ON GALOIS EXTENSION OF RINGS

TERUO KANZAKI

To the memory of TADASI NAKAYAMA

1. Introduction. Let Λ be a ring and G a finite group of ring automorphisms of Λ. The totality of elements of Λ which are left invariant by G is a subring of Λ. We call it the G-fixed subring of Λ. 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 $\lambda \in \Lambda$, and let Γ be a subring of the G-fixed subring of Λ which has the same identity as Λ. Then we have a ring homomorphism

$$\delta: \ \Delta(\Lambda, G) \to \mathrm{Hom}_\Gamma^r(\Lambda, \Lambda)$$

defined by $\delta(\lambda u_\sigma)(x) = \lambda\sigma(x)$, where $\mathrm{Hom}_\Gamma^r(\Lambda, \Lambda)$ is the Γ-endomorphism ring of Λ regarded as Γ-right module.

In [4], we generalized the notion of Galois extension, which was first defined by Auslander and Goldman [1] for commutative rings, to non commutative case, and discussed the Galois theory for non commutative rings. Our definition of Galois extension is as follows. A ring Λ is called a *Galois extension* of Γ relative to G if the following conditions are satisfied:

I. Γ is the G-fixed subring of Λ,

II. Λ is a finitely generated projective Γ-right module,

III. δ is an isomorphism of $\Delta(\Lambda, G)$ to $\mathrm{Hom}_\Gamma^r(\Lambda, \Lambda)$.

On the other hand, Chase, Harrison and Rosenberg [3] gave another definition of Galois extension, which is equivalent to the above in commutative case, and developed a Galois theory for commutative rings. In order to state other definition, we set $Tr(x) = \sum_{\sigma\in G}\sigma(x)$ for $x \in \Lambda$. Then Λ is called to be a Galois extension of Γ relative to G if the following two conditions are satisfied:

CHR I. $\Gamma = Tr(\Lambda)$.

CHR II. There exist $x_1, x_2, \ldots$ and x_r and $y_1, y_2, \ldots y_r$ in Λ such that

Received February 8, 1965.

https://doi.org/10.1017/S0027763000011831 Published online by Cambridge University Press

for $\sigma \in G$ $\sum_i x_i\sigma(y_i) = \begin{cases} \mathrm{I}, & \text{if } \sigma = 1 \\ 0, & \text{if } \sigma \neq 1. \end{cases}$

In §2, we discuss the relationship between these two definitions of Galois extension and we shall show that if Λ and Γ are algebras over a commutative ring R and Γ is R-separable then they are equivalent to each other. In §3, we shall give an improvement of the Galois theory established in [4] which is also a generalization of the Galois theory in [3] to non commutative case. In §4, for a Galois extension Λ of Γ relative to G, we consider a ring-automorphism ρ of Λ which leaves invariant each element of Γ and we shall show that ρ is an element of G under some assumption.

2. Galois extension. Throughout this section, Λ stands for a ring with identity, G a finite group of ring automorphisms of Λ and Γ a subring of Λ which has the same identity as Λ. We shall call Λ a Galois extension of Γ relative to G if the three condition I, II, III in §1 are satisfied. Λ is regarded as $\Delta(\Lambda, G)$- left module through δ. Then a right multiplication of an element γ of Γ induces a $\Delta(\Lambda, G)$- endomorphism of Λ if Γ is a subring of the G-fixed subring of Λ We shall denote it by γ_r and set $\{\gamma_r \mid \gamma \in \Gamma\} = \Gamma_r$. Then the condition I is equivalent to

I′. $$\Gamma_r = \mathrm{Hom}^l_\Delta(\Lambda, \Lambda).$$

The following lemma is proved in [4].

LEMMA 2.1. *Λ is a Galois extension of Γ relative to G if and only if $\Gamma_r = Hom^l_\Delta(\Lambda, \Lambda)$ and $\Delta(\Lambda, G) = \Lambda u \Lambda$, where $u = \sum_{\sigma \in G} u_\sigma$.*

LEMMA 2.2. *$\Lambda u \Lambda = \Delta(\Lambda, G)$ if and only if the condition CHR*II *holds.*

Proof. Since $\Lambda u \Lambda$ is a two sided ideal of $\Delta(\Lambda, G)$, $\Delta(\Lambda, G) = \Lambda u \Lambda$ if and only if $1 \in \Lambda u \Lambda$. But $1 \in \Lambda u \Lambda$ if and only if there exist $x_1, x_2, \ldots x_r, y_1, y_2, \ldots y_r$ in Λ such that $1 = \sum_{i=1}^r x_i u y_i = \sum_{i=1, \sigma \in G}^r x_i\sigma(y_i) u_\sigma$. Thus we obtain this lemma.

PROPOSITION 2.3. *$Tr(\Lambda) = Hom^l_\Delta(\Lambda, \Lambda)$ if and only if Λ is a finitely generated projective Δ-module.*

Proof. In Lemma 3 in [4], we obtained the isomorphism κ; $\mathrm{Hom}^l_\Delta(\Lambda, \Delta) \to u\Lambda$, defined by $\kappa(f) = f(1)$. For the homomorphism γ: $\mathrm{Hom}^l_\Delta(\Lambda, \Delta) \to \mathrm{Hom}^l_\Delta(\Lambda, \Lambda)$ defined by $\gamma(f)(\lambda) = f(\lambda)1$, the following diagram is commutative;

https://doi.org/10.1017/S0027763000011831 Published online by Cambridge University Press

$$\begin{array}{ccc} \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta) & \xrightarrow{\gamma} & \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda) \\ \downarrow{\scriptstyle\kappa} & & \downarrow{\scriptstyle\kappa'} \\ u\Lambda & \xrightarrow{\gamma'} & \Lambda \end{array}$$

where κ' is a monomorphism defihed by $\kappa'(f) = f(1)$ for $f \in \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda)$, and γ' is a homomorhpism defined by $\gamma'(u\lambda) = (u\lambda)1 = Tr(\lambda)$ for $u\lambda \in u\Lambda$. Since $\mathrm{Im}(\gamma'\kappa) = \mathrm{Im}(\gamma') = Tr(\Lambda)$, $\mathrm{Im}(\kappa') = Tr(\Lambda)$ if and only if γ is an epimorphism. On the other hand, for epimorphism τ: $\mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda) \to \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta) \otimes_{\Delta} \Lambda$ defined by $\tau(f) = f \otimes 1$, and for the homomorphism μ: $\mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta) \otimes_{\Delta} \Lambda \to \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta)$ defined by $\mu(f \otimes \lambda)(x) = f(x)\lambda$, we have the following commutative diagram:

$$\begin{tikzcd} \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta) \arrow[r, "\gamma"] \arrow[d, "\tau"] & \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda) \\ \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Delta) \otimes_{\Delta} \Lambda \arrow[ur, "\mu"'] & \end{tikzcd}$$

Because, for $f \in \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda)$, $\mu\tau(f)(\lambda) = \mu(f \otimes 1)(\lambda) = f(\lambda)1 = \gamma(f)(\lambda)$. Therefore γ is an epimorphism if and only if μ is an epimorphism. But by Proposition A. 1 in [2], μ is an epimorphism if and only if Λ is a finitely generated projective Δ-module. Therefore we obtain this proposition.

Proposition 2.4. *a) Λ is a Galois extension of Γ relative to G if and only if the condition I and CHR II. are satisfied. b) The condition CHR I. holds if and only if the condition I holds and Λ is a finitely generated projective Δ-module.*

Proof. a) is obtained in above. b) Since $Tr(\Lambda)$ is a two sided ideal of the G-fixed subring of Λ, $Tr(\Lambda) = \Gamma$ if and only if $Tr(\Lambda)_r = \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda)$ and $\Gamma_r = \mathrm{Hom}^{l}_{\Delta}(\Lambda, \Lambda)$. Therefore b) follows from Proposition 2.3.

Theorem 2.5. *Let $\Gamma \subset \Lambda$ be algebras over a commutative ring R, and let Γ be separable over R. Then Λ is a Galois extension of Γ relative to G if and only if the conditions CHR I. and CHR II. hold.*

Proof. If Γ is separable over R and Λ is a Galois extension of Γ relative to G, then $\Delta = \mathrm{Hom}^{r}_{\Gamma}(\Lambda, \Lambda)$ is separable over R and Λ is a finitely generated projective Δ-module by Colrollary 1 in [4]. Therefore by Proposition 2.4 CHR I. and CHR II. hold. The converse follows from Proposition 2.4.

Corollary 2.6. (Chase, Harrison and Rosenberg) *Let Λ be a commutative ring. Λ is a Galois extension of Γ relative to G if and only if the conditions CHR I. and CHR II. hold.*

https://doi.org/10.1017/S0027763000011831 Published online by Cambridge University Press

Proof. Setting $\Gamma=R$ in Theorem 2.5 we have this corollary.

3. **Galois theory.** In this section, we shall improve Theorem 5 in [4] and develope the Galois theory of separable algebra over a commutafive ring having the indecomposable center by using the Galois theory of commutative indecomposable ring in [3].

PROPOSITION 3.1. *Let $\Gamma\subset\Lambda$ be algebras over a commutative ring R, Λ a Galois extension of Γ ralative to G, and Γ a separable algebra over R. Then, for every subgroup H of G, the H-fixed subring Λ^H of Λ is also a separable algebra over R.*

Proof. Since Γ is separable over R, by Proposition 4 in [4] $\Delta(\Lambda, G)$ is also separable over R. For the decompositions of G with respect to H; $G=H\sigma_1+H\sigma_2+\cdots+H\sigma_r=\sigma_1'H+\sigma_2'H+\cdots+\sigma_r'H$, $\sigma_1=\sigma_1'=1$, we have $\Delta(\Lambda,G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma=\Delta(\Lambda,H)\oplus\sum_{i=2}^{r}\Delta(\Lambda,H)u_{\sigma_i}$ and $\sum_{i=2}^{r}\Delta(\Lambda,H)u_{\sigma_i}=\sum_{i=2}^{r}u_{\sigma_i'}\Delta(\Lambda,H)$. We shall show that $\Delta(\Lambda,H)$ is an R-separable subalgebra of $\Delta(\Lambda,G)$. Since $\Delta(\Lambda,G)$ is separble over R, $\Delta(\Lambda,G)$ is a $\Delta(\Lambda,G)^e$-projective module. Now $\Delta(\Lambda,G)^e=\Delta(\Lambda,G)\otimes_R\Delta(\Lambda,G)^0=\sum_{i,j}\oplus\Delta(\Lambda,H)^e u_{\sigma_i}\otimes u^0_{\sigma_{j'}}$, therefore $\Delta(\Lambda,G)$ is a $\Delta(\Lambda,H)^e$-projective module. Since $\Delta(\Lambda,H)$ is a direct summand of $\Delta(\Lambda,G)$ as $\Delta(\Lambda,H)^e$-module, $\Delta(\Lambda,H)$ is $\Delta(\Lambda,H)^e$-projective, therefore $\Delta(\Lambda,H)$ is separable over R. On the other hand, Λ is a finitely generated projective Γ-module, hence by Corollary 1 in [4] Λ is a finitely generated projective $\Delta(\Lambda,G)$-module. Since $\Delta(\Lambda,G)$ is a $\Delta(\Lambda,H)$-free module, Λ is a finitely generated projective $\Delta(\Lambda,H)$-module. Therefore by Corollary 1 in [4] $\mathrm{Hom}_{\Delta(\Lambda,H)}(\Lambda,\Lambda)=\Delta^H$ is separable over R.

Using Theorem 2.3 in [3] and Theorem 5 in [4], we have

THEOREM 3.2. *Let Λ and Γ be separable algebras over a commutative ring R, and suppose that the following conditions are satisfied:*

1) *The center C of Λ is indecomposable.*

2) *There is a finite group G of ring automorphisms of Λ such that G induces the group of automorphisms of C isomorphic to G.*

3) *Γ is the G-fixed subring of Λ.*

4) *Λ is finitely generated and projective over R.*

Then Λ is a Galois extension of Γ relative to G, and there is a $1-1$ dual cor-

respondence between subgroups of G and R-separable subalgebra of Λ containing Γ in the usual sense of Galois theory.

Proof. Simce Λ is separable and finitely generated projective over R, the center C of Λ is finitely generated projective and separable over R. From Theorem 2.3 in [3], the indecomposable ring C is a Galois extension of the G-fixed subring S of C relative to G. From Theorem 5 in [4], Λ is a Galois extension of Γ relative to G. By Proposition 3.1, for every subgroup H of G the H-fixed subring Λ^H is separable over R, and Λ is a Galois extension of Λ^H relative to H by Theorem 5 in [4]. Conversely, for every separable subalgebra Ω over R such that $\Gamma \subset \Omega \subset \Lambda$, Ω is separable over S, and Proposition 6 in [4] holds for the indecomposable ring C by Theorem 3.3 in [3], hence by the same argument as in Theorem 5 in [4] we have that Λ is a Galois extension of Ω relative to a subgroup of G. Therefore Ω is the fixed subring of Λ by a subgroup of G. Thus we obtain a Galois theory for separable algebra over R.

4. Automorphisms of Galois extension. In this section, we assume that Λ is a central separable algebra over C, G is a finite group of ring automorphisms of Λ which induces the group of automorphisms of C isomorphic to G, and for the G-fixed subring R of C, C is a Galois extension of R relative to G. Then by Theorem 5 in [4] Λ is a Galois extension of Γ relative to G, where Γ is the G-fixed subring of Λ.

LEMMA 4.1. *Let C be a ring, M a projective C-module. For any subset x_1, $x_2, \ldots x_n$ in M, in which at least one element x_i is not zero, there exist elements $c_1, c_2, \ldots c_n$ in C such that at least one of c_i's is not zero and $\sum_{i=1}^{n} x_i y_j = 0$ with $y_i \in C$ implies always $\sum_{i=1}^{n} c_i y_i = 0$.*

Proof. we can prove the lemma similarly to Lemma 6 in [4].

PROPOSITION 4.2. *Let ρ be a ring automorphism of Λ which leaves invariant each element of Γ. Then we have $\rho = \sum_{\sigma = G} \lambda_\sigma \sigma$ where $\{\lambda_\sigma\}$ is a family of orthogonal idempotents in the center C, and $1 = \sum_{\sigma \in G} \lambda_\sigma$. Furthermore, if $\sigma \neq \tau$ and $\lambda_\sigma \neq 0$ $\lambda_\tau \neq 0$, then $\sigma^{-1}(\lambda_\sigma) \neq \tau^{-1}(\lambda_\tau)$.*

Proof. Since $\rho \in \mathrm{Hom}_{\Gamma}^{r}(\Lambda, \Lambda) \cong \Delta(\Lambda, G) = \sum_{\sigma \in G} \oplus \Lambda u_\sigma$, we have $\rho = \sum_{\sigma \in G} \lambda_\sigma \sigma$ with $\lambda_\sigma \in \Lambda$. For any x in Λ, $\rho \cdot x = \rho(x) \cdot \rho$, therefore $\sum_{\sigma \in G} \lambda_\sigma \cdot \sigma(x) \cdot \sigma = (\sum_{\tau \in G} \lambda_\tau \tau(x)) \cdot$

$(\sum_{\sigma\in G}\lambda_\sigma\sigma)$, and we obtain

$$(*) \qquad \lambda_\sigma\sigma(x) = \sum_{\tau\in G}\lambda_\tau\tau(x)\lambda_\sigma \qquad \text{for } x\in\Lambda \text{ and } \sigma\in G.$$

If x is taken in C, then $\lambda_\sigma\sigma(x) = \sum_{\tau\in G}\lambda_\tau\lambda_\sigma\tau(x)$, therefore $\sum_{\substack{\sigma\neq\tau\\ \tau\in G}}\lambda_\tau\lambda_\sigma\tau(x) + (\lambda_\sigma^2 - \lambda_\sigma)\sigma(x) = 0$ for any x in C. By Lemma 4.1 and linearly independence of $\{\sigma\}_{\sigma\in G}$ over C, we obtain $\lambda_\sigma = \lambda_\sigma^2$ and $\lambda_\tau\lambda_\sigma = 0$ for $\tau\neq\sigma$. Therefore $\{\lambda_\sigma\}$ is a family of orthogonal idempotents and $\sum_{\sigma\in G}\lambda_\sigma = 1$ since $\rho(1)=1$. On the orther hand, from $(*)$ we have for x, y in Λ, $\lambda_\sigma\sigma(xy) = \sum_{\tau\in G}\lambda_\tau\tau(xy)\lambda_\sigma$, and we have $\lambda_\sigma\cdot\sigma(x)\cdot\sigma(y) = \sum_{\tau\in G}\lambda_\tau\tau(x)\lambda_\sigma\tau(y)$ for any $x\in\Lambda$ and $y\in C$. By the same reason as above, we have $\lambda_\sigma\cdot\sigma(x) = \lambda_\sigma\sigma(x)\lambda_\sigma$ and $\lambda_\tau\cdot\tau(x)\cdot\lambda_\sigma = 0$ for $\tau\neq\sigma$, therefore $\lambda_\sigma x = \lambda_\sigma\cdot x\lambda_\sigma$ for every x in Λ. On the other hand, for any x in Λ, $x\lambda_\sigma = \sum_{\tau\in G}\lambda_\tau x\lambda_\sigma = \sum_{\tau\in G}\lambda_\tau x\lambda_\tau\lambda_\sigma = \lambda_\sigma x\lambda_\sigma$, therefore λ_σ is contained in the center C of Λ. Since $\rho(\Lambda)=\Lambda$, for any y in Λ there exist x in Λ such that $y = \rho(x) = \sum_{\sigma\in G}\lambda_\sigma\cdot\sigma(x)$. Since $\lambda_\sigma y = \lambda_\sigma\cdot\sigma(x) = \sigma(\sigma^{-1}(\lambda_\sigma)\cdot x)$ for each σ in G, it follows that $\sigma^{-1}(\lambda_\sigma y) = \sigma^{-1}(\lambda_\sigma)\cdot x$ for each $\sigma\in G$. Accordingly, if λ_σ and λ_τ are non zero and $\sigma\neq\tau$, then $\sigma^{-1}(\lambda_\sigma)\neq\tau^{-1}(\lambda_\tau)$. Because, if $\sigma^{-1}(\lambda_\sigma) = \tau^{-1}(\lambda_\tau)$ then $\sigma^{-1}(\lambda_\sigma y) = \tau^{-1}(\lambda_\tau y)$. Put $y=\lambda_\sigma$, and we have $\sigma^{-1}(\lambda_\sigma) = \sigma^{-1}(\lambda_\sigma^2) = \tau^{-1}(\lambda_\tau\lambda_\sigma) = \tau^{-1}(0) = 0$, it is a contradiction.

Corollary 4.3. *If the center C of Λ is indecomposable, then any Γ-ring automorphism of Λ is contained in G.*

Proposition 4.4. *If there are orthogonal indecomposable idempotent elements $e_1, e_2 \ldots e_n$ in C such that $\sum_{i=1}^n e_i = 1$, and if there exist $\sigma_1, \sigma_2, \ldots \sigma_n$ of G such that $\sigma_i^{-1}(e_i)\neq\sigma_j^{-1}(e_j)$ for $i\neq j$, then $\rho = \sum_{i=1}^n e_i\sigma_i$ is a Γ-ring automorphism of Λ.*

Proof. ρ is clearly a ring endomorphism, and leaves invariant each element of Γ. Now, we shall show that ρ is an epimorphism of Λ to Λ. Since e_i is indecomposable in C and $\sum_{i=1}^n e_i = 1$, $\sigma_j^{-1}(e_i)$ is also indecomposable in C and $\sum_{j=1}^n\sigma_i^{-1}(e_j) = 1$ for each i, therefore $\sigma_i^{-1}(e_i)$ is one of $\{e_k\}$. But, $\sigma_i^{-1}(e_i)\neq\sigma_j^{-1}(e_j)$ for $i\neq j$, hence $\{e_1, e_2, \ldots e_n\} = \{\sigma_1^{-1}(e_1), \sigma_2^{-1}(e_2), \ldots \sigma_n^{-1}(e_n)\}$. Therefore $1 = \sum_{i=1}^n\sigma_i^{-1}(e_i)$, and $\sigma_i^{-1}(e_i)\cdot\sigma_j^{-1}(e_j) = 0$ for $i\neq j$. For any y in Λ, put $x_i = \sigma_i^{-1}(e_i)\cdot\sigma_i^{-1}(y)$, $i = 1, 2, \ldots n$, and $x = \sum_{i=1}^n x_i$, then $\sigma_j^{-1}(e_j)x_i = 0$ for $i\neq j$, and $\sigma_i^{-1}(e_i)x_i = x_i$. Hence $\rho(x) = \sum_{i=1}^n e_i\sigma_i(x) = \sum\sigma_i(\sigma_i^{-1}(e_i)x) = \sum_i\sigma_i(x_i) = \sum_i\sigma_i(\sigma_i^{-1}(e_i)\sigma_i^{-1}(y)) = \sum_{i=1}^n e_i y = y$. Thus

ρ is an epimorphism.

We shall prove that ρ is a monomorphism. The following proof of this part is due to Professor H. Nagao. If $\rho(x)=0$, then $\sigma_j^{-1}(\rho(x))=\sum_{i\neq j}\sigma_j^{-1}(e_i)\sigma_j^{-1}(\sigma_i(x))$ $+\sigma_j^{-1}(e_j)x=0$ for each j, and $\sigma_j^{-1}(e_j)\sigma_j^{-1}(\rho(x))=\sigma_j^{-1}(e_j)x=0$ for $j=1, 2, \ldots n$, therefore $x=\sum_{j=1}^{n}\sigma_j^{-1}(e_j)x=0$. Accordingly, ρ is an automorphism of Λ.

References

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

[2] ——, Maximal order, Trans. Amer. Math. Soc. Vol. **97** (1960), 1-24.

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

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

Osaka Gakugei Daigaku