Kanzaki, T.
Osaka J. Math.
2 (1965), 309–317

ON GALOIS ALGEBRA OVER A COMMUTATIVE RING

TERUO KANZAKI

(Received April 12, 1965)

In [1], M. Auslander and O. Goldman introduced the notion of a Galois extension of a commutative ring. Galois theory for separable extension of a commutative ring has been developed by S. U. Chase, D. K. Harrison and A. Rosenberg in [3]. The author, in [6] and [7], generalized the notion of a Galois extension of a commutative ring to the case of non commutative ring, and developed the Galois theory for separable algebra over a commutative ring. We call here an algebra Λ over a commutative ring R a *Galois algebra* if Λ is a Galois extension of R. The study of Galois algebra over a commutative ring has been done by F. R. DeMeyer in [4] and [5], and Y. Takeuchi in [11]. In this note we investigate the structure of such Galois algebra over a commutative ring.

In §2 we prove that if Λ is a Galois algebra over a commutative ring R with group G and if C is the center of Λ then Λ is a direct sum of C-submodule J_σ of Λ with $\sigma \in G$ where $J_\sigma = \{a \in \Lambda \mid \sigma(x)a = ax$ for every x in $\Lambda\}$. Using this fact, we give shorter proofs of the results of F. DeMeyer in [4] and [5] and Y. Takeuchi in [11]. In §3 we prove that if Λ is a Galois algebra over R with group G then, for each σ in G, $c_\sigma = J_\sigma J_{\sigma^{-1}}$ is an idempotent ideal of the center of Λ which is generated by an idempotent element. As corollary to this theorem, we reduce the following Harrison-DeMeyer's theorems. If Λ is a Galois algebra over R with group G and if the center C of Λ is indecomposable then Λ is a Galois algebra over C and C is a Galois algebra over R. If Λ is a Galois algebra over R with cyclic group G, then Λ is commutative.

The author wishes to gives hearty thanks to Professor H. Nagao and Prefessor M. Harad for helpful discussion and their advice.

Throughout this note we assume that every ring has an identity element.

1. Definitions and Preliminary results.

Let Λ be a ring, G a finite group of ring automorphisms of Λ, and let $\Delta = \Delta(\Lambda, G) = \sum_{\sigma \in G} \oplus \Lambda U_\sigma$ be the crossed product of Λ and G with trivial factor set, i.e. $\{U_\sigma\}$ is a Λ-free basis of Δ and $U_\sigma U_\tau = U_{\sigma\tau}$, $U_\sigma\lambda = \sigma(\lambda)U_\sigma$ for $\lambda \in \Lambda$. We let Λ^G denote the totality of elements of Λ which are left invariant by G. For λ in Λ, we let λ_r (or λ_l) denote the right (or left) multiplication by λ on Λ and Γ_r (or Γ_l) denote the totality of λ_r (or λ_l) with $\lambda \in \Gamma$. In [6] we generalized the notion of Galois extension defined first by M. Auslander and O. Goldman [1] to the non commutative case. Our definition of Galois extension is as follows. A ring Λ is called a Galois extension of a ring Γ relative to G, if the following conditions are satisfied;

I. $\Gamma = \Lambda^G$,

II. Δ is finitely generated projective Γ_r-module.

III. $\delta : \Delta(\Lambda, G) \to \mathrm{Hom}_{\Gamma_r}(\Lambda, \Lambda)$ is and isomorphism where δ is defined by $\delta(\lambda U_\sigma) = \lambda_r \sigma$ for $\lambda \in \Lambda$.

If Λ is an algebra over a commutative ring R, and if Λ is a Galois extension of R relative to G, then we call Λ a *Galois algebra* over R with group G. If Λ is a Galois algebra over R with Group G, and if R is the center of Λ, then we call Λ *central Galois algebra* over R with group G. In [3], Chase, Harrison and Rosenberg gave another definition of Galois extension for the case of commutative ring which is equivalent to the definition by Auslander and Goldman [1]. We consider the following Deffinition the case of non commutative ring; Λ is called a Galois extension of Γ with group G, if the following conditions are satisfied;

I′. $\Gamma = \mathrm{Tr}(\Lambda)$, where $\mathrm{Tr}(x) = \sum_{\sigma \in G} \sigma(x)$ for $x \in \Lambda$,

II′. there exist $x_1, x_2, \cdots, x_s$ and $y_1, y_2, \cdots, y_s$ in Λ such that for $\sigma \in G$

$$\sum_{i=1}^{s} x_i \sigma(y_i) = \begin{cases} 1, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$$

In [7], we have seen that if Λ is an algebra over R then "Galois extension Λ of R" in our sense and that in their sense are equivalent.

Now, let Λ be an arbitrary ring, and C the center of Λ. We generalize the argument for J_σ in [10], § 3. For any ring automorphism σ of Λ, let $J_\sigma = \{a \in \Lambda \mid \sigma(x)a = ax$ for every $x \in \Lambda\}$. Then J_σ is a C-submodule of Λ and we may show easily the following properties. If σ and τ are ring automorphisms of Λ, then

1) $J_\sigma J_\tau \subset J_{\sigma\tau}$,

2) $\tau(J_\sigma) = J_{\tau\sigma\tau^{-1}}$,

3) $J_\sigma \Lambda = \Lambda J_\sigma$ is a two sided ideal of Λ,

4) for the identity mapping 1 of Λ, $J_1 = C$.

For a central separable algebra Λ over C, using the result in Rosenberg and Zelinsky [10], we have

Lemma 1. *Let Λ be a central separable algebra over C and σ a ring automorphism of Λ which leaves C element wise fixed. Then we have*

1) $J_\sigma\Lambda=\Lambda J_\sigma=\Lambda$,
2) $J_\sigma J_{\sigma^{-1}}=J_{\sigma^{-1}}J_\sigma=C$,
3) *σ is an inner automorphism of Λ if and only if there is an element x in J_σ such that $xC=J_\sigma$ (cf. Lemma in 5 in [10]),*
4) *if C is a semi-local ring then σ is an inner automorphism of Λ.*

Proof. 1). By Theorem 3. 1 in [1], the homomorphism $g: \Lambda\underset{C}{\otimes}J_\sigma\to\Lambda$, defined by $g(\lambda\otimes a)=\lambda a$ for $\lambda\in\Lambda$ and $a\in J_\sigma$, is an isomorphism as C-module. Therefore, we have $\Lambda J_\sigma=\Lambda$. 2). $\mathfrak{c}_\sigma=J_\sigma J_{\sigma^{-1}}$ is an ideal of C, and $\mathfrak{c}_\sigma\Lambda=J_\sigma J_{\sigma^{-1}}\Lambda=J_\sigma\Lambda=\Lambda$. Since Λ is central separable, $\mathfrak{c}_\sigma=\mathfrak{c}_\sigma\Lambda\cap C=C$. 3) is calear by 1). 4). We suppose that C is semi-local. Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ be the maximal ideals of C. We first show that there is an element x in J_σ such that $x\notin\mathfrak{p}_iJ_\sigma$ for every maximal ideal $\mathfrak{p}_i$ of C. Since $J_\sigma J_{\sigma^{-1}}=C$, we have $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_rJ_\sigma\not\subset\mathfrak{p}_iJ_\sigma$ for $i=1, 2, \cdots, r$. For each i, there is an element x_i in J_σ such that

$$x_i\in\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_rJ_\sigma \text{ and } x_i\notin\mathfrak{p}_iJ_\sigma\,.$$

Put $x=\sum_{i=1}^{r}x_i$. Then x is contained in J_σ, but is not contained in $\mathfrak{p}_iJ_\sigma$ for every $\mathfrak{p}_i$. Now, we shall show $xC=J_\sigma$. Since, by Proposition 4 in [10], J_σ is a finitely generated projective and rank one C-module, we have $[J_\sigma\underset{C}{\otimes}C/\mathfrak{p}_i : C/\mathfrak{p}_i]=1$ for every $\mathfrak{p}_i$. Since $xC\not\subset\mathfrak{p}_iJ_\sigma$, $J_\sigma=xC+\mathfrak{p}_iJ_\sigma$ for $i=1, 2, \cdots, r$. By Nakayama's Lemma, we have $J_\sigma=xC$. By 3), this completes the proof.

2. Structure theorem.

Proposition 1. *If Λ is a Galois extension of Γ relative to G, then*

$$V_\Lambda(\Gamma)=\sum_{\sigma\in G}\oplus J_\sigma$$

where $V_\Lambda(\Gamma)$ is the commutor ring of Γ in Λ.

Proof. From our definition of Galois extension, we may identify $\Delta=\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda U_\sigma$ and $\mathrm{Hom}_{\Gamma_r}(\Lambda, \Lambda)$ by the isomorphism δ. Then we may denote $\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda_l\sigma$. It follows that $V_\Delta(\Lambda)=V_{\mathrm{Hom}_{\Gamma_r}(\Lambda,\Lambda)}(\Lambda_l)=\mathrm{Hom}_{\Lambda_l\Gamma_r}(\Lambda, \Lambda)=(V_\Lambda(\Gamma))_r$. On the other hand, an easy computation shows $V_\Delta(\Lambda)=\sum_{\sigma\in G}\oplus J_{\sigma^{-1}}U_\sigma=(\sum_{\sigma\in G}\oplus J_{\sigma^{-1}})_r$. Therefore, we have $V_\Lambda(\Gamma)=\sum_{\sigma\in G}\oplus J_\sigma$. From this proposition we have immediately

Theorem 1. *Let Λ be a Galois algebra over a commutative ring R with group G. Then we have $\Lambda=\sum_{\sigma\in G}\oplus J_\sigma$.*

Proposition 2. *Let Λ be a Galois algebra over R with group G, G the center of Λ, and let $\mathfrak{c}_\sigma=J_\sigma\Lambda\cap C$ for each σ in G. Then $\mathfrak{c}_\sigma$ is an ideal of C and $\mathfrak{c}_\sigma\Lambda=J_\sigma\Lambda$. For σ, τ in G, we have the following properties;*

1) $\mathfrak{c}_\sigma=0$ *if and only if* $J_\sigma=0$,
2) $J_\sigma J_\tau=\mathfrak{c}_\sigma J_{\sigma\tau}=\mathfrak{c}_\tau J_{\sigma\tau}$,
3) $J_\sigma J_{\sigma^{-1}}=J_{\sigma^{-1}}J_\sigma=\mathfrak{c}_\sigma$, *therefore* $\mathfrak{c}_\sigma=\mathfrak{c}_{\sigma^{-1}}$,
4) $\mathfrak{c}_\sigma J_\sigma=J_\sigma$,
5) $\mathfrak{c}_\sigma^2=\mathfrak{c}_\sigma$,
6) $\mathfrak{c}_\sigma=C$ *if and only if σ leaves each element of the center C invariant, i.e.* $\sigma|C=1$,
7) *if* $\sigma|C=1$ *or* $\tau|C=1$ *then* $J_\sigma J_\tau=J_{\sigma\tau}$.

Proof. Let Λ be a Galois algebra over R with group G. Then Λ is separable over R (cf. Proposition 4 in [6]), therefore Λ is central separable over C and C is separable over R. From the central separability of Λ, we obtain $\mathfrak{c}_\sigma\Lambda=J_\sigma\Lambda$ for $\mathfrak{c}_\sigma=C\cap J_\sigma\Lambda$. Since $\Lambda=\sum_{\sigma\in G}\oplus J_\sigma$, we have $\mathfrak{c}_\sigma\Lambda=\sum_{\tau\in G}\oplus\mathfrak{c}_\sigma J_\tau$ and $J_\sigma\Lambda=\sum_{\tau\in G}J_\sigma J_\tau$. Since $J_\sigma J_\tau\subset J_{\sigma\tau}$ and $\mathfrak{c}_\sigma\Lambda=J_\sigma\Lambda$, we have $J_\sigma\Lambda=\sum_{\tau\in G}\oplus J_\sigma J_\tau$ and $\mathfrak{c}_\sigma J_{\sigma\tau}=J_\sigma J_\tau$. Similarly, $\mathfrak{c}_\tau J_{\sigma\tau}=J_\sigma J_\tau$. In paticular, taking $\tau=\sigma^{-1}$ or $\tau=1$, we have $J_\sigma J_{\sigma^{-1}}=\mathfrak{c}_\sigma=\mathfrak{c}_{\sigma^{-1}}$ or $\mathfrak{c}_\sigma J_\sigma=J_\sigma$, and $\mathfrak{c}_\sigma^2=\mathfrak{c}_\sigma J_\sigma J_{\sigma^{-1}}=J_\sigma J_{\sigma^{-1}}=\mathfrak{c}_\sigma$. If σ is an automorphism of the central separable algebra Λ over C which leaves C element wise fixed, then by Lemma 1 we have $\Lambda J_\sigma=\Lambda$, therefore $\mathfrak{c}_\sigma=C\cap\Lambda J_\sigma=C$. Conversely, if $\mathfrak{c}_\sigma=C$, then by definition of J_σ we have $(\sigma(x)-x)a=0$ for every x in C and a in J_σ. Since $\mathfrak{c}_\sigma=J_\sigma J_{\sigma^{-1}}$, $(\sigma(x)-x)C=(\sigma(x)-x)\mathfrak{c}_\sigma=0$ for every x in C. Therefore $\sigma(x)=x$ for every x C. If $\sigma|C=1$ then by 6) and 2) $J_\sigma J_\tau=\mathfrak{c}_\sigma J_{\sigma\tau}=J_{\sigma\tau}$.

From Theorem 1 and Proposition 2, we obtain easily the following

Corollary 1. *If Λ is a central Galois algebra over C with group G, then $\Lambda=\sum_{\tau\in G}\oplus J_\sigma$, $J_\sigma J_\tau=J_{\sigma\tau}$ and $\mathfrak{c}_\sigma=J_\sigma J_{\sigma^{-1}}=C$ for every σ in G.*

Corollary 2. (De Meyer and Takeuchi) *If Λ is a central Galois algebra over C with group G, and if every element σ of G is an inner automorphism of Λ associated with a unit u_σ in Λ, then $J_\sigma=Cu_\sigma$ and $\Lambda=\sum_{\sigma\in G}\oplus Cu_\sigma$.*

Proposition 3. *Let Λ be a Galois algebra over R with group G, C the center of Λ, and $H=\{\sigma\in G\,|\,\sigma(x)=x$ for every x in $C\}$. Then Λ is a central Galois algebra over C with group H if and only if $J_\tau=0$ for every τ in G such that $\tau\notin H$, and then C is a Galois algebra over R with group G/H.*

Proof. Let Λ be Galois algebra over R with G. Then $\Lambda=\sum_{\sigma\in G}\oplus J_\sigma$. If Λ is acentral Galois algebra over C with group H, then $\Lambda^H=C$ and C is a Galois extension of R with group G/H (cf. proof of Theorem 3.1 in [3], or Theorem 1 in [11]). If Λ is a central Galois algebra over C with group H, then, by Theorem 1, $\Lambda=\sum_{\sigma\in H}\oplus J_\sigma$, therefore $J_\tau=0$ for $\tau\notin H$. Conversely, if $J_\tau=0$ for every $\tau\notin H$, then $\Lambda=\sum_{\sigma\in H}\oplus J_\sigma$. Since by Theorem 3 in [6] Λ is a Galois extension of Λ^H relative to H, by Proposition 1 we have $V_\Lambda(\Lambda^H)=\sum_{\sigma\in H}\oplus J_\sigma$. therefore $\Lambda=V_\Lambda(\Lambda^H)$, and $\Lambda^H\subset C$. Since $C\subset\Lambda^H$, we have $\Lambda^H=C$, thus Λ is a central Galois algebra over. C. This completes the proof.

Proposition 4. *Let Λ be a Galois algebra over R with group G, and let $N(\sigma)=\{\tau\in G\mid\tau\sigma=\sigma\tau\}$ for each $\sigma\in G$, then we have the following statements;*

1) *for $J_\sigma\neq 0$ and J_τ, $J_\sigma=J_\tau$ if and only if $\sigma=\tau$,*
2) *each element of $N(\sigma)$ induces an automorpxism of C-module J_σ, and if $J_\sigma\neq 0$ then τ is contained in $N(\sigma)$ if and only if $\tau(J_\sigma)=J_\sigma$,*
3) *for $\sigma\neq 1$ in G and x in J_σ, if $\tau(x)=x$ for every τ in $N(\sigma)$, then $x=0$.*
4) *for $\sigma\neq 1$ and for every x in J_σ, $\sum_{\tau\in N(\sigma)}\tau(x)=0$,*
5) *for $\sigma\neq 1$ in G and for every x in J_σ, $\mathrm{Tr}(x)=0$.*

Proof. 1) and 2) are clear. To prove 3), let $\tau_1, \tau_2, \cdots, \tau_r$ be the right coset representatives of G modulo $N(\sigma)$. If x in J_σ satisfies $\tau(x)=x$ for every τ in $N(\sigma)$, then we put $y=\sum_{i=1}^{r}\tau_i(x)$. Since $\nu(y)=\sum_i\nu\tau_i(x)=\sum_i\tau_i(x)=y$ for every ν in G, y is contained in $\Lambda^G=R$, and therefore $y\in J_1=C$. On the other hand, $\tau_i(x)\in\tau_i(J_\sigma)=J_{\tau_i\sigma\tau_i^{-1}}\neq J_1$, and by 2) $\tau_i(J_\sigma)\neq\tau_j(J_\sigma)$ if $i\neq j$. Since Λ is a direct sum of J_σ for $\sigma\in G$, we have $\tau_i(x)=0$ $i=1, 2, \cdots, r$, and therefore $x=0$. 4) is easily proved by 3). Now, for every element x in J_σ, $\mathrm{Tr}(x)=\sum_{\sigma\in G}\sigma(x)=\sum_{i=1}^{r}\tau_i(\sum_{\nu\in N(\sigma)}\nu(x))=0$, therefore we have 5).

Using this proposition we have

Proposition 5. *Let Λ be a Galois algebra over R with group G, C the center of Λ, and let $H=\{\sigma\in G\mid\sigma|C=1\}$. Then the order $|H|$ of H is a unit in R.*

Proof. By 5) in Proposition 4, $\mathrm{Tr}(J_\sigma)=0$ for $\sigma\neq 1$ in G. Therefore $\mathrm{Tr}(\Lambda)=\mathrm{Tr}(\sum_{\sigma\in G}J_\sigma)=\sum_{\sigma\in G}\mathrm{Tr}(J_\sigma)=\mathrm{Tr}(J_1)=\mathrm{Tr}(C)$, and $R=\mathrm{Tr}(C)$. Then there is an element a in C such that $\mathrm{Tr}(a)=1$. Let $G=\sigma_1 H+\cdots+\sigma_r H$ be the right decomposition of G modulo H. We have $\mathrm{Tr}(a)=\sum_{\sigma\in G}\sigma(a)=|H|(\sum_{i=1}^{r}\sigma_i(a))=1$. However, $\sum_{i=1}^{r}\sigma_i(a)$ is contained in $\Lambda^G=R$. Therefore $|H|$ is a unit in R.

Corollary 3. (De Meyer and Takeuchi) *Let Λ be a central Galois algebra over C with group G. Then the order $|G|$ of G is a unit in C.*

Corollary 4. *Let Λ be a central Galois algebra over C with group R. Then Λ is a strongly separable algebra over C in the sense of* [9].

Proof. By Theorem 1 in [9], Λ is a strongly separable algebra over C if and only if $\Lambda/\mathfrak{p}\Lambda$ is a strongly separable algebra over $C/\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of C[1]. For a maximal ideal $\mathfrak{p}$ of C, $\Lambda/\mathfrak{p}\Lambda$ is a central simple algebra with minimum condition over $C/\mathfrak{p}$, and $[\Lambda/\mathfrak{p}\Lambda : C/\mathfrak{p}]=[\Lambda\otimes_C C_{\mathfrak{p}} : C_{\mathfrak{p}}]=|G|$. Therefore the degree of the central simple algebra $\Lambda/\mathfrak{p}\Lambda$ is a unit in $C/\mathfrak{p}$. Thus the degree of $\Lambda/\mathfrak{p}\Lambda$ is prime to the characteristic of $C/\mathfrak{p}$. By definition of strongly separbility in [8], $\Lambda/\mathfrak{p}\Lambda$ is a strongly separable algebra over $C/\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of C, which completes the proof.

3. Main theorem.

Proposition 6. *Let Λ be a Galois algebra over R with group G, C the center of Λ, and $\mathfrak{c}_\sigma$ the ideal defined in Proposition 2 for each $\sigma\in G$. Then we have the following statements;*

1) $\mathfrak{c}_\sigma\mathfrak{c}_\tau=\mathfrak{c}_\sigma\mathfrak{c}_{\sigma\tau}=\mathfrak{c}_\tau\mathfrak{c}_{\sigma\tau}$,
2) $\mathfrak{c}_\sigma\subset\mathfrak{c}_{\sigma^i}$ *for any integer i, therefore* $\mathfrak{c}_\sigma\neq 0$ *implies* $\mathfrak{c}_{\sigma^i}\neq 0$,
3) *for* $\tau\in G$, $\tau(\mathfrak{c}_\sigma)=\mathfrak{c}_{\tau\sigma\tau^{-1}}$,
4) *for* $H=\{\sigma\in G\,|\,\sigma|C=1\}$, *if* $\sigma\equiv\tau \pmod H$ *then* $\mathfrak{c}_\sigma=\mathfrak{c}_\tau$.

Proof. 1) and 3) are clear by Proposition 2, and 2) and 4) are easily proved by 1).

Lemma 2. *Let C be a commutative algebra over R, and $\mathfrak{c}$ an ideal of C such that $\mathfrak{c}$ is idempotent and finitely generated over R. Then $\mathfrak{c}$ is generated by an idempotent element iu C.*[2]

Proof. Let $\mathfrak{c}=\sum_{i=1}^{r}Rx_i$. Since $\mathfrak{c}$ idempotent, $\mathfrak{c}^2=\mathfrak{c}=\sum_{i=1}^{r}\mathfrak{c}x_i$. Then, we

1) Let A be a central separable algebra over C. Then A is strongly separable over C if and only if $A/\mathfrak{p}A$ is strongly separable over $C/\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of C. (Cf. proof of Theorem 1 in [9].)

2) This lemma suggested to me by M. Harada. I express here my thanks to him.

have $x_i=\sum_j a_{ij}x_j$ with some a_{ij} in $\mathfrak{c}$. Let be the deteriminant of the matrix $E-(a_{ij})$, where E is the unit matrix. Then, we can easily see that $d=1-e$ with some e in $\mathfrak{c}$ and $xd=0$ for every x in $\mathfrak{c}$. Therefore, we have $e^2=e$ and $ex=x$ for every $\mathfrak{c}$, thus $\mathfrak{c}=eC$.

From this lemma, we have the following main theorem;

Theorem 2. *Let Λ be a Galois algebra over R with group G, C, the center of Λ. Then $\mathfrak{c}_\sigma=J_\sigma J_{\sigma^{-1}}$ is generated by an idempotent element e_σ in C for each σ in G.*

As a corollary of Theorem 2, we have

Theorem 3. (Harrison, De Meyer) *Let Λ be a Galois algebra over R with group G, and let C be the center of Λ. If C is indecomposable, then Λ is a central Galois algebra over C with group H, and C is a Galois algebra over R with group G/H, where $H=\{\sigma\in G \mid \sigma \mid C=1\}$.*

Proof. Since the idempotent elements in C are only 0 and 1, for each $\sigma\in G$, by Theorem 2, $\mathfrak{c}_\sigma$ is either 0 or C. Therefore, if $\tau\notin H$ then $J_\tau=0$. By Proposition 3, the proof is completed.

Proposition 7. *Let Λ be a Galois algebra over R with group G, and let $\mathfrak{a}_\sigma=\{x\in C \mid x\mathfrak{c}_\sigma=0\}$. Then we have the following statements;*

1) $\mathfrak{a}_\sigma=\mathfrak{a}_{\sigma^{-1}}\supset\mathfrak{a}_{\sigma^i}$ *for any integer i,*
2) $\mathfrak{a}_\sigma\Lambda=\{x\in\Lambda \mid xJ_\sigma=0\}$,
3) $\mathfrak{a}_\sigma\Lambda\cap J_\tau=\mathfrak{a}_\sigma J_\tau$,
4) *for $x\in J_\sigma$, $x=0$ if and only if $xJ_\sigma=0$ (or $x\mathfrak{c}_\sigma=0$).*
5) *if $x\in J_\sigma$ and $xJ_{\sigma^i}=0$ for some integer i, then $x=0$.*

Proof. 1) and 2) are clear by 4) in Proposition 6. Since $\Lambda=\sum_{\sigma\in G}\oplus J_\sigma$, we have $\mathfrak{a}_\sigma\Lambda=\sum_{\tau\in G}\oplus\mathfrak{a}_\sigma J_\tau$, therefore $\mathfrak{a}_\sigma\Lambda\cap J_\tau=\mathfrak{a}_\sigma J_\tau$. In particular, taking $\sigma=\tau$, we have $\mathfrak{a}_\sigma\Lambda\cap J_\sigma=\mathfrak{a}_\sigma J_\sigma=\mathfrak{a}_\sigma\mathfrak{c}_\sigma J_\sigma=0$, which proves 4). 5) is clear by 1).

For a Galois algera with abelian group, we have the following proposition with a weaker assumption than Theorem 3.

Proposition 8. *Let Λ be a Galois algebra over R with abelian group G. Then Λ is a strongly separable algebra over R. If R is indecomposable, then Λ is a central Galois algebra over the center C and the center C is a Galois algebra over R.*

Proof. We prove first the second part. Since G is abelian, for every τ in G, $\tau(\mathfrak{c}_\sigma)=\mathfrak{c}_{\tau\sigma\tau^{-1}}=\mathfrak{c}_\sigma$. If $\mathfrak{c}_\sigma\neq 0$, then there is a non zero idempotent element e_σ in C such that $\mathfrak{c}_\sigma=e_\sigma C$, and for every τ in G, $\tau(e_\sigma)=e_\sigma$, Therefore, e_σ is contained in $\Lambda^G=R$. It must be $e_\sigma=1$. Thereforec $\mathfrak{c}_\sigma=C$. By Proposition 3, this completes the proof of the second part. By Theorem 1 in [9] and the second part of this proposition, we can prove the first part; for every maximal ideal $\mathfrak{p}$ of R, $\Lambda\underset{R}{\otimes}R_{\mathfrak{p}}$, is strongly separable over $R_{\mathfrak{p}}$, therefore Λ is strongly seprarable over R[3)].

Proposition 9. *Let Λ be a Galois algebra over R with group G. If Λ is a strongly separable algebra over R, then we have the following statements;*

1) *for each $\sigma\in G$, $\sigma|J_\sigma=1$, i.e. $\sigma(x)=x$ for all x in J_σ,*
2) *for each integer i, if $a\in J_\sigma$ and $b\in J_{\sigma^i}$ then $ab=ba$.*

Proof. If Λ is a strongly separable algebra over R, then by Proposition 1 in [9], $\Lambda=C\oplus[\Lambda, \Lambda]$ where C is the center of Λ and $[\Lambda, \Lambda]$ is a C-submodule of Λ generated by $xy-yx$ for every x, y in Λ. For any x, y in J_σ and z in $J_{\sigma^{-1}}$, it follows that $\sigma(x)yz=yxz=xzy$. Since zy and yz are in $J_\sigma J_{\sigma^{-1}}=J_{\sigma^{-1}}J_\sigma=\mathfrak{c}_\sigma\subset C$, we have $zy-yz\in[\Lambda, \Lambda]\cap C=0$, and therefore $zy=yz$. Thus $\sigma(x)yz=xyz$, and $(\sigma(x)-x)yz=0$. Therefore, $(\sigma(x)-x)J_\sigma J_{\sigma^{-1}}=(\sigma(x)-x)\mathfrak{c}_\sigma=0$, and hence $\sigma(x)=x$. Thus we have 1). By 1), we obtain the statement 2); for every $a\in J_\sigma$ and $b\in J_{\sigma^i}$, $ab=\sigma^i(a)b=ba$.

We now obtain the following Harrison- De Meyers, Theorem.

Theorem 4. (Harrison-De Meyer) *Let Λ be a Galois algebra over R with cyclic group G. Then Λ is commutative.*

Proof. Since G is abelian, by Proposition 8, Λ is strongly separable over R. Now, suppose Λ is non commutative. Let $G=(\sigma)$. Since $\Lambda=\sum_i\oplus J_{\sigma^i}$, there is $J_{\sigma^i}\neq 0$. Let $k=\min(i>0|J_{\sigma^i}\neq 0)$. If $k\not| i$ then, by 1) in Proposition 6, $\mathfrak{c}_{\sigma^k}\mathfrak{c}_{\sigma^i}=\mathfrak{c}_{\sigma^k}\mathfrak{c}_{\sigma^{i-nk}}=0$ where n is an integer such that $0<i-nk<k$. Therefore, if $k\not| i$ then $J_{\sigma^i}J_{\sigma^k}=J_{\sigma^k}J_{\sigma^i}=0$. If $k|i$, i.e. $i=kr$, then by 2) in Proposition 9, $ab=ba$ for every $a\in J_{\sigma^k}$ and $b\in J_{\sigma^{kr}}=J_{\sigma^i}$. Thus $J_{\sigma^k}\neq 0$ is contained in the center $C=J_1$, this is a contradiction. Therefore Λ is commutative.

Now, let Λ be a Galois algebra over R with group G, and C the center of Λ. Then for each $\sigma\in G$, there is an idempotent element e_σ such that $e_\sigma C=\mathfrak{c}_\sigma$. Let $e_\sigma=\sum_{i-1}^r a_ib_i$, $a_1\in J_\sigma$, $b_i\in J_{\sigma^{-1}}$. Then we have

Proposition 10. *Under the above assumption, $e'_\sigma=\sum_{i=1}^r b_ia_i$ is an element in $\mathfrak{c}_\sigma$, and satisfies the following conditions;*

3) By Theorem 1 in [9], if A is a separable algebra over R, then A is strongly separable over R if and only if $A\otimes_R R\mathfrak{p}$ is strongly separable over $R\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of R.

1) $\sigma(x)=e'_\sigma x$ *for every* $x\in J_\sigma$,

2) $e'^2_\sigma=e_\sigma$ *and* $e'_\sigma C=\mathfrak{c}_\sigma$, *therefore* $\sigma^2|J_\sigma=1$.

Proof. Since $\sigma(x)\in J_\sigma$ for every $x\in J_\sigma$, we have $\sigma(x)=e_\sigma\sigma(x)=\sum_{i=1}^{r}a_ib_i\sigma(x)=\sum_{i=1}^{r}b_i\sigma(x)a_i=\sum_{i=1}^{r}b_ia_ix=e'_\sigma x$ for $x\in J_\sigma$. Now, $e'^2_\sigma=\sum_{ij}b_i(a_ib_j)a_j=\sum_{ij}(a_ib_j)b_ia_j=\sum_{ij}a_ib_j(b_ia_j)=\sum_{ij}a_i(b_ia_j)b_j=e^2_\sigma=e_\sigma$. It follows that $e'_\sigma C=\mathfrak{c}_\sigma$ and $\sigma^2(x)=\sigma(\sigma(x))=e'_\sigma\sigma(x)=e'^2_\sigma x=e_\sigma x=x$ for all x in J_σ.

OSAKA GAKUGEI DAIGAKU

References

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

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

[3] S. U. Chase, D. K. Harrison and A. Rosenberg: Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. no. 52 (1965).

[4] F. R. De Meyer: *Galois theory in algebra over a commutative ring*, to appear in Ill. J. Math.

[5] ———: *Some note on the general Galois theory of ring*, Osaka J. Math. **2** (1965) 117–127.

[6] T. Kanzaki: *On commutor ring and Galois theory of separable algebras*, Osaka J. Math. **1** (1964) 103–115.

[7] ———: *On Galois extension of rings*, Nagoya Math. J. (1965)

[8] ———: *A type of separable algebra*, J. Math. Osaka City Univ. **13** (1962) 39–43.

[9] ———: *Special type of separable algebra over a commutative ring*, Proc. Japan Acad. **40** (1964) 781–786.

[10] A. Rosenberg and D. Zelinsky: *Automorphisms of separable algebras*, Pacific. J. Math. **11** (1957) 1109–1118.

[11] Y. Takeuchi: *On Galois extension over a commutative ring*, Osaka J. Math. **2** (1965) 137–145.