

SUPPLEMENTARY RESULTS ON GALOIS EXTENSION

MANABU HARADA

(Received June 12, 1965)

Recently, Galois theory of commutative ring has been developed by Auslander, Chase, Goldman, Harrison and Rosenberg in [1], [2] and many important results in it has been generalized for separable R -algebra by DeMeyer, Kanzaki and Takeuchi in [3], [8], [9], [10] and [11]. There are some equivalent definitions of a Galois extension, which will be given in §1.

Let Λ be an R -algebra which is a finitely generated R -module and G a finite group of R -automorphisms of Λ .

In §2 we consider some relations between Λ^T and $V_\Lambda(\Lambda^T)$ for a Galois extension Λ with G and for a subgroup T , which contains some results in [3], [10] and [11]. We give a sufficient condition of Λ being a central Galois, which is a converse of [10], Theorem 2.

In §3 we study a criterion of the center C of Λ being a Galois extension. Let e be a primitive idempotent in C and $T = \{\sigma \in G, \sigma(e) = e\}$ and $H = \{\sigma \in T, \sigma \text{ induces the identity mapping on the center of } \Lambda e\}$. Under an assumption that R is indecomposable, we obtain that C is a Galois extension of R if and only if H is a normal subgroup in G , which is a generalization of [10], Proposition 10.

The author would like to express his thanks to Professor T. Kanzaki for many useful suggestions.

1. Definitions and notations.

Let R be a commutative ring with identity and Λ an R -algebra. We always assume that every R -algebra is finitely generated R -module. A group G means a finite group of R -algebra automorphisms of Λ . We recall the definition of Galois extension.

Let Γ be the fixed ring of G , which we denote by Λ^G . If Λ satisfies one of the following conditions, then we call Λ a *Galois extension of Γ with G* :

I. Λ is a finitely generated projective right Γ -module and $\Delta(\Lambda, G)$ is isomorphic to $\text{Hom}_\Gamma(\Lambda, \Lambda)$ by defining $(\lambda u_\sigma) \cdot \mu = \lambda \sigma(\mu)$, where $\Delta(\Lambda, G)$ is a trivial crossed product with basis u_σ and $\lambda, \mu \in \Lambda$.

II. There exist elements x_i, y_i in Λ such that $\sum_i x_i y_i = 1, \sum_i x_i \sigma(y_i) = 0$ if $\sigma \neq 1$.

We call such $\{x_i, y_i\}$ a Galois generator.

We know that this definition is symmetric with respect to right and left. By $c(\Lambda)$ we mean the center of Λ and we denote it by C sometimes.

We note that many results in [2] for a commutative case are valid with a slight modification for a non-commutative case. So we quote them without proof.

2. Central Galois extension

Let G be a finite group of automorphism of Λ as an R -algebra. We put $J_\sigma = \{x | \in \Lambda, xy = \sigma(y)x \text{ for all } y \text{ in } \Lambda\}$ for $\sigma \in G$. Then it is clear that J_σ is a C -module, $J_\sigma J_\tau \subseteq J_{\sigma\tau}$ and $J_1 = C$, where C is the center of Λ . First, we give a converse of [10], Theorem 2.

Theorem 1. *Let Λ be a separable R -algebra with automorphism group G . If $\Lambda = \sum_{\sigma \in G} \oplus J_\sigma$ and $J_\sigma J_{\sigma^{-1}} = C$ for any σ in G , then Λ is a Galois extension of the center C with G .*

*Proof.*¹⁾ Since Λ is R -separable, Λ is central separable by [1], Theorem 2.3. Hence, $\text{Hom}_C(\Lambda, \Lambda) \approx \Lambda_r \otimes_C \Lambda_l$ by [1] Theorem 2.1, where Λ_r (resp. Λ_l) means the set of multiplications of elements in Λ from the right (resp. left) side. $\Lambda_r = \sum \oplus (J_\sigma)_r$. It is clear that $(J_\sigma)_r = (J_\sigma)_l \sigma^{-1}$. Hence, $\Lambda_r \otimes_C \Lambda_l = \sum \oplus (J_\sigma)_l \Lambda_l \sigma^{-1} = \sum \oplus (J_\sigma \Lambda)_l \sigma^{-1} = \sum \Lambda_l \sigma = \Delta(\Lambda, G)$ since $J_\sigma \Lambda = \Lambda$ by the assumption.

The converse of the following corollary was given in [3], [13] and we shall consider it later.

Corollary. *Let Λ and C be as above. We assume that G consists of inner-automorphisms which is induced by unit elements u_σ . If $\Lambda = \sum \oplus C u_\sigma$, then Λ is a Galois extension of C with G .*

Proof. It is clear that $J_\sigma = C u_\sigma$ and $J_\sigma J_{\sigma^{-1}} = C$.

Proposition 2. *Let Λ be a separable R -algebra with automorphism group G . If $R = \Lambda^G$ and $J_\sigma = 0$ for $\sigma \neq 1$, then Λ is a Galois extension of R and Λ is a commutative ring. The converse is also true.*

1) The first proof was a little longer and Prof. Kanzaki pointed out this proof to the author.

Proof. We define an automorphism ψ of $\Lambda \otimes_R \Lambda$ by setting $\psi(\lambda \otimes \mu) = \lambda \otimes \sigma(\mu)$. Since Λ is separable over R , then there exist elements x_i, y_i in Λ such that $\sum x_i y_i = 1$ and $x(\sum x_i \otimes y_i) = (\sum x_i \otimes y_i)x$ for all $x \in \Lambda$. Hence, $x \sum x_i \otimes \sigma(y_i) = \sum x_i \otimes \sigma(y_i) \sigma(x)$. Therefore, $x \sum x_i \sigma(y_i) = \sum x_i \sigma(y_i) \sigma(x)$, which means $\sum x_i \sigma(y_i) \in J_{\sigma^{-1}} = (0)$ if $\sigma \neq 1$. Thus, we can find a Galois generator $\{x_i, y_i\}$. Hence, Λ is a Galois extension of R and $\Lambda = V_\Lambda(\Lambda^G) = C \oplus J_\sigma \oplus \dots = C$ by [10], Proposition 1.

Proposition 3. *Let Λ be a Galois extension of R with G and $C = \Lambda^H$ for a subgroup H . Then $H \cap T = (1)$ for a subgroup T of G if and only if $V_\Lambda(\Lambda^T) = C$. In this case we have $\Lambda^S = C^S \otimes_{C^T} \Lambda^T$ for $S \subseteq T$.*

Proof. We assume $H \cap T = (1)$. Then T is isomorphic to the induced automorphism group $T|C$. Hence, $\Lambda = C\Lambda^T$ by [3], Lemma 2. Therefore, $V_\Lambda(\Lambda^T) = V_\Lambda(C\Lambda^T) = C$. If $V_\Lambda(\Lambda^T) = C$, then $c(\Lambda^T) = C \cap \Lambda^T = C^T$. C and Λ are Galois extensions of C^T and Λ^T , respectively. Hence, $C \otimes_{C^T} \Lambda^T$ is a Galois extension of Λ^T . Since $c(C \otimes \Lambda^T) = C$ and $C \otimes \Lambda^T$ is separable, $C \otimes \Lambda^T \approx C\Lambda^T$. Hence, $C\Lambda^T$ and Λ are Galois extensions of Λ^T with T . Therefore, $C\Lambda^T = \Lambda$ by [2], Theorem 3.4, which means $H \cap T = (1)$. The last part is clear from [3], Lemma 2.

For a twised group ring the following lemma is well known.

Lemma 4. *Let $\Delta(\Lambda, G)$ be a trivial crossed product of R -algebra Λ and $H = \{\sigma \mid \sigma \in G, \sigma|c(\Lambda) = I_{c(\Lambda)}\}$. If Δ is R -separable then the order $|H|$ of H is a unit in R and $\text{Tr}_G(\Delta) = \Lambda^G$.*

Proof. Let $\Delta = \Delta(\Lambda, G) = \Lambda \oplus \Lambda\sigma \oplus \dots$. Since Δ is R -separable, there exists an element θ in $\Delta \otimes_R \Delta$ such that $\varphi(\theta) = 1$ and $\delta\theta = \theta\delta$ for $\delta \in \Delta$, where φ is a natural homomorphism of $\Delta \otimes \Delta$ to Δ . Let $\theta = \sum \oplus a_{\sigma, \tau}(\sigma \otimes \tau)$, where $a_{\sigma, \tau} = \sum_i \lambda_i(\sigma, \tau) \otimes \mu_i(\sigma, \tau) \in \Lambda \otimes_R \Lambda$. Since $\lambda\theta = \theta\lambda$ for $\lambda \in \Lambda$, we can easily see that $\varphi(a_{1,1})$ is in C . Furthermore, by the standard argument we has

$$(1) \quad \varphi(a_{1,1}) = \sum_i \rho(\lambda_i(\rho^{-1}, \rho) \cdot \mu_i(\rho^{-1}, \rho)) \quad \text{for } \rho \in G.$$

Let $G = H + H\tau_2 + \dots + H\tau_s$. Replacing ρ^{-1} by $\xi\tau_i$ in (1) we have $\tau_i^{-1}\varphi(a_{1,1}) = \sum \lambda_i(\sigma^{-1}, \sigma)\sigma^{-1}(\mu_i(\sigma^{-1}, \sigma))$, where $\sigma = \xi\tau_i$. Therefore, $1 = \varphi(\theta) = |H|(\varphi(a_{1,1}) + \tau_2^{-1}(\varphi(a_{1,1})) + \dots + \tau_s^{-1}(\varphi(a_{1,1}))) = |H|\text{Tr}_{G/H}(\varphi(a_{1,1}))$. Hence $|H|$ is a unit in R and $\text{Tr}_G(\Delta) = \Lambda^G$.

The following is a slight generalization of [10], Proposition 5.

Proposition 5. *Let Λ be a Galois extension of Λ^G with G and $H =$*

$\{\sigma \mid \sigma \in G, \sigma|C = I_C\}$. We assume Λ^G is R -separable. Then $|H|$ is a unit in R and $\text{Tr}_G(\Lambda) = \Lambda^G$.

Proof. By [8], Proposition 4 we know that $\Delta(\Lambda, G)$ is R -separable.

Proposition 6. *Let Λ be a Galois extension of an R -separable algebra Λ^G with G . Let H be a subgroup of G . Then the center of Λ^H is equal to C if and only if $V_\Lambda(\Lambda^H)$ is a Galois extension of C with H .*

Proof. We put $\Gamma = \Lambda^H$ and $\Omega = V_\Lambda(\Lambda^H)$. If the center of Γ is equal to C , then $\Lambda = \Gamma \otimes_C \Omega$ by [1], Theorem 3.3. We note that H induces an automorphism group on Ω . $\text{Hom}_C(\Omega, \Omega) \otimes_C \Gamma \approx \text{Hom}_\Gamma(\Omega \otimes_C \Gamma, \Omega \otimes_C \Gamma) \approx \Delta(\Omega \otimes_C \Gamma, H)$ since Λ is a Galois extension of Γ by [11], Theorem 1 and Ω is C -projective. Furthermore, $\Delta(\Omega \otimes_C \Gamma, H) \approx \Delta(\Omega, H) \otimes_C \Gamma$. In the above isomorphism we can easily check that $\Delta(\Omega, H)$ is isomorphic to $\text{Hom}_C(\Omega, \Omega)$ by the natural mapping. Hence, $C = \text{c}(\text{Hom}_C(\Omega, \Omega)) = V_{\text{Hom}_C(\Omega, \Omega)}(\Delta(\Omega, H)) = \Omega^H$. Therefore, Ω is a Galois extension of C with H . Conversely, it is clear that $\text{c}(\Gamma) = \text{c}(\Omega)$. Let x be in that center. Then $x \in V_\Lambda(\Omega) \cap \Omega = \Lambda^H \cap \Omega = \Omega^H = C$ by [8], Theorem 2. Hence, C is the center of Γ .

Corollary. *Let Λ be as above and Γ a separable C -subalgebra. Let $H = \{\sigma \mid \sigma \in G, \sigma(x) = x \text{ for } x \in V_\Lambda(\Gamma)\}$. Then H induces an automorphism group of Γ . If $\Gamma^H = C$, then Λ and Γ are Galois extensions of $V_\Lambda(\Gamma)$ and C with H , respectively.*

Proof. Since $V_\Lambda(V_\Lambda(\Gamma)) = \Gamma$, the first part is clear. Let x be in the center of Λ^H . Since $\Lambda^H \supseteq V_\Lambda(\Gamma)$, $x \in \Gamma \cap \Lambda^H = \Gamma^H = C$. Hence $V_\Lambda(\Lambda^H)$ is a Galois extension of C with H by Proposition 6. Furthermore, $V_\Lambda(\Lambda^H) \subseteq \Gamma$. If we apply [2], Theorem 3.4 to the inclusion map, we have $\Gamma = V_\Lambda(\Lambda^H)$. Hence, $V_\Lambda(\Gamma) = \Lambda^H$.

Corollary. *Let Λ be a Galois extension of Λ^G with G . We assume Λ^G is R -separable. Let H be an inner-subgroup of G which is induced by unit elements u_σ and $A = \sum C u_\sigma$. Then the following conditions are equivalent.*

- 1) $\text{c}(\Lambda^H) = C$.
- 2) $\Lambda = A \otimes_C \Lambda^H$.
- 3) A is a Galois extension of C with H .

In this cases $A = \Sigma \oplus C u_\sigma$.

Proof. It is clear that A is C -algebra and $V_\Lambda(A) = \Lambda^H$. Since $|H|$ is a unit by Lemma 4, A is C -separable by [5], Lemma 4. Hence,

$V_\Lambda(\Lambda^H) = A$ by [8], Theorem 2. Therefore, we have the first part by Proposition 6, since $c(A) = c(\Lambda^H)$. Since $A_r \otimes \Lambda_l \approx \Delta(\Lambda, H)$ $A = \sum \oplus C u_\sigma$.

3. Central subgroup.

Let Λ be a Galois extension of R with G and C the center of Λ . Let $H = \{\sigma \in G, \sigma|_C = I_C\}$. We call H the *central subgroup* of G .

In this section we study a criterion of C being the fixed ring of H .

First, we consider a criterion of a separable subalgebra Γ of Λ being a fixed subalgebra of a subgroup T .

In commutative case we know a condition “*strongly distinct*” (see [2], p. 16) and it was shown in [2] that this condition gives a criterion of the above. We shall generalize this condition to a case of non-commutative ring.

Let f, g be homomorphisms of R -algebra Γ to Λ ($f \neq g$). We consider a condition :

(*) For any $x \neq 0$ in Λ we can find y in Γ such that

$$x\Lambda(f(y) - g(y)) \neq (0).$$

If Λ and Γ are commutative and (*) is satisfied, then f and g are strongly distinct. Conversely, we assume $\Lambda = \Gamma$ and Λ is R -separable. If f, g are strongly distinct two automorphisms of Λ , then there exist elements x_i, y_i in Λ such that $\sum_i x_i y_i = 1$ and $\sum x_i f^{-1}g(y_i) = 0$ by [2], Lemma 1.2. Hence, $1 = \sum x_i (y_i - f^{-1}g(y_i)) = \sum f(x_i)(f(y_i) - g(y_i))$. Therefore, (*) is satisfied.

We note that if Λ is a Galois extension of R with G and T a subgroup, then Λ^T is R -separable (see, [9]).

Theorem 7. Let Λ be a Galois extension of R with G and Γ a separable R -subalgebra of Λ . We put $T = \{\sigma \in G, \sigma|_\Gamma = I_\Gamma\}$. Then $\Gamma = \Lambda^T$ if and only if distinct two elements σ, τ in G satisfy the above (*) on Γ condition.

Proof. We assume $\Gamma = \Lambda^T$. Then there exist x_i, y_i in Γ such that $\sum x_i y_i = 1$ and $\sum x_i \tau(y_i) = 0$ if $\tau \notin T$ by [2], p. 23. Hence, Γ satisfies (*). Conversely, we assume Γ satisfies (*). $\alpha = \text{Hom}_R(\Lambda, \Lambda) \approx \Delta(\Lambda, G) = \sum \oplus \Lambda_l \cdot \tau$ and $\text{Hom}_\Gamma(\Lambda, \Lambda) = V_\alpha(\Gamma_r)$. Let x be in $V_\alpha(\Gamma_r)$. $x = x(1)_l + x(\sigma)_l \sigma + \dots$. Since $\gamma_r x = x \gamma_r$ for any $\gamma \in \Gamma$, we have $\gamma_r x(\sigma)_l = x(\sigma)_l \gamma_r = x(\sigma)_l \sigma(\gamma)_r$. Hence, $x(\sigma) \Lambda(\gamma - \sigma(\gamma)) = (0)$. Since Γ satisfies (*), if $\sigma \notin T$, $x(\sigma) = 0$. Therefore, $\text{Hom}_\Gamma(\Lambda, \Lambda) = \sum_{\tau \in T} \oplus \Lambda_l = \Delta(\Lambda, T)$. Since $c(\alpha) = R$ and

Γ_r is separable R -algebra, $\Gamma_r = V_\Lambda(V_\Lambda(\Gamma_r)) = V_\Lambda(\Delta(\Lambda, T)) = (\Lambda^T)_r$ by [8], Theorem 2.

Corollary. *Let Λ, Γ, G and T be as above. We assume that R is a hereditary ring. Then $\Gamma = \Lambda^T$ for a subgroup T if and only if Γ is G -strong, (see the definition in [2], p. 22).*

Proof. It is sufficient to show that the condition “ G -strong” implies the above condition (*), if R is hereditary. We note that if $x\Lambda$ is Λ -projective, then $x\Lambda \approx e\Lambda$ for an idempotent e . Hence, if $x\Lambda(y - \sigma(y)) = 0$ for all $y \in \Gamma$ and $\sigma \in T$, then $e\Lambda(y - \sigma(y)) = (0)$. Hence, $e = 0$ and $x = 0$. Thus, we may show that Λ is right hereditary. Since $\Delta(\Lambda_r, G) \approx \text{Hom}_R^l(\Lambda, \Lambda)$ and Λ is R -projective, $\Delta(\Lambda_r, G)$ is right hereditary by [5], Lemma 1.2. Hence, Λ_r is right hereditary by [4], Proposition 10.

REMARK. We can easily extend the same argument of [2], §2 to a non-commutative case except Theorem 2.2 in [2]. Theorem and its corollary are concerned with that theorem.

Finally, we consider the problem mentioned in the beginning of this section. Namely we consider the case in which T is the central group and $\Gamma = C$ in Theorem 7.

We always assume that C is a direct sum of indecomposable ideals (e.g. if R is indecomposable, then C is as above, see [7], Theorem 7).

Let e_1, e_2, \dots, e_n be the set of primitive idempotents in C . Let $T_i = \{\sigma \in G, \sigma(e_i) = e_i\}$. We call T_i a *decomposition group* of e_i . We can classify e_i by a relation $e_i \equiv e_j$ if $e_j = \sigma(e_i)$ for some $\sigma \in G$. Let e_i be one of the classes. Then $E_i = \sum_{e_j \in e_i} e_j$ is an idempotent and $E_i \in \Lambda^G = R$. In this case $\Lambda = \sum_i \Lambda E_i$ and we can easily see that if Λ is a Galois extension of R with G , then each ΛE_i is a Galois extension of RE_i with G , which implies that each element of G operates faithfully on each ΛE_i . The converse is clear.

Lemma 8. *Let C be a commutative separable R -algebra as above, and $R = C^G$. C is a Galois extension of R with G if and only if for $\sigma \neq 1$ in G there exist no idempotents e such that $\sigma|Ce = I_{Ce}$.*

Proof. Let $\sigma \neq 1$. If there exists e such that $\sigma|Ce = I_{Ce}$, then $\sigma(C(1 - e)) = C(1 - e)$. Hence, σ is not strongly distinct from 1. Conversely, if σ is not strongly distinct from 1, then there exists an idempotent e such that $\sigma(x)e = xe$ for all $x \in C$. We may assume that e is primitive. Then $\sigma(e) = e$. Hence, $\sigma|Ce = I_{Ce}$.

Proposition 9. *Let Λ be a Galois extension of R with G . We assume*

a natural homomorphism φ of $\Delta(\Lambda, G)$ to $\text{Hom}_R(\Lambda, \Lambda) = \text{Hom}_R(\Lambda e_1 \oplus \cdots \oplus \Lambda e_i, \Lambda e_1 \oplus \cdots \oplus \Lambda e_i)$. We consider an operation of $\varphi(\Delta(\Lambda_i, T_i)u_{\sigma_i, j})$ on Λe_k . If $\sigma_{i, j}(e_k) = e_i$, $\varphi(\Delta(\Lambda_i, T_i)u_{\sigma_i, j})(\Lambda e_k) = \varphi(\Delta(\Lambda_i, T_i))(\Lambda e_i)$. Since Λ_i is a Galois extension of Re_i , $\varphi(\Delta(\Lambda_i, T_i)) \approx \Delta(\Lambda_i, T_i) = \text{Hom}_R(\Lambda e_i, \Lambda e_i)$. Hence, $\Delta(\Lambda_i, T_i)u_{\sigma_i, j} \approx \varphi(\Delta(\Lambda_i, T_i)u_{\sigma_i, j}) = \text{Hom}_R(\Lambda e_k, \Lambda e_i)$ and $\varphi(\Delta(\Lambda_i, T_i)u_{\sigma_i, j})(\Lambda e_{k'}) = (0)$ if $k \neq k'$. Conversely, we can find, for $\text{Hom}_R(\Lambda e_i, \Lambda e_j)$, $\Delta(\Lambda_s, T_s)u_\sigma$ such that $\varphi(\Delta(\Lambda_s, T_s)u_\sigma) \approx \text{Hom}_R(\Lambda e_i, \Lambda e_j)$. Hence, φ is isomorphic. Therefore, Λ is a Galois extension of R with G .

OSAKA CITY UNIVERSITY

References

- [1] M. Auslander and O. Goldman: *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960) 337-409.
- [2] S.U. Chase, D.K. Harrison and A. Rosenberg: *Galois theory and Galois cohomology of commutative ring*, Mem. Amer. Math. Soc. no. 52 (1965).
- [3] F. R. DeMeyer: *Some note on the general Galois theory of ring*, Osaka J. Math. **2** (1965) 117-127.
- [4] M. Harada: *Note on dimension of modules and algebras*, J. Inst. Polytech. Osaka City Univ. **7** (1956) 17-27.
- [5] —————: *Multiplicative ideal theory in hereditary orders*, J. Math. Osaka City Univ. **14** (1963) 83-106.
- [6] —————: *Some criterion for heredity of crossed products*, Osaka J. Math. **1** (1964) 69-80.
- [7] D. K. Harrison: *Abelian extension of commutative rings*, Mem. Amer. Math. Soc. no. 52, (1965).
- [8] T. Kanzaki: *On commutator ring and Galois theory of separable algebras*, Osaka, J. Math. **1** (1964) 103-115.
- [9] —————: *On Galois extension of rings*, Nagoya Math. J. to appear.
- [10] —————: *On a Galois extension algebra over a commutative ring*, to appear in this J.
- [11] Y. Takeuchi: *On Galois extensions over commutative rings*, Osaka J. Math. **2** (1965) 137-145.