \mid as=0$ for some s in $S\}$. Now it is obvious that for any $\sigma \in G$ we can obtain an automorphism $\bar{\sigma}$ of A_S by $\bar{\sigma}(x\otimes 1/s)=\sigma(x)\otimes 1/s$ for $x \in A$ and $s \in S$.

On the other hand there exist x_i, y_i $(i=1, 2, \cdots, m)$ in A such that $\Sigma x_i\sigma(y_i)=\delta_{1\sigma}$, since A is a Galois extension of B relative to G. Suppose $\bar{\sigma}=1_{A_S}$ for some $\sigma\neq 1$ in G. Then for any $x \in A$, $\sigma(x)-x \in \mathfrak{N}$. Hence $1=\Sigma x_iy_i-\Sigma x_i\sigma(y_i)=\Sigma x_i(y_i-\sigma(y_i)) \in \mathfrak{N}$, a contradiction. Therefore, we see that G acts on A_S faithfully. Next we will show $(A_S)^G=B_S$. Let $x\otimes 1/t \in (A_S)^G$ with $x \in A$ and $t \in S$. Then for each $\sigma \in G$, $(\sigma(x)-x)\otimes 1 =0$, and there exists $s_\sigma \in S$ such that $(\sigma(x)-x)s_\sigma=0$. Let $s=\prod s_\sigma$. Then $(\sigma(x)-x)s=\sigma(xs)-xs=0$ for all $\sigma \in G$. Hence $xs=r \in B=A^G$, and we have $x\otimes 1/t=r\otimes 1/st \in B_S$. Thus $(A_S)^G\subseteq B_S \cdot (A_S)^G\supseteq B_S$ is obvious. Finally it is clear that $x_i\otimes 1$, $y_i\otimes 1$ $(i=1, 2, \cdots, m)$ satisfy the condition of Galois extension. Thus A_S is a Galois extension of B_S relative to G.

Let us say that A is an inner Galois extension of B relative to G if A is a Galois extension of B relative to a Group G all of whose elements are inner automorphisms. Note that every inner Galois extension is an H-separable extension by Theorem 3 [10].

Proposition 1. *Let A be an H-separable Galois extension of B relative to G. Then for any prime ideal $\mathfrak{p}$ of C, $A_\mathfrak{p}$ is an inner Galois extension of $B_\mathfrak{p}$ relative to G.*

Proof. B is a C-algebra, since $B=V_A(V_A(B))\supset C$ by Proposition 3 (1) [10]. $A_\mathfrak{p}$ is a Galois extension of $B_\mathfrak{p}$ relative to G by Lemma 1 and also an H-separable extension of $B_\mathfrak{p}$ by Proposition 1.7 [9]. Let $\bar{C}$ be the center of $A_\mathfrak{p}$ and $\bar{D}=V_{A_\mathfrak{p}}(B_\mathfrak{p})$. Regarding $A_\mathfrak{p}$ as A-A-module, we have $\bar{C}=(A_\mathfrak{p})^{A_\mathfrak{p}}=(A_\mathfrak{p})^A$ and $\bar{D}=(A_\mathfrak{p})^{B_\mathfrak{p}}=(A_\mathfrak{p})^B$. Then since A is H-separable over B, we have $\bar{D}=(A_\mathfrak{p})^B\cong D\otimes_C(A_\mathfrak{p})^A=D\otimes_C\bar{C}$. Now let J_σ be as above and set $\bar{J}_\sigma=\{\alpha \in A_\mathfrak{p} \mid \beta\alpha=\alpha\sigma(\beta)$ for all β in $A_\mathfrak{p}\}$. Then $\bar{D}=\Sigma^{\oplus}_{\sigma\in G}\bar{J}_\sigma$ and $D=\Sigma^{\oplus}_{\sigma\in G}J_\sigma$ by Proposition 1 [6]. Hence we have $\Sigma^{\oplus}J_\sigma\otimes_C\bar{C}=\Sigma^{\oplus}\bar{J}_\sigma$. But $\varphi(J_\sigma)\bar{C}\subset\bar{J}_\sigma$ for each $\sigma \in G$, where φ is the natural map of A to $A_\mathfrak{p}$.

Therefore $J_\sigma \otimes_C \bar{C} \cong \bar{J}_\sigma$ for each $\sigma \in G$. Then since $\bar{C}$ is a $C_\mathfrak{p}$-algebra, and J_σ is rank 1 C-projective, $\bar{J}_\sigma \cong J_\sigma \otimes_C \bar{C} \cong J_\sigma \otimes_C C_\mathfrak{p} \otimes_{C_\mathfrak{p}} \bar{C} \cong C_\mathfrak{p} \otimes_{C_\mathfrak{p}} \bar{C} \cong \bar{C}$. Hence $\bar{J}_\sigma = \gamma \bar{C}$ for some $\gamma \in \bar{J}_\sigma$. Then since $A_\mathfrak{p}$ is H-separable over $B_\mathfrak{p}$, $\bar{D} = \bar{D}\bar{J}_\sigma = \bar{J}_\sigma \bar{D} = \gamma \bar{D} = \bar{D}\gamma$. Hence γ is a unit, and we have $\sigma(\alpha) = \bar{\gamma}^1 \alpha \gamma$ for all $\alpha \in A_\mathfrak{p}$.

Lemma 2. *Let σ be an inner automorphism of A of a finite order, and suppose that A is a Galois extension of B relative to $G = \langle \sigma \rangle$. Then we have $V_A(B) = C'$ and $V_A(C') = B$.*

Proof. There exists a unit u in D such that $\sigma(x) = u^{-1}xu$ for all $x \in A$. Then $J_{\sigma^i} = Cu^i$ for $i = 1, 2, \cdots, n-1$, where n is the order of σ. Since $\sigma^j(cu^i) = u^{-j}cu^iu^j = cu^i$ for each i, we have $\sigma^j | J_{\sigma^i} = \text{identity}$. Thus we have $D = \sum^{\oplus} J_{\sigma^i} \subset A^G = B$, which means that $D = V_B(B) = C'$. Finally since A is H-separable over B by Theorem 3 [10], we have $B = V_A(V_A(B)) = V_A(C')$ by Proposition 3 [10].

Theorem 1. *Let A be an H-separable Galois extension of B relative to a cyclic group $G = \langle \sigma \rangle$. Then we have $V_A(B) = C'$ and $V_A(C') = B$. Furthermore,* Aut $(A|B)$ *is Abelian.*

Proof. Let $\mathfrak{m}$ be any maximal ideal of C. Then by Proposition 1, $A_\mathfrak{m}$ is an inner Galois extension of $B_\mathfrak{m}$ relative to $G = \langle \sigma \rangle$. Hence $D_\mathfrak{m} \subseteq V_{A_\mathfrak{m}}(B_\mathfrak{m}) \subseteq B_\mathfrak{m}$ by Lemma 2. Thus $(D+B)_\mathfrak{m} = B_\mathfrak{m}$ for all maximal ideal $\mathfrak{m}$ of C. Then $D+B = B$ and $D \subset B$. Hence $D = C'$, and $V_A(C') = V_A(V_A(B)) = B$. Finally since Aut $(A|B) \subseteq \text{Hom}\,({}_BA_B, {}_BA_B) \cong C' \otimes_C C'$ by Proposition 3.1 [4], Aut $(A|B)$ is Abelian.

Automorphisms in H-separable extensions. First observe the following facts. If A is H-separable over B, D is C-finitely generated projective, and consequently ${}_CC < \oplus_C D$. Then for any $\sigma \in$ Aut $(A|B)$, we have $J_\sigma J_{\sigma^{-1}} = J_{\sigma^{-1}} J_\sigma = C$, because $DJ_\sigma = D$, $DJ_\sigma J_{\sigma^{-1}} = DJ_{\sigma^{-1}} = D$ and $J_\sigma J_{\sigma^{-1}} = (DJ_\sigma J_{\sigma^{-1}}) \cap C = D \cap C = C$. Thus J_σ is rank 1 C-projective.

Theorem 2. *Let A be an H-separable extension of B. Then all elements of* Aut $(A|B)$ *are inner automorphisms, if C is a semi-local ring.*

Proof. Let σ be any element of Aut $(A|B)$, and $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_r$ the set of all maximal ideals of C. Now we can follow the same lines as the proof of Lemma 1 [6]. Since $J_\sigma J_{\sigma^{-1}} = C$, we have $\mathfrak{m}_i J_\sigma \not\supset \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1} \mathfrak{m}_{i+1} \cdots \mathfrak{m}_r J_\sigma$ for each i $(1 \leqq i \leqq r)$. Hence there exists a_i in $\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1} \mathfrak{m}_{i+1} \cdots \mathfrak{m}_r J_\sigma$ such that $a_i \notin \mathfrak{m}_i J_\sigma$. Set $a = \Sigma a_i$. Then, $a \in J_\sigma$ and $a \notin \mathfrak{m}_i J_\sigma$ for each i. But J_σ is rank 1 C-projective. Hence $[J_\sigma/\mathfrak{m}_i J_\sigma : C/\mathfrak{m}_i] = 1$, and $J_\sigma/\mathfrak{m}_i J_\sigma = (a + \mathfrak{m}_i J_\sigma)C/\mathfrak{m}_i$. Thus we have $J_\sigma = aC + \mathfrak{m}_i J_\sigma$ for each maximal ideal $\mathfrak{m}_i$ of C. Hence $J_\sigma = aC$ by Nakayama's Lemma. Then $Da = aD = D$ $(= DJ_\sigma)$, and a is a unit. Hence σ is inner.

Corollary 1. *Let A be an H-separable extension of B such that $V_A(V_A(B)) = B$. Then if C' is a semi-local ring, all elements of* Aut

$(A|B)$ *are inner automorphisms.*

Proof. Let J be the Jacobson radical of C'. Then C'/J is semisimple artinean, and $C'=V_B(B)=D\cap B=V_D(D)\supset C$. Hence D is finitely generated as C'-module. Then D/JD is artinean, and we see that JD is contained in every maximal left ideal of D by Nakayama's Lemma. Hence D is also a semi-local ring. But C is a C-direct summand of D. Hence $\mathfrak{a}D\cap C=\mathfrak{a}$ for any ideal $\mathfrak{a}$ of C. This implies that every proper ideal of C is contained in a maximal left ideal of D. If $\mathfrak{m}$ and $\mathfrak{m}'$ are any two maximal ideals of C which are contained in a maximal left ideal $\mathfrak{l}$ of D, then $1\in\mathfrak{m}+\mathfrak{m}'\subset\mathfrak{l}$, a contradiction. Hence $\mathfrak{m}=\mathfrak{m}'$. Thus we see that C is a semi-local ring.

References

[1] F. Demeyer and E. Ingraham: Separable algebras over commutative rings. Lect. notes in Math., vol. 181, Springer (1971).

[2] F. Demeyer: Some note on the general Galois theory of rings. Osaka J. Math., **1**, 117–127 (1964).

[3] K. Hirata: Some types of separable extensions of rings. Nagoya Math. J., **33**, 107–115 (1968).

[4] ——: Separable extensions and centralizers of rings. ibid., **35**, 31–45 (1969).

[5] ——: Some remarks on separable extensions (to appear in Hokkaido Math. J.).

[6] T. Kanzaki: On Galois algebras over a commutative ring. Osaka J. Math., **2**, 309–317 (1965).

[7] ——: Note on abelian Galois algebras over a commutative ring. ibid., **3**, 1–6 (1966).

[8] K. Kishimoto: Note on cyclic extensions of rings. J. Fac. Sci. Shinshu Univ., **5**, 29–32 (1970).

[9] K. Sugano: Note on semisimple extensions and separable extensions. Osaka J. Math., **4**, 265–270 (1967).

[10] ——: Note on automorphisms in separable extensions (to appear in Hokkaido Math. J.).

[11] ——: On a special type of Galois extensions (to appear in Hokkaido Math. J.).

[12] ——: On Automorphisms in separable extensions of rings. Proc. 13th symposium of ring theory, 1980, Okayama, Japan (1980).