Kanzaki, T.
Osaka J. Math.
1 (1964), 103-115

ON COMMUTOR RINGS AND GALOIS THEORY OF SEPARABLE ALGEBRAS

TERUO KANZAKI

(Received May 20, 1964)

The purpose of this paper is to establish the Galois theory for a separable algebra over a commutative ring in the sense of Auslander-Goldman [1]. The notion of Galois extension defined in [1] for a commutative ring will be naturally extended to a non commutative ring in the following way. Let Λ be a ring, G a finite group of ring-automorphisms of Λ, and Γ the fixed subring of Λ under G, i.e. the totality of elements which are left invariant by G. If the homomorphism δ of the crossed product $\Delta(\Lambda, G)$ of Λ and G with trivial factor set to the Γ-endomorphism ring $\mathrm{Hom}_{\Gamma}^{r}(\Lambda, \Lambda)$ of Λ as Γ-right module; $\delta: \Delta(\Lambda G)=\sum_{\sigma\in G}\oplus\Lambda u_{\sigma}\to\mathrm{Hom}_{\Gamma}^{r}(\Lambda, \Lambda)$ defined by $\delta(\lambda u_{\sigma})(x)=\lambda\cdot\sigma(x)$ for λ, $x\in\Lambda$, is an isomorphism, and if Λ is a finitely generated projective Γ-right module, then Λ is called a *Galois extension* of Γ relative to G.

In § 1 we shall show that a commutor ring of an arbitrary separable subalgebra Γ over R in the central separable algebra Λ over R (we denote it by $V_{\Lambda}(\Gamma)$) is also a separable algebra over R, and $V_{\Lambda}(V_{\Lambda}(\Gamma))=\Gamma$. Further we obtain that if Λ is an R-separable algebra and M is a finitely generated faithful Λ-projective module then for $\Omega=\mathrm{Hom}_{\Lambda}(M, M)$ M is a finitely generated Ω-projective module, and $\mathrm{Hom}_{\Omega}(M, M)=\Lambda$. In § 2 we shall show that for Galois extension of non commutative ring we have similar results to the case of commutative ring in [1]. Moreover we shall show that if Λ is a Galois extension of Γ relative to G and H is a subgroup of G then for the fixed subring Ω of Λ under H Λ is a Galois extension of Ω relative to H. In § 3 we consider a Galois extension of a separable algebra and its crossed product with trivial factor set. Let Λ be a central separable algebra over C and G a finite group of (ring-) automorphisms of Λ as follows; 1) G induces a group of automorphisms of C such that it is isomorphic to G, 2) for the fixed subring R of C under G C is a Galois extension of R relative to G. Then we can prove that the crossed product $\Delta(\Lambda, G)$ of Λ and G with trivial factor set is a separable algebra over R. In § 4 we have the Galois theorem under the above assumption in §3. That is

1) if Γ is the fixed subring of Λ under G then Λ is a Galois extension of Γ relative to G and Γ is a central separable algebra over R,
2) Γ is a direct summand of Λ as Γ-two sided module,
3) for an arbitrary subgroup H of G and the fixed subring Ω of Λ under H, Λ is a Galois extension of Ω relative to H, and Ω is a separable algebra over R. Moreover if we suppose that C is an integral domain, then we have
4) if Ω is an arbitray intermediate subring between Λ and Γ such that Ω is a separable algebra over R, then Λ is a Galois extension of Ω relative to H where

$$H=\{\sigma\in G\,|\,\sigma(x)=x \quad \text{for all} \quad x\in\Omega\}\,.$$

Throughout this paper we assume that every ring has an identity element, every subring of a ring has common identity element, and every module is unitary. Furthermore we shall denote by the ring R always a commutative ring and an R-algebra means an algebra over R, and a central R-algebra means an algebra having the center R. We use the same notation as in [1].

1. Commuter ring in a central separable algebra

This section is concerned with a central separable R-algebra Λ and a separable R-subalgebra Γ of Λ containing R. We denote by $V_\Lambda(\Gamma)$ the subring of Λ which consists of all element λ satisfying $\gamma\lambda=\lambda\gamma$ for all $\gamma\in\Gamma$.

Lemma 1. (*Auslander, Goldman*) *Let Λ be a central separable R-algebra and Γ a central separable R-subalgbra of Λ having the same center R. Then $V_\Lambda(\Gamma)$ is central separable R-algebra and $V_\Lambda(V_\Lambda(\Gamma))=\Gamma$.*

Proof. See [1], Theorem 3. 3.

Lemma 2. *Let Λ be a separable R-algebra and M a Λ-module. If M is a finitely generated projective R-module then M is a finitely generated projective Λ-module* (cf. [1], Theorem 1. 8).

Proof. For any Λ-module N we have the isomorphism

$$\theta:\ \mathrm{Hom}_{\Lambda^e}(\Lambda,\ \mathrm{Hom}_R(M,N))\longrightarrow \mathrm{Hom}_\Lambda(M,N)$$

defined by $\theta(g)(m)=g(1)(m)$ for $g\in\mathrm{Hom}_{\Lambda^e}(\Lambda,\ \mathrm{Hom}_R(M,N))$, $m\in M$. Since Λ is a projective Λ^e-module and M is a projective R-module,

$\mathrm{Hom}_{\Lambda^e}(\Lambda, \mathrm{Hom}_R(M, N))$ is an exact functor relative to N, therefore $\mathrm{Hom}_\Lambda(M, N)$ is so. Consequently, M is a projective Λ-module.

Theorem 1. *Let M be a faithfule Λ-module, and set $\Omega = \mathrm{Hom}_\Lambda(M, M)$. If Λ is a separable R-algebra and M is a finitely generated projective Λ-module, then we have that Ω is also a separable R-algebra, M is a finitely generated projective Ω-module and $\mathrm{Hom}_\Omega(M, M) = \Lambda$. If Λ is central over R then Ω is also central over R.*

Proof. Let M be a faithful and finitely generated projective Λ-module, and let Λ be a central separable C-algebra. Since Λ is a finitely generated projective C-module, M is a finitely generated projective C-module. By Proposition 5.1 in [1], $\mathrm{Hom}_C(M, M)$ is a central separable C-algebra. Since Λ is a central separable C-subalgebra of $\mathrm{Hom}_C(M, M)$, from Lemma 1 $\Omega = \mathrm{Hom}_\Lambda(M, M) = V_{\mathrm{Hom}_C(M,M)}(\Lambda)$ is a central separable C-algebra and $\mathrm{Hom}_\Omega(M, M) = V_{\mathrm{Hom}_C(M,M)}(\Omega) = V_{\mathrm{Hom}_C(M,M)}(V_{\mathrm{Hom}_C(M,M)}(\Lambda)) = \Lambda$. By Lemma 2 M is a finitely generated projective Ω-module, since Ω is a central separable C-algebra. If Λ is a separable R-algebra in general, then from Theorem 2.3 in [1] we have that Λ is a central separable C-algebra and C is a separable R-algebra where C is the center of Λ. Therefore $\Omega = \mathrm{Hom}_\Lambda(M, M)$ is a central separable C-algebra. Hence Ω is a separable R-algebra.

Corollary 1. *Let Λ be a separable R-algebra and M a Λ-module. If M is a finitely generated projective R-module then $\Omega = \mathrm{Hom}_\Lambda(M, M)$ is a separable R-algebra and M is finitely generated and projective over Ω.*

Proof. Since the image Λ' of the natural homomorphism $\Lambda \to \mathrm{Hom}_R(M, M)$ is also a separable R-algebra, M is a finitely generated projective Λ'-module by Lemma 2. Therefore $\Omega = \mathrm{Hom}_\Lambda(M, M) = \mathrm{Hom}_{\Lambda'}(M, M)$ is a separable R-algebra and M is a finitely generated projective Ω-module by Theorem 1.

Corollary 2. *If Λ is a separable R-algebra and e is an idempotent element in Λ, then $e\Lambda e$ is also a separable R-algebra.*

Proof. Since Λe is a projective Λ-left module, we have that $\mathrm{Hom}_\Lambda^l(\Lambda e, \Lambda e) \cong e\Lambda e$ is a separable R-algebra.

Theorem 2. *Let Λ be a central separable R-algebra. If Γ is an arbitrary separable R-subalgebra of Λ containing R, then $V_\Lambda(\Gamma)$ is a separable R-algebra and we have $V_\Lambda(V_\Lambda(\Gamma)) = \Gamma$.* (cf. [1], Theorem 3.3)

Proof Since Λ is a finitely generated projective R-module, $\Gamma \otimes_R \Lambda^0$

is a subring of $\Lambda^e=\Lambda\otimes_R\Lambda^0$. Since R is a direct summand of Λ as R-module, Λ and Λ^0 may be regarded as subring of $\Lambda\otimes_R\Lambda^0$. Then $\Lambda\otimes_R\Lambda^0=\Lambda\cdot\Lambda^0$ and $V_{\Lambda\otimes\Lambda^0}(\Lambda^0)=\Lambda$ ([1], Theorem 3.5). It follows that $V_{\Lambda\otimes\Lambda^0}(\Gamma\otimes_R\Lambda^0)=V_\Lambda(\Gamma)$. Now we consider $\Lambda\otimes_R\Lambda^0\supset\Gamma\otimes_R\Lambda^0\supset R$, and then $\Gamma\otimes_R\Lambda^0$ is a separable R-subalgebra of the central separable R-algebra $\Lambda\otimes_R\Lambda^0$ ([1], Proposition 1.5). Let $\Lambda^0=R\oplus\Lambda_1$ where Λ_1 is an R-submodule of Λ^0, then we have $\Lambda\otimes_R\Lambda^0=\Lambda\oplus\Lambda\otimes_R\Lambda_1$ and $\Gamma\otimes_R\Lambda^0=\Gamma\oplus\Lambda\otimes_R\Lambda_1$. Since $\Gamma\otimes_R\Lambda^0\subset\Lambda\otimes_R\Lambda^0$, $\Gamma\subset\Lambda$ and $\Gamma\otimes_R\Lambda_1\subset\Lambda\otimes_R\Lambda_1$, we have $(\Gamma\otimes_R\Lambda^0)\cap\Lambda=\Gamma$. Now $V_\Lambda(V_\Lambda(\Gamma))=V_{\Lambda\otimes_R\Lambda^0}(V_\Lambda(\Gamma)\otimes\Lambda^0)=V_{\Lambda\otimes\Lambda^0}(V_{\Lambda\otimes\Lambda^0}(\Gamma\otimes_R\Lambda^0))\cap V_{\Lambda\otimes\Lambda^0}(\Lambda^0)=V_{\Lambda\otimes\Lambda^0}(V_{\Lambda\otimes\Lambda^0}(\Gamma\otimes_R\Lambda^0))\cap\Lambda$, it is sufficient to show that $V_{\Lambda\otimes_R\Lambda^0}(\Gamma\otimes_R\Lambda^0)$ is a separable R-algebra and $V_{\Lambda\otimes_R\Lambda^0}(V_{\Lambda\otimes\Lambda^0}(\Gamma\otimes_R\Lambda^0))=\Gamma\otimes_R\Lambda^0$. Since $\Lambda\otimes_R\Lambda^0\cong\mathrm{Hom}_R(\Lambda,\Lambda)$ and Λ is a finitely generated projective R-module, we may show that if M is a finitely generated projective R-module, $\Lambda=\mathrm{Hom}_R(M,M)$, and Γ is a separable R-subalgebra of Λ, then $V_\Lambda(\Gamma)$ is a separable R-algebra and $V_\Lambda(V_\Lambda(\Gamma))=\Gamma$. Let S be the center of Γ. Then $\Lambda\supset\Gamma\supset S\supset R$. We regard M as S-module. Since S is R-separable, by Lemma 2 M is a finitely generated projective S-module, therefore $\mathrm{Hom}_S(M,M)$ is a central separable S-algebra. Then $V_\Lambda(\Gamma)=V_{\mathrm{Hom}_R(M,M)}(\Gamma)=\mathrm{Hom}_\Gamma(M,M)$. By Theorem 1 $V_\Lambda(\Gamma)$ is a separable R-algebra. Since S is the center of Γ, we have $\mathrm{Hom}_\Gamma(MM)=V_{\mathrm{Hom}_S(M,M)}(\Gamma)$. Since $\mathrm{Hom}_S(M,M)\supset\Gamma\supset S$, $\mathrm{Hom}_\Gamma(M,M)\supset S$, and $\mathrm{Hom}_S(M,M)$ and Γ are central separable S-algebra, we have by Lemma 1

$$V_\Lambda(V_\Lambda(\Gamma))=V_{\mathrm{Hom}_S(M,M)}(V_{\mathrm{Hom}_S(M,M)}(\Gamma))=\Gamma\,.$$

Corollary 3. *Let Λ be a central separable R-algebra and Γ an arbitrary separable R-subalgebra containing R. Then $\Gamma\cdot V_\Lambda(\Gamma)$ is a separable R-algebra and it is isomorphic to $\Gamma\otimes_S V_\Lambda(\Gamma)$ where S is the center of Γ. In particular, if $S=R$ then $\Lambda=\Gamma\cdot V_\Lambda(\Gamma)\cong\Gamma\otimes_R V_\Lambda(\Gamma)$* (cf. [1], Theorem 3.3).

Proof. By Theorem 1.4 $V_\Lambda(\Gamma)$ is a central separable S-algebra, therefore $\Gamma\otimes_S V_\Lambda(\Gamma)$ is a central separable S-algebra ([1], Proposition 1.5). In the homomorphism $\psi:\Gamma\otimes_S V_\Lambda(\Gamma)\to\Gamma\cdot V_\Lambda(\Gamma)$ defined by $\psi(x\otimes y)=x\cdot y$ for $x\in\Gamma$, $y\in V_\Lambda(\Gamma)$, the kernel of ψ is a two sided ideal of $\Gamma\otimes_S V_\Lambda(\Gamma)$. By Corollary 3.2 in [1] there exists an ideal $\mathfrak{a}$ of S such that $\ker\psi=\mathfrak{a}\cdot\Gamma\otimes V_\Lambda(\Gamma)$, but $0=\psi(\mathfrak{a})=\mathfrak{a}$, therefore ψ is an isomorphism. The case of $S=R$ was proved in [1], Theorem 3.3.

REMARK. In Theorem 2, the second part "$V_\Lambda(V_\Lambda(\Gamma))=\Gamma$" is proved in the following way too. Since Λ is a finitely generated projective R-module, and since Γ is a separable R-algebra, Λ is a finitely generated projective Γ-right (or left) module by Lemma 2, and $\mathfrak{B}=\mathrm{Hom}_\Gamma^r(\Lambda,\Lambda)$ is a separable R-algebra, and $\mathrm{Hom}_{\mathfrak{B}}(\Lambda,\Lambda)=\Gamma_r$, where Γ_r is the ring of right multiplications by the elements of Γ (Theorem 1). Hence Λ is, in the sense of Nakayama [5], $\mathfrak{B}$-Galois extension over Γ. Therefore Γ is a direct summand of Λ as Γ-right module by Proposition 1 in [5], and we have $V_\Lambda(V_\Lambda(\Gamma))=\Gamma$ by Theorem 3.5 in [4].

2. Galois extension

In this section we assume that Λ is any ring and Γ is a subring of Λ having the common identity. We define a Galois extension for the case of non-commutative rings similarly to the case of commutative rings in [1]. Let G be a finite group of (ring) automorphisms of Λ. We consider the crossed product $\Delta=\Delta(\Lambda, G)$ with trivial factor set, that is $\Delta=\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$, $u_\sigma\lambda=\sigma(\lambda)\cdot u_\sigma$, $u_\sigma\cdot u_\tau=u_{\sigma\tau}$ for σ, $\tau\in G$, $\lambda\in\Lambda$. Then we may assume that u_1 is the identity of Δ and Λ is a subring of Δ. The subring Γ consisting of all elements of Λ fixed by every element of G will be called the fixed subring of Λ under G. Then we shall say that Λ is a (right-) Galois extension of Γ relative to G if it satisfies the following condition: 1) Λ is a finitely generated projective Γ-right module, 2) the ring-homomorphism δ: $\Delta(\Lambda, G)\rightarrow\mathrm{Hom}^r_\Gamma(\Lambda, \Lambda)$ where $\mathrm{Hom}^r_\Gamma(\Lambda, \Lambda)$ is the Γ-endomorphism ring of Λ as Γ-right module, defined by $\delta(\lambda u_\sigma)(x)=\lambda\cdot\sigma(x)$, λ, $x\in\Lambda$, $\sigma\in G$, is an isomorphism.

REMARK. If Λ be an algebra over R, Γ is a separable R-subalgebra of Λ whose elements are left invariant by G, and if the condition 1) and 2) are satisfied, then it follows that Γ is the fixed subring of Λ under G from Theorem 1. In this case, Λ is a $\mathfrak{B}$-Galois over Γ, in the sense of Nakayama [5], where $\mathfrak{B}=\mathrm{Hom}^r_\Gamma(\Lambda, \Lambda)$.

We may regard Λ as a left Δ-module by setting $a\cdot\lambda=\delta(a)\cdot\lambda$. Then we have a similar proposition to Proposition A. 1 in [1].

Proposition 1. *Let Γ be a subring of a ring Λ, G a finite group of automorphisms of Λ. Then Λ is a Galois extension of Γ relative to G if and only if Γ is the fixed subring of Λ under G and $\mathfrak{T}_\Delta(\Lambda)=\Delta$ where $\mathfrak{T}_\Delta(\Lambda)$ is the trace ideal of Δ-module M.* (See [1] and [2].)

Proof. This is proved similarly to Proposition A. 1 in [1].

We regard the module $\mathrm{Hom}_\Delta(\Lambda, \Delta)$ as Γ-left module by setting $(\gamma\cdot f)(\lambda)=f(\lambda\cdot\gamma)$ for $f\in\mathrm{Hom}_\Delta(\Lambda, \Delta)$, $\gamma\in\Lambda$, $\lambda\in\Lambda$. Let κ be a homomorphism of $\mathrm{Hom}_\Delta(\Lambda, \Delta)$ into Δ defined by $\kappa(f)=f(1)$ for $f\in\mathrm{Hom}_\Delta(\Lambda, \Delta)$. Then we have

Lemma 3. *The homomorphism κ is a Γ-monomorphism, and the image of κ is $u\cdot\Lambda$ where $u=\sum_{\sigma\in G}u_\sigma$ in Δ.*

Proof. If $f \in \mathrm{Hom}_\Delta(\Lambda, \Delta)$, $\gamma \in \Gamma$, then $\kappa(\gamma\cdot f)=(\gamma\cdot f)(1)=f(\gamma)=\gamma\cdot f(1)=\gamma\cdot\kappa(f)$. Therefore κ is a Γ-monomorphism. We shall show that $\mathrm{Im}(\kappa)=u\cdot\Lambda$. Let f be any homomorphism of Λ into Δ without operator. Then f is a Δ-homomorphism if and only if $f(x)=x\cdot f(1)$ and $\sigma(x)\cdot f(1)=u_\sigma\cdot x\cdot f(1)$ for all $x\in\Lambda$, $\sigma\in G$. Therefore f is in $\mathrm{Hom}_\Delta(\Lambda, \Delta)$ if and only if there exists a in Δ such that $f(x)=x\cdot a$ and $a=u_\sigma a$ for all $x\in\Lambda$ and $\sigma\in G$. Now we set $a=\sum_{\sigma\in G}\lambda_\sigma u_\sigma$ where $\lambda_\sigma\in\Lambda$. Then a satisfies $u_\sigma a=a$ for all $\sigma\in G$ if and only if $\sigma(\lambda_\tau)=\lambda_{\sigma\tau}$ for all $\sigma, \tau\in G$. If in $\sigma(\lambda_\tau)=\lambda_{\sigma\tau}$ we put $\tau=1$ then we have $\sigma(\lambda_1)=\lambda_\sigma$. Conversely if we put $\lambda_\sigma=\sigma(\lambda_1)$ for every $\sigma\in G$ where λ_1 is an element of Λ, then we obtain $\lambda_{\sigma\tau}=\sigma\tau(\lambda_1)=\sigma(\tau(\lambda_1))=\sigma(\lambda_\tau)$ for all $\sigma, \tau\in G$. Consequently f is a Δ-homomorphism if and only if for every $x\in\Lambda$ it satisfies $f(x)=x\cdot a$ where $a=\sum_{\sigma\in G}\sigma(\lambda_1)u_\tau=\sum_{\sigma\in G}u_\sigma\lambda_1=u\cdot\lambda_1$ for any $\lambda_1\in\Lambda$. Therefore we have $\mathrm{Im}(\kappa)=u\Lambda$.

Proposition 2. *Let G be a finite group of automorphisms of Λ, and Γ the fixed subring of Λ under G. Then $\mathfrak{T}_\Delta(\Lambda)=\Delta$ if and only if $\Delta=\Lambda u\Lambda$.*

Proof. We have the homomorphism $\psi: \Lambda\otimes_\Gamma u\Lambda\to\Delta$ defined by $\psi(\lambda\otimes u\lambda')=\lambda u\lambda'$ for $\lambda, \lambda'\in\Lambda$. In the following commutative diagram

$$\begin{tikzcd}
\Lambda\otimes_\Gamma \mathrm{Hom}_\Delta(\Lambda, \Delta) \arrow[rr, "1\otimes\kappa"] \arrow[dr, "\tau"'] & & \Lambda\otimes_\Gamma u\Lambda \arrow[dl, "\psi"] \\
 & \Delta &
\end{tikzcd}$$

where τ is the trace mapping, $\tau(\lambda\otimes f)=f(\lambda)$, we have $\mathfrak{T}_\Delta(\Lambda)=\mathrm{Im}(\tau)=\mathrm{Im}(\psi\circ(1\otimes\kappa))=\Lambda u\Lambda$. Therefore we have that $\mathfrak{T}_\Delta(\Lambda)=\Delta$ if and only in $\Delta=\Lambda u\Lambda$.

Corollary 4. *Let G be finite group of automorphisms of Λ, and Γ a subring of Λ. Then Λ is a Galois extension of Γ relative to G if and only if Γ is the fixed subring of Λ under G and $\Delta(\Lambda, G)=\Lambda u\Lambda$.*

Theorem 3. *Let Λ be a Galois extension of Γ relative to G. If H is a subgroup of G and Ω is the fixed subring of Λ under H, then Λ is a Galois extension of Ω relative to H.*

Proof. Since Λ is a Galois extension of Γ relative to G, we have $\Delta=\Delta(\Lambda, G)=\Lambda u\Lambda$. Let $\Delta_H=\Delta(\Lambda, H)=\sum_{\tau\in H}\oplus\Lambda u_\tau$ be the crossed product of Λ and H. Then we may regard Δ_H as a subring of $\Delta=\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$. Now we shall show that $\Delta_H=\Delta(\Lambda, H)=\Lambda u_0\Lambda$ for $u_0=\sum_{\tau\in H}u_\tau$. Let

$G=\sigma_1 H+\sigma_2 H+\cdots+\sigma_r H$ be a left decomposition of G with respect to H where $\sigma_1=1$. Then it follows that $\Delta=\sum_{\sigma\in G}\oplus\Lambda u_\sigma=\sum_{i=1,\tau\in H}^{r}\oplus\Lambda u_{\sigma_i}u_\tau=\sum_{i=1}^{r}\oplus u_{\sigma_i}\sum_{\tau\in H}\Lambda u_\tau=\sum_{i=1}^{r}\oplus u_{\sigma_i}\Delta_H$ and $u=\sum_{\sigma\in G}u_\sigma=\sum_{i=1,\tau\in H}^{r}u_{\sigma_i}u_\tau=\sum_{i=1}^{r}u_{\sigma_i}u_0$. Since $\Delta=\Lambda u\Lambda$ we have $\Delta=\sum_{i=1}^{r}u_{\sigma_i}\Delta_H=\Lambda u\Lambda=\Lambda\sum_{i=1}^{r}u_{\sigma_i}u^0\Lambda\subset\sum_{i=1}^{r}u_{\sigma_i}(\Lambda u_0\Lambda)\subset\sum_{i=1}^{r}u_{\sigma_i}\Delta_H=\Delta$. Therefore $\sum_{i=1}^{r}\oplus u_{\sigma_i}\Delta_H=\sum_{i=1}^{r}\oplus u_{\sigma_i}\Lambda u_0\Lambda$. Since $u_{\sigma_i}\Lambda u_0\Lambda\subset u_{\sigma_i}\Delta_H$ for $i=1,2,\cdots,r$, it follows that $u_{\sigma_i}\Lambda u_0\Lambda=u_{\sigma_i}\Delta_H$. Consequently, we have $\Lambda u_0\Lambda=\Delta_H$. By Corollary 4 Λ is the Galois extension of Ω relative to H.

Proposition 3. *Let G be a finite group of automorphisms of Λ, and C the center of Λ. We suppose that the group of automorphisms of C induced by G is isomorphic to G. If for the fixed subring R of C under G, C is a Galois extenston of R relative to G, then Λ is a Galois extension of Γ relative to G where Γ is the fixed subring of Λ under G.*

Proof. We denote by $\Delta(C,G)=\sum_{\sigma\in G}\oplus Cu_\sigma$ the crossed product of C and G, and denote by $\Delta(\Lambda G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$ the crossed product of Λ and G. We may regard $\Delta(C,G)$ as a subring of $\Delta(\Lambda,G)$. By Corollary 4 we have $\Delta(C,G)=CuC$ for $u=\sum_{\sigma\in G}u_\sigma$, since C is a Galois extension of R relative to G. Therefore for every $\sigma\in G$, u_σ is contained in $CuC\subset\Lambda u\Lambda$. Therefore $\Lambda u_\sigma\subset\Lambda u\Lambda$ and $\Delta(\Lambda G)=\Lambda u\Lambda$. By Corollary 4 Λ is a Galois extension of Γ relative to G.

3. Separability of crossed product with trivial factor set

Proposition 4. *Let Λ be a Galois extension of Γ relative to G, C the center of Λ, and R the fixed subring of C under G. If Γ is a separable R-algebra, then $\Delta(\Lambda,G)$ and Λ are separable R-algebrar and the center of $\Delta(\Lambda,G)$ coincides with the center of Γ.*

Proof. If Γ is a separable R-algebra then by Theorem 1, $\mathrm{Hom}_\Gamma^r(\Lambda,\Lambda)$ is a separable R-algebra, since Λ is a finitely generated projective Γ-right module. Therefore $\Delta=\Delta(\Lambda,G)$ is a separable R-algebra, and Δ is a projective $\Delta^e=\Delta\otimes_R\Delta^0$-module where $\Delta^0=(\Delta(\Lambda,G))^0$ is the opposite ring of Δ. Since $\Delta(\Lambda,G)^0=\Delta(\Lambda^0,G)$, $\Delta=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$ is a direct summand of a Δ^e-free module as Δ^e-module, and $\Delta^e=\Delta\otimes_R\Delta^0=\sum_{\sigma,\tau\in G}\oplus\Lambda\otimes_R\Lambda^0\cdot u_\sigma\otimes u_\tau^0$ is a $\Lambda\otimes_R\Lambda^0$-free module. It follows that Λ is a direct summand of $\Lambda\otimes_R\Lambda^0$-free module as $\Lambda\otimes_R\Lambda^0$-module. Therefore Λ is a separable R-algebra. Since Γ is a separable R-algebra and Λ is a finitely generated projective Γ-

right module, we have $\mathrm{Hom}^l_\Delta(\Lambda, \Lambda)=\Gamma$ by Theorem 1. Therefore the center of $\Delta=\Delta(\Lambda, G)$ coincides with the center of Γ.

We now show that under the following assumption Λ is the Galois extension of the fixed subring Γ under G and the crossed product $\Delta(\Lambda, G)$ is separable over R.

($\sharp$) Λ is a central separable C-algebra, G is a finite group of automorphisms of Λ which induces a group of automorphisms of C isomorphic to G, and C is the Galois extension of R relative to G, where R is the fixed subring of C under G.

Remark. If C is a field then Λ and Γ are simple algebras and the assumption ($\sharp$) means that Λ is an outer-Galois extension of Γ.

Lemma 4. *Let R be a subring of a commutative ring C, G a finite group of automorphisms of C having the fixed ring R. We set $Tr(c)=\sum_{\sigma\in G}\sigma(c)$ for $c\in C$. If C is a Galois extension of R relative to G, there exists an element c in C such that $Tr(c)=1$.*

Proof. We consider two homomorphisms $\mu: C\otimes_R \mathrm{Hom}_R(C, R)\rightarrow \mathrm{Hom}_R(C, C)$ defined by $\mu(c\otimes f)(x)=f(x)\cdot c$ and $\tau: C\otimes_R \mathrm{Hom}_R(C, R)\rightarrow R$ defined by $\tau(c\otimes f)=f(c)$. Since C is a finitely generated projective R-module, μ and τ are isomorphisms ([2], Proposition A. 1 and A. 3). Regarding C as submodule of $\mathrm{Hom}_R(C, C)$, we denote by t the homomorphism $\tau\circ\mu^{-1}$ restricted on C. By Proposition A. 4 in [1] we have $\mathrm{Hom}_R(C, R)=t\circ C$. Since C is a finitely generated projective R-module there exists f in $\mathrm{Hom}_R(C, R)$ such that $f(C)=R$. Accordingly there exist a and b in C such that $f=t\circ a$ and $f(b)=1$. By Proposition A. 3 in [1], $t(x)=\sum_{\sigma\in G}\sigma(x)$ for $x\in C$. It follows that $1=f(b)=t\circ a(b)=t(ab)=\sum_{\sigma\in G} Tr(ab)$.

Theorem 4. *Under the assumption ($\sharp$), Λ is a Galois extension of Γ relative to G when Γ is the fixed subring of Λ under G, aud $\Delta(\Lambda, G)$ is a separable R-algebra.*

Proof. By Proposition 3, Λ is a Galois extension of Γ relative to G. For the opposite ring Λ^0 of Λ, G is regarded as a group of automophisms of Λ^0 by setting $\sigma(\lambda^0)=(\sigma(\lambda))^0$ for $\sigma\in G$ and $\lambda\in\Lambda$. We have a opposite correspondence between $\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$ and $\Delta^0=\Delta(\Lambda^0, G)=\sum_{\sigma\in G}\oplus\Lambda^0 v_\sigma$ defined by $\lambda u_\sigma\leftrightarrow(\lambda u_\sigma)^0=v_{\sigma^{-1}}\lambda^0$. In $\Lambda^e=\Lambda\otimes_R\Lambda^0$ and $\Delta^e=\Delta\otimes_R\Delta^0$ we set $J_1=\{\lambda\otimes 1^0-1\otimes\lambda^0\in\Lambda^e \mid \lambda\in\Lambda\}$, $J_2=R$-submodule of Δ^e generated by $\{u_\sigma\otimes 1^0-1\otimes v_{\sigma^{-1}}\in\Delta^e \mid \sigma\in G\}$, and $\boldsymbol{J}=\{\boldsymbol{x}\otimes 1^0-1\otimes\boldsymbol{x}^0\in\Delta^e \mid \boldsymbol{x}\in\Delta\}$. Then we have $\Delta^e\boldsymbol{J}=\Delta^e J_1+\Delta^e J_2$, because $\lambda u_\sigma\otimes 1^0-1\otimes(\lambda u_\sigma)^0=u_\sigma\sigma^{-1}(\lambda)\otimes 1^0-1\otimes v_{\sigma^{-1}}\lambda^0=u_\sigma\sigma^{-1}(\lambda)\otimes 1^0-u_\sigma\otimes\sigma^{-1}(\lambda)^0+u_\sigma\otimes\sigma^{-1}(\lambda^0)-1\otimes\sigma^{-1}(\lambda^0)u_{\sigma^{-1}}=u_\sigma\otimes 1^0\cdot(\sigma^{-1}(\lambda)\otimes 1^0-1$

$\otimes\sigma^{-1}(\lambda^0))+1\otimes\sigma^{-1}(\lambda^0)\cdot(u_\sigma\otimes 1^0-1\otimes v_{\sigma^{-1}})$. We denote by A the right annihilator of J_1 in Λ^e, and denote by $\boldsymbol{A}$ the right annihilator of $\boldsymbol{J}$ in Δ^e. We have easily $\boldsymbol{A}\subset\sum_{\sigma,\tau\in G}\oplus A\, u_\sigma\otimes v_\tau$. We define the automorphism $\sigma\times\tau$ of Λ^e by setting $\sigma\times\tau(x\otimes y^0)=\sigma(x)\otimes\tau(y^0)$ for every $\sigma\times\tau\in G\times G$ and $x\otimes y^0\in\Lambda^e$. For any element $f=\sum_{\sigma,\tau\in G}a(\sigma,\tau^{-1})u_\sigma\otimes v_{\tau^{-1}}$ in $\sum_{\sigma,\tau\in G}Au_\sigma\otimes v_{\tau^{-1}}$, $(a(\sigma,\tau^{-1})\in A)$, $f\in\boldsymbol{A}$ if and only if $(u_\gamma\otimes 1^0-1\otimes v_{\gamma^{-1}})\cdot f=0$ for all $r\in G$. Since $(u_\gamma\otimes 1^0-1\otimes v_{\gamma^{-1}})\cdot f=\sum_{\sigma,\tau\in G}\{\gamma\times 1(a)\gamma^{-1}\sigma,\tau^{-1}))-1\times\gamma^{-1}(a(\sigma,\gamma\tau^{-1}))\}u_\sigma\otimes v_{\tau^{-1}}$, we have that $f\in\boldsymbol{A}$ if and only if $\gamma\times\gamma(a(\gamma^{-1}\sigma,\tau^{-1}))=a(\sigma,\gamma\tau^{-1})$ for all $\sigma,\tau,\gamma\in G$. We set $\gamma^{-1}\sigma=\sigma_0$, $\tau^{-1}=\tau_0$, then $f\in\boldsymbol{A}$ if and only if $\gamma\times\gamma(a(\sigma_0,\tau_0))=a(\gamma\sigma_0,\gamma\tau_0)$ for all $\gamma,\sigma_0,\tau_0\in G$. We remark that $\gamma\times\gamma(A)=A$ for every $\gamma\in G$. If we set $\tau_0=1$ and $\gamma\cdot\sigma_0=\delta$, then we get $a(\delta,\gamma)=\gamma\times\gamma(a(\gamma^{-1}\delta,1))$ from the above. Therefore $\boldsymbol{A}$ contains every element f of the following form; $f=\sum_{\delta,\gamma\in G}\gamma\times\gamma(a(\gamma\delta^{-1},1))u_\delta\otimes v_\gamma$ where $a(\tau,1)\in A$ for $\tau\in G$. We set $a(\tau,1)=0$ if $\tau\neq 1$. Then we have that for any element a in A, $\sum_{\gamma\in G}\gamma\times\gamma(a)\cdot u_\gamma\otimes v_\gamma$ is contained in $\boldsymbol{A}$. We remark that $v_\gamma=(u_{\gamma^{-1}})^0$ and $\varphi(\gamma\times\gamma(a))=\gamma(\varphi(a))$ for the homomorphism $\varphi:\Lambda^e\to\Lambda$ defined by $\varphi(x\otimes y^0)=xy$. Then for the homomorphism $\boldsymbol{\varphi}:\Delta^e\to\Delta$ (defined by $\boldsymbol{\varphi}(\boldsymbol{x}\otimes\boldsymbol{y}^0)=\boldsymbol{x}\cdot\boldsymbol{y}$) we have $\boldsymbol{\varphi}(\sum_{\gamma\in G}\gamma\times\gamma(a)\cdot u_\gamma\otimes v_\gamma)=\boldsymbol{\varphi}(\sum_{\gamma\in G}\gamma\times\gamma(a)\cdot u_\gamma\otimes(u_{\gamma^{-1}})^0)=\sum_\gamma\varphi(\gamma\times\gamma(a))=\sum_\gamma\gamma(\varphi(a))=Tr(\varphi(a))$. Therefore $\boldsymbol{\varphi}(\boldsymbol{A})\supset Tr(\varphi(A))$. Since Λ is a central separable C-algebra and by Corollary A. 5 in [1] C is separable over R, therefore Λ is separable over R ([1], Theorem 2. 3). Accordingly, by Proposition 1. 1 in [1] $\varphi(A)=C$, and have $\boldsymbol{\varphi}(\boldsymbol{A})\supset Tr(C)$. On the other hand by Lemma 4 $Tr(C)$ contains the identity of R, therefore $\boldsymbol{\varphi}(\boldsymbol{A})\ni 1$ and Δ is a separable R-algebra.

Corollary 5. *Under the same assumption as in Theorem* 4, Γ *as a separable R-algebra.*

Proof. Since Λ is a finitely generated projective C-module and C is a finitely generated projective R-module, Λ is a finitely generated projective R-module ([3], IX Corollary 2. 5). If we regard Λ as $\Delta(\Lambda,G)$-left module, then Λ is a finitely generated projective $\Delta(\Lambda,G)$-module from Lemma 2 since Δ is a separable R-algebra. By Theorem 1 the $\Delta(\Lambda G)$-endomorphism ring $\mathrm{Hom}^l_\Delta(\Lambda,\Lambda)$ is a separable R-algebra. Since $\mathrm{Hom}^l_\Delta(\Lambda,\Lambda)\cong\Gamma$ we have that Γ is a separable R-algebra.

From Proposition 4 and the above proof we have

Corollary 6. *Let* Λ *be an R-algebra satisfying the same assumption* (♯) *except "*Λ *is a separable C-algebra". If* Λ *is a finitely generated projective R-module and* $\Delta(\Lambda,G)$ *is a* (*central*) *separable R-algebra, then* Γ

is also a (central) separable R-algebra.

4. Galois theory

In this section we shall consider a ring Λ satisfying the assumption ($\sharp$) in § 3.

Lemma 5. *Let Λ be a ring satisfying the assumption ($\sharp$) in § 3. Then $\Delta(\Lambda, G)$ and Γ are central separable R-algebra, where Γ is the fixed subring of Λ under G.*

Proof. From Theorem 4 and Corollary 5, $\Delta(\Lambda, G))$ and Γ are separable R-algebra, and by Proposition 3 Λ is a Galois extension of Γ relative to G. By Proposition 4 the center of $\Delta(\Lambda, G)$ coinsides with the center of Γ. We shall show that the center of $\Delta(\Lambda, G)$ in R. We denote by S the center of Γ (=the center of $\Delta(\Lambda, G)$). We have $R=\{c\in C|\sigma(c)=c$ for all $\sigma\in G\}=C\cap\{\lambda\in\Lambda|\tau(\lambda)=\lambda$ for all $\sigma\in G\}=C\cap\Gamma$. Since the center of Γ is contained in the center of Λ, we have $S\subset C\cap\Gamma=R$. On the other hand R is contained in the center of Δ, we have $R=S$.

Proposition 5. *Let C be a commutative ring, and let C be a Galois extension of R relative to G. If S is an intermediate ring between C and R such that C is a Galois extension of S relative to a subgroup H of G, then S is a separable R-algebra.*

Proof. Since C is a Galois extension of R, C is a separable R-algebra, therefore C is a projective $C\otimes_R C$-module, and C is a finitely generated projective S-module since C is a Galois extension of S. It follows that $C\otimes_R C$ is a projective $S\otimes_R S$-module ([3], IX Proposition 2. 3), and S is a direct summand of C as two sided S-module, therefore S is a separable R-algebra.

Proposition 6. *Let C be a commutative integral domain, and let C be a Galois extension of R relative to G. If S is an intermediate ring betweeen C and R such that S is a separable R-algebra, then C is a Galois extension of S relative to a subgroup H of G where $H=\{\sigma\in G|\sigma(x)=x$ for all $x\in S\}$, and C is a separable S-algebra.*

Proof. Since C is a finitely generated projective R-module and S is a separable R-algebra, from Lemma 2 C is a finitely generated projective S-module. We set $T=\mathrm{Hom}_S(C, C)$. From Proposition A. 2 and A. 3 in [2] we have $\mathrm{Hom}_T(C, C)=S$. Since $\mathrm{Hom}_R(C, C)\cong\Delta(C, G)=\sum_{\sigma\in G}Cu_\sigma$, $T=V_{\mathrm{Hom}_R(C,C)}(S)=V_{\Delta(C,G)}(S)$. Now we shall show that $V_{\Delta(C,G)}(S)$ is a crossed product $\Delta(C, H)=\sum_{\tau\in\mathcal{A}} Cu_\tau$ of C and H where $H=\{\sigma\in G\,|\,\sigma(x)=x$ for all $x\in S\}$. If $\sum_\sigma a_\sigma u_\sigma$ is an arbitrary element in $V_{\Delta(C,G)}(S)$, then we have $a_\sigma\cdot\sigma(x)=a_\sigma\cdot x$ for all $x\in S$ and $\tau\in G$. Since C is an integral domain, for every x in S, $a_\sigma(\sigma(x)-x)=0$ implies $a_\sigma=0$ or $x=\sigma(x)$. Therefore, if σ is not contained in H then $a_\sigma=0$. Consequently, $\sum_\sigma a_\sigma v_\sigma$ is contained in $\sum_{\tau\in\mathcal{A}} Cu_\tau=\Delta(C,H)$. Since $\Delta(C,H)\subset V_{\Delta(C,G)}(S)=T$, we have $T=\Delta(CH)$. Since $S=\mathrm{Hom}_T(C,C)$, S is the fixed subring of C under H. By Theorem 3 C is a Galois extension of S relative to H, and by Corollary A. 5 in [1] C is a separable S-algebra.

Lemma 6. *Let C be a commutative ring, M a projective C-module, and m a non zero elemen in M. If $cm=0$ for an element c in C, then there exists a non zero element c' in C such that $c\cdot c'=0$ and c' is independent of c.*

Proof. If M is a projective C-module then it can be imbedded in a free C-module $F=\sum_i\oplus Cv_i$. Then we have $m=\sum_{i=1}^r c_iv_i$ for $m\neq 0$ in M. If $cm=\sum_i cc_iv_i=0$ then we have $cc_i=0$ where c_i is independent of c.

Theorem 5. *Let Λ be a central separable algebra over a commutative ring C, and let G be a finite group of automorphisms of Λ such that G induce the group of automorphisms of C isomorphic to G and for the fixed subring R of C under G C is a Galois extension of R relative to G. Then we have*

1) *if Γ is the fixed subring of Λ under G then Λ is a galois extension of Γ and Γ is a central separable algebra over R,*

2) *Γ is a direct summand of Λ as Γ-two sided module,*

3) *for an arbitrary subgroup H of G, the fixed subring Ω of Λ under H is a separable R-subalgebra of Λ containing Γ, and Λ is a Galois extension of Ω relative to H.*

Furthermore if we suppose that C is an integral domain, then we have

4) *if Ω is an arbitrary intermediate ring between Λ and Γ such that Ω is a separable R-algebra, then Λ is a Galois extension of Ω relative to H where $H=\{\sigma\in G\,|\,\sigma(x)=x$ for all $x\in\Omega\}$.*

Proof. 1). We have proved it above, but we may prove it also as follows. By Lemma 5 $\Delta=\Delta(\Lambda, G)$ is a central separable R-algebra and $\Delta_0=\Delta(C,G)$ is so. From Theorem 2 the commutor ring $V_\Delta(\Delta_0)$ of a separable R-subalgebra Δ_0 in a central separable R-algebra Δ is a separable R-algebra. On the other hand we have $V_\Delta(\Delta_0)=\Gamma$. Because, if $\sum_\sigma \lambda_\sigma u_\sigma$ is an arbitrary element in $V_\Delta(\Delta_0)$, then $\sum_\sigma \lambda_\sigma x u_\sigma = \sum_\sigma \lambda_\sigma \cdot \sigma(x) u_\sigma$ for all $x \in C$, therefore $\lambda_\sigma(x-\sigma(x))=0$ for all $x \in C$. Since Λ is a projective C-module, if $\lambda_\sigma \neq 0$ then by Lemma 6 there exists a non zero element c in C such that $c(x-\sigma(x))=0$ for all x in C. If $\sigma \neq 1$, then u_σ and 1 are linearly independent over C in $\Delta(C, G)$, therefore in $\mathrm{Hom}_R(C, C)$, σ and 1 are so. It follows that $\lambda_\sigma=0$ for $\sigma \neq 1$. Thus we have $V_\Delta(\Delta) \subset \Lambda$. Therefore we have that $V_\Delta(\Delta_0)$ is the fixed subring Γ of Λ under G. Since the center of $\Delta(\Lambda, G)$ is R, by Proposition 4 Γ is a central separable R-algebra, and $V_\Delta(\Gamma)=\Delta_0$ from Theorem 2.

2). Since $V_\Delta(\Delta_0)=\Gamma$ and Δ_0 is a central separable R-subalgebra of Δ, we have $\Delta=\Delta_0 \cdot \Gamma \cong \Delta_0 \otimes_R \Gamma$ from Corollary 3. Since C is a finitely generated projective R-module, R is a direct summand of C as R-module, and R is a direct summand of $\Delta_0=\Delta(C, G)$ as R-module. Therefore $\Gamma=R \otimes_R \Gamma$ is a direct summand of $\Delta \cong \Delta_0 \otimes_R \Gamma$ as two sided Γ-module. Since $\Delta \supset \Lambda \supset \Gamma$ we have that Γ is a direct summand of Λ as two sided Γ-module.

3). From Theorem 3 Λ is a Galois extension of Ω relative to H. We denote by S the fixed subring of C under H. Then C is a Galois extension of S relative to H, and from 1) Ω is a central separable S-algebra. Since S is a separable R-algebra by Proposition 5, Ω is a separable R-algebra by Theorem 2.3 in [1].

4). We suppose that Ω is an intermediate separable R-algebra between Λ and Γ. Since $\Delta=\Delta(\Lambda, G)$ is a central separable R-algebra and Ω is a separable R-subalgebra of Δ. We have $V_\Delta(V_\Delta(\Omega))=\Omega$, and $V_\Delta(\Omega)$ is a separable R-algebra. On the other hand $V_\Delta(\Lambda)=C$ and $V_\Delta(\Gamma)=\Delta_0=\Delta(C, G)$. Set $T=V_\Delta(\Omega)$, so that $R \subset C \subset T \subset \Delta_0$. Since Δ_0 is a central separable R-algebra and T is a separable R-subalgebra of Δ_0, $V_{\Delta_0}(T)$ is a separable R-algebra and $V_{\Delta_0}(V_{\Delta_0}(T))=T$. We set $S=V_{\Delta_0}(T)$. We have $V_{\Delta_0}(C)=C$, $V_{\Delta_0}(\Delta_0)=R$, and $R \supset S \supset C$. Since C is a Galois extension of R relative to G, by Proposition 6 C is a Galois extension of S relative to H where $H=\{\sigma \in G \mid \sigma((x)=x \text{ for all } x \in S\}$. Therefore $\Delta(C, H) \cong \mathrm{Hom}_S(C, C)$. Regarding $\Delta(C, H)=\mathrm{Hom}_S(C, C)$, we have $T=V_{\Delta_0}(S)=V_{\mathrm{Hom}_R(C,C)}(S)=\mathrm{Hom}_S(C, C)=\Delta(C, H)$, and $V_\Delta(\Omega)=T=\Delta(C, H)$. Since $\Omega=V_\Delta(T)$, Ω is the fixed subring of Λ under H. Therefore, from Theorem 3 we have that Λ is the Galois extension of Ω relative to a subgroup H of G.

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] ——————: *Maximal order*, Trans. Amer. Math. Soc. **97** (1960) 1–24.

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

[4] A. Hattori: *Semisimple algebra over a commutative ring*, J. Math. Soc. Japan **15** (1963), 404–419.

[5] T. Nakayama: *On a generalized notion of Galois extension of a ring*, Osaka Math. J. **15** (1963), 11–23.