KŌDAI MATH. SEM. REP.
23 (1971), 198—203

A NOTE ON GALOIS EXTENSION OF SEPARABLE ALGEBRAS

By Akira Inatomi

Introduction. In [7], Kanzaki established a Galois theory of central separable algebras. Further Miyashita introduced the notion of outer G-Galois extension and extended the Galois theory of commutative rings (see [3]) to general rings in [8].

This note consists of three sections. In § 1 we shall show some property of a certain subalgebra in a separable algebra over a commutative ring. In § 2 we shall give some relationship between a Galois extension in the sense of Kanzaki and that in the sense of Miyashita. In § 3 we shall give a shorter proof of the following Harrison-Demeyer's theorem: Let A be an algebra over a commutative ring K. If A/K is a G-Galois extension and G is a cyclic group, then A is commutative.

Throughout this note all rings have identities, all modules are unitary and all ring homomorphisms carry the identity into the identity.

§ 1. Let K be a commutative ring. Let A and B be two K-algebras and $A\supset B$. We denote by B^0 the opposite algebra of B. If M is a left A-, right B-module, we can convert M into a left $A\underset{K}{\otimes} B^0$-module. In particular, A itself may be regarded as a left $A\underset{K}{\otimes} B^0$-module.

Now, let M be a left A-, right B-module. If we define the map of

$$\mathrm{Hom}_{A\underset{K}{\otimes} B^0}(A, M)\rightarrow M$$

by

$$h\longmapsto h(1),\ h\in \mathrm{Hom}_{A\underset{K}{\otimes} B^0}(A, M),$$

it is easily seen that the map induces an isomorphism

$$\alpha\colon \mathrm{Hom}_{A\otimes B^0}(A, M)\simeq M^B,$$

where M^B is the subset of M consisting of all m in M such that $xm=mx$ for all x in B.

Let A' be a K-algebra and $f\colon A\rightarrow A'$ a K-algebra epimorphism. We set $B'=f(B)$. We can regard A' as a left $A\underset{K}{\otimes} B^0$-module by setting

$$(a\otimes b^0)a'=f(a)a'f(b) \quad \text{for} \quad a\in A,\ b\in B \quad \text{and} \quad a'\in A';$$

then f may be regarded as a left $A\underset{K}{\otimes} B^0$-epimorphism.

Received August 6, 1970.

LEMMA 1. *If A is a projective $A\underset{K}{\otimes}B^0$-module, then $f(V_A(B))=V_{A'}(B')$.*[1)]

Proof. We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_{A\underset{K}{\otimes}B^0}(A, A) & \xrightarrow{f^*} & \mathrm{Hom}_{A\underset{K}{\otimes}B^0}(A, A') \\ \alpha \downarrow & & \downarrow \alpha' \\ V_A(B)=A^B & \xrightarrow[f]{} & A'^B=V_{A'}(B'), \end{array}$$

where α and α' are the above mentioned isomorphisms and $f^*=\mathrm{Hom}_{A\underset{K}{\otimes}B^0}(1,f)$. f^* is an epimorphism since A is $A\underset{K}{\otimes}B^0$-projective. Thus f is an epimorphism.

PROPOSITION 1. *Let A be a separable algebra over K. If A is pojective as a right B-module, then $f(V_A(B))=V_{A'}(B')$.*

Proof. Since A is projective as a right B-module, A is projective as a left B-module. Hence $A\underset{K}{\otimes}A^0$ is projective as a left $A\underset{K}{\otimes}B^0$-module ([2], chap. IX, § 2). A is projective as a left $A\underset{K}{\otimes}A^0$-module since A is separable over K. Thus A is projective as a left $A\underset{K}{\otimes}B^0$-module ([2], chap. II, § 6). We obtain the proposition by Lemma 1.

COROLLARY 1. *If A satisfies the hypothesis of Proposition 1, and if $V_A(B)$ is the center C of A, then $V_{A'}(B')$ is the center C' of A'.*

Proof. Since A is separable over K, $f(C)$ is the center C' of A' ([1], Prop. 1. 4). Thus $V_{A'}(B')=f(V_A(B))=f(C)=C'$.

REMARK 1. We can regard A also as a left $B\underset{K}{\otimes}A^0$-module. If we make the same argument as above for left $B\underset{K}{\otimes}A^0$-modules, we have the following result: Let A be a separable algebra over K. If A is projective as a left B-module, then $f(V_A(B))=V_{A'}(B')$.

COROLLARY 2. *Let A be a separable algebra over the center C of A. Let B be a separable algebra over C and $A\supset B\supset C$. Then $f(V_A(B))=V_{A'}(B')$.*

Proof. Since A is a projective B-module by Lemma 2 of [7], we obtain the corollary by Proposition 1.

§ 2. Let A be a ring and G a finite group of automorphisms of A. We denote by A^G the subring of all elements of A left invariant by all the automorphisms in G. We set $B=A^G$.

We call A/B a *G-Galois extension* if there exist elements $x_1, \cdots, x_n, y_1, \cdots, y_n$ of A such that $\sum_{i=1}^n x_i\sigma(y_i)=\delta_{1,\sigma}$ for all $\sigma\in G$.

Following Miyashita [8], we call A/B an *outer G-Galois extension* if A/B is a

1) We denote by $V_A(B)$ the commutor of B in A.

G-Galois extension and $V_A(B)=C$ (the center of A).

LEMMA 2. *Let A/B be a G-Galsis extension. If we give $\sigma(\neq 1)\in G$ and any maximal ideal $\mathfrak{P}$ of A, there exists an element a in A such that $\sigma(a)-a\notin\mathfrak{P}$.*

Proof. We can prove the lemma by the same way as the proof of Theorem 1.3, (f) in [3].

If A/B is an outer G-Galois extension, the center R of B is $B\cap C$ and $R=C^{G^*}$, where G^* is the group of automorphisms of C induced by G.

PROPOSITION 2. *Let A/B be an outer G-Galois extension. Let A be a separable algebra over C (central separable algebra). If C is a separable algebra over R, then $G\simeq G^*$ and C/R is a G^*-Galois extension.*

Proof. A is a separable algebra over R since A is separable over C and C is separable over R. Let H be the cyclic subgroup of G generated by $\sigma(\neq 1)$ in G and we set $L=A^H$. It is easily seen that A/L is an outer H-Galois extension. A is projective as a right L-module ([4], Th. 1).

Now we suppose that there exists a maximal ideal $\mathfrak{p}$ of C that contains the set $\{\sigma(c)-c; c\in C\}$. We set $\mathfrak{P}=A\mathfrak{p}$. Then $\mathfrak{P}$ is a maximal two-sided ideal of A and $\mathfrak{P}\cap C=\mathfrak{p}$ ([1], Cor. 3.2). We set $A'=A/\mathfrak{P}$ and $C'=C/\mathfrak{p}$. Let f be the natural epimorphism $A\to A'$ and we set $\bar{x}=f(x)$ for $x\in A$. Then A' is a finite dimentional simple algebra with the center C'. Moreover, $V_{A'}(f(L))=C'$ by Corollary 1. $\rho(\mathfrak{P})=\mathfrak{P}$ for any ρ in H since $\sigma(x)-x\in\mathfrak{p}$ for any x in $\mathfrak{p}$. Hence ρ induces an automorphism $\bar{\rho}$ of A' by setting $\bar{\rho}(\bar{x})=\overline{\rho(x)}$ for $x\in A$ and the map given by $\rho\to\bar{\rho}$ induces an epimorphism from H into the group H of automorphisms of A' generated by $\bar{\sigma}$. But this epimorphism is an isomorphism by Lemma 2.

We set $L'=A'^H$. Then $L'\supset C'$ and $V_{A'}(L')=C'$ since $L'\supset f(L)$. Since $L'\supset C'$, $\bar{\sigma}$ is an inner automorphism induced by a regular element in $V_{A'}(L')=C'$. Hence $H\simeq\bar{H}=\{1\}$. This is impossible since $\sigma\neq 1$. Thus, given $\sigma(\neq 1)\in G$ and any maximal ideal $\mathfrak{p}$ of C, there exists an element c is C such that $\sigma(c)-c\notin\mathfrak{p}$. The proposition follows easily from Theorem 1.3 of [3].

COROLLARY 3 ([9], Prop. 2.11.). *Let A/B be an outer G-Galois extension. If B is a separable algebra over R, then $G\simeq G^*$ and C/R is a G^*-Galois extension.*

Proof. Since A/B is a separable extension ([5], Prop. 3.3) and B/R is a separable extension, A is a separable algebra over R. Hence A is a central separable algebra and C is separable over R ([1], Th. 2.3). The corollary follows easily from Proposition 2.

REMARK 2. From the result of Proposition 2, under the same assumption as in the proposition it follows that A/B is a Galois extension in the sense of Kanzaki ([7], 3, (♯)). Hence B is separable over R and $A=BC\simeq B\otimes_R C$.[2] Conversely, if A/B is a Galois extension in the sense of Kanzaki, it follows easily that A/B is an

2) We denote BC the subring of A generated by B and C.

outer G-Galois extension and C is separable over R.

REMARK 3. If we use Th. 3.3 of [1], we can prove Corollary 3 in the following way, too. It follows easily that BC is separable over C and C is the center of BC. $V_A(BC)=C$, and so $A=V_A(C)=V_A(V_A(BC))=BC$ by Th. 3.3 of [1]. If we choose any maximal ideal $\mathfrak{p}$ of C and $\sigma(\neq 1)\in G$ and we set $\mathfrak{P}=A\mathfrak{p}$, there exists an element a in A such that $\sigma(a)-a\notin\mathfrak{P}$. We can write a as

$$a=b_1c_1+\cdots+b_rc_r,$$

where $c_i\in C$, $b_i\in B$, $1\leqq i\leqq r$. Then

$$\sigma(a)-a=b_1(\sigma(c_1)-c_1)+\cdots+b_r(\sigma(c_r)-c_r).$$

If $\sigma(c_i)-c_i\in\mathfrak{p}$ for every c_i, then $\sigma(a)-a\in\mathfrak{P}$. Thus there exists an element c_i in C such that $\sigma(c_i)-c_i\notin\mathfrak{p}$.

REMARK 4. Here, we shall use the same notation as in Theorem 5 of [7]. When C is not necessarily an integral domain, in Th. 5 of [7] we must replace 4) with the following: if Ω is an intermediate ring between Λ and Γ such that Ω is separable over S and S is a separable G-strong R-subalgebra of C (see [3]), where $S=C\cap\Omega$, then Λ/Ω is a Galois extension with respect to H where $H=\{\sigma\in G;\ \sigma(x)=x$ for all $x\in\Omega\}$. The above fact is proved by the same way as the proof of Th. 5, 4) of [7]. The above assumption is equivalent to that of 4), when C is an integral domain.

COROLLARY 4. *Let A be a separable algebra over C. If A/B is an outer G-Galois extension, then $G\simeq G^*$.*

Proof. Let H be the kernel of the natural epimorphism

$$G\to G^*.$$

We set $L=A^H$. Then A/L is an outer H-Galois extension and the center of L is C. Hence $H\simeq H^*=\{1\}$ by Proposition 2. Thus $G\simeq G^*$.

Let $\sum_{\sigma\in G}\oplus Au_\sigma$ be the *trivial crossed product* of A with G. Following Miyashita [8], G is said *completely outer* if Au_σ and Au_ρ $(\sigma\neq\rho)$ are unrelated as two-sides A-modules.[3)]

If G is completely outer, A/B is an outer G-Galois extension ([8], Prop. 6.4).

Let A' be a ring and f a ring epimorphism from A into A'. Let G' be a finite group of automorphisms of A' such that $G\overset{g}{\simeq}G'$ and $f(\sigma(x))=\sigma'f(x)$, where $x\in A$, $\sigma\in G$ and $\sigma'=g(\sigma)$. Then we can regard $A'u_{\sigma'}A'$ as a two-sided A-module by setting

$$au_{\sigma'}b=f(a)u_{\sigma'}f(b),\qquad a, b\in A.$$

3) See [8], § 6.

If we define the map

$$g_\sigma:\quad M_\sigma = Au_\sigma \to M_{\sigma'} = A'u_{\sigma'}$$

by

$$au_\sigma \mapsto f(a)u_{\sigma'},$$

then g_σ is a two-sided A-module epimorphism.

LEMMA 3. *If G is completely outer, then G' is completely outer.*

Proof. If $M_{\sigma'}$ and $M_{\rho'}$ are related, $M_1'/N_1' \simeq M_2'/N_2'$, where M_1'/N_1' and M_2'/N_2' are nonzero subquotients of $M_{\sigma'}$ and $M_{\rho'}$, respectively. We set $M_1 = g_\sigma^{-1}(M_1')$, $N_1 = g_\sigma^{-1}(N_1')$, $M_2 = g_\rho^{-1}(M_2')$ and $N_2 = g_\rho^{-1}(N_2')$. Then $M_1/N_2 \simeq M_1'/N_1' \simeq M_2'/N_2' \simeq M_2/N_2$, and so M_σ and M_ρ are related.

PROPOSITION 3. *Let A be a separable algebra over the center C. If G is completely outer, then $G \simeq G^*$ and C/R is a G^*-Galois extension.*

Proof. We shall use the same notation as in the proof of Proposition 2. It follows that the cyclic group H is completely outer. Hence the H is completely outer by Lemma 3, and so $V_{A'}(A'^H) = C'$. Thus we can prove the proposition by the same way as the proof of Proposition 2.

§ 3. Let K be a commutative ring. Let A be an algebra over K.

THEOREM ([4], § 2, Th. 11). *If A/K is a G-Galois extension and G is a cyclic group, then A is a commutative ring.*

This theorem was proved by Harrison in case K is a field and the general case was proved by Demeyer. The author proved this theorem when A is a simple algebra [6]. Here, we shall give a shorter proof of the theorem.

At first, we shall assume that K is an integral domain. Let Q be the quotient field of K. Then $A \otimes_K Q/Q$ is a G-Galois extension and since G is a cyclic group and Q is a field, $A \otimes_K Q$ is commutative by the result of Harrison. On the other hand, A is a projective K-module since A/K is a G-Galois extension. Hence we have the exact sequence

$$0 \to A \otimes_K K \to A \otimes_K Q.$$

Thus A is a commutative ring.

Let C be the center of A. If we prove that $G \simeq G^*$ and C/K is a G^*-Galois extension in the general case, the theorem is valid by Remark 2. Let $\sigma (\neq 1) \in G$ and we suppose that $\mathfrak{m}$ is a maximal ideal of C that contains the set $\{\sigma(c) - c;\, c \in C\}$. We set $\mathfrak{M} = A\mathfrak{m}$. σ induces the automorphism $\bar{\sigma}$ of $A' = A/\mathfrak{M}$ as in the proof of Proposition 2.

We set $\mathfrak{p}=\mathfrak{M}\cap K=\mathfrak{m}\cap K$. Then $\mathfrak{p}$ is a prime ideal of K. Since $A\underset{K}{\otimes}K/\mathfrak{p}/K/\mathfrak{p}$ is a G-Galois extension and $K/\mathfrak{p}$ is an integnal domain, $A\underset{K}{\otimes}K/\mathfrak{p}$ is a commutative ring. Hence $A\underset{K}{\otimes}K/\mathfrak{p}=i(C\underset{K}{\otimes}K/\mathfrak{p})$ ([1], Cor. 1. 6), where $i(C\underset{K}{\otimes}K/\mathfrak{p})$ is the natural image of $C\underset{K}{\otimes}K/\mathfrak{p}$ into $A\underset{K}{\otimes}K/\mathfrak{p}$. Hence $A\underset{K}{\otimes}K/\mathfrak{p}\simeq A/A\mathfrak{p}=C+A\mathfrak{p}/A\mathfrak{p}$, so $A=C+A\mathfrak{p}$ $\supset\mathfrak{M}\supset A\mathfrak{p}$. Thus $A=C+\mathfrak{M}$. If $c\in C+\mathfrak{M}=A$, $\sigma(c)-c\in\mathfrak{M}$, and so $\bar{\sigma}=1$. But $\bar{\sigma}\neq 1$ by Lemma 2. From this contradiction, given $\sigma(\neq 1)\in G$ and any maximal ideal $\mathfrak{m}$ of C, there exists an element c in C such that $\sigma(c)-c\notin\mathfrak{m}$. Thus $G\simeq G^*$ and A/K is a G^*-Galois extensions.

References

[1] Auslander, M., and O. Goldman, The Brauer group of a commutative ring. Trans. Amer. Math. Soc. **97** (1960), 367–409.

[2] Cartan, H., and S. Eilenberg, Homological algebra. Princeton (1956).

[3] Chase, S. U., D. K. Harrison, and A. Rosenberg, Galois theory and Galois cohomology of commutative rings. Mem. Amer. Math. Soc. **52** (1965), 15–33.

[4] DeMeyer, F. R., Some notes on the general Galois theory of rings. Osaka Math. J. **2** (1965), 117–127.

[5] Hirata, K., and K. Sugano, On semi-simple extensions and separable extensions over non-commutative rings. J. Math. Soc. Japan **18** (1966), 360–373.

[6] Inatomi, A., Remark on Galois theory of simple ring. Kōdai Math. Sem. Rep. **14** (1962), 160–161.

[7] Kanzaki, T., On commutator rings and Galois theory of separable algebra. Osaka J. Math. **1** (1964), 103–115.

[8] Miyashita, Y., Finite outer Galois theory of non-commutative rings. J. Fac. Sci. Hokkaido Univ., Ser. I, **19** (1966), 114–134.

[9] Miyashita, Y., Locally finite outer Galois theory. J. Fac. Sci. Hokkaido Univ., Ser. I, **20** (1967), 1–26.

Meiji University.