Kanzaki, T.
Osaka J. Math.
3 (1966), 1-6

A NOTE ON ABELIAN GALOIS ALGEBRA OVER A COMMUTATIVE RING

TERUO KANZAKI

(Received September 6, 1965)

Let Λ be a faithful algebra over a commutative ring R with unit element 1, and G a finite group of R-algebra automorphisms of Λ. In the following we shall identify $R\cdot 1$ with R. We shall call Λ a (central, abelian) Galois algebra over R with group G, if Λ is a galois extension of (the center) R relative to (abelian) group G in the sense of [1], [7] and [8]. In [3], Chase, Harrison and Rosenberg proved the nomal basis theorem for a commutative Galois algebra overa semi-local ring, and in [5], De Meyer proved it for a central abelian Galois algebra Λ over its center with group of inner automorphisms of Λ. In this note, in §1, we shall prove the nomal basis theorem for any abelian Galois algebra over a semi-local ring. Furtheremore, we show that if the normal basis theorem holds for an R-algebra Λ with a finite abelian group G of R-algebra automorphisms of Λ, and if Λ is a strongly separable algebra (see [9]) then Λ is a Galois algebra over R with G. In §2 and §3, we shall show some properties an abelian Galois algebra over an indecomposable commutative ring. Throughout this note, we assume that every fing has a unit element.

1. Normal basis. Let Λ be an algebra over a commutative ring, and G a finite abelian group of R-algebra automorphisms of Λ.

Theorem 1. *Let R be a local ring, and Λ an abelian Galois algebra over R with abelian group G. Then Λ is isomorphic to the group ring RG of group G over ring R as RG-module.*

Proof. Since R is local and G is abelian, by [10], Λ is a Galois extension of the center C with the subgroup H and the center C is a Galois extension of R with group G/H, where $H=\{\sigma\in G:\sigma\,|\,C=\text{identity}\}$. Therefore, $\Lambda\otimes_R C$ is a Galois extension of the center $C\otimes_R C$ with group H and $C\otimes_R C$ is a Galois extension of $R\otimes_R C=C$ with group G/H. Let $\{\sigma_1=1, \sigma_2, \cdots, \sigma_r\}$ be a representative system of the residue class group

G/H. By [3], $C\otimes_R C=\sum_{i=1}^{r}\oplus Ce_{\sigma_i}=\sum_{i=1}^{r}\oplus C\sigma_i(e_1)$, where $e_1, e_{\sigma_2}, \cdots, e_{\sigma_r}$ are orthogonal idempotent elements in $C\otimes_R C$ and $\sum_{i=1}^{r} e_{\sigma_i}=1$, and hence $\Lambda\otimes_R C=\sum_{i=1}^{r}\oplus(\Lambda\otimes_R C)\sigma_i(e_1)=\sum_{i=1}^{r}\oplus\sigma_i(\Lambda\otimes_R C)e_1)$. On the other hand, $(\Lambda\otimes_R C)e_1$ is a central Galois extension of $Ce_1=(C\otimes_R C)e_1$ with group H. Since C is semi-local, by Lemma 1 in [10], H is a group of inner automorphisms of $(\Lambda\otimes_R C)e_1$. By [5], there is an element ϑ in $(\Lambda\otimes_R C)e_1$ such that $(\Lambda\otimes_R C)e_1=\sum_{\tau\in H}\oplus C\tau(\vartheta)$. Therefore, we have

$$\Lambda\otimes_R C = \sum_{i=1}^{r}\oplus\sigma_i((\Lambda\otimes_R C)e_1) = \sum_{i=1,\tau\in H}^{r}\oplus C\sigma_i\tau(\vartheta) = \sum_{\tau\in G}\oplus C\sigma(\vartheta).$$

Hemce $\Lambda\otimes_R C$ is isomorphic to the group ring CG of group G over ring C as CG-module. Since C is a finite rank R-free module, CG is a finitely generated RG-projective module and $\Lambda\otimes_R C$ is a finitely generated RG-projectine module. Since R is a direct summund of C as R-module, Λ is a finitely generated projective RG-module. For the remainder of the proof, we proceed similarly to the proof of Theorem 4.2 in [3]. For the maximal ideal $\mathfrak{m}$ of R, we have $\Lambda\otimes_R C/\mathfrak{m}C\cong RG\otimes_R R/\mathfrak{m}C$. Using the Krull-Schmidt Theorem, we obtain $\Lambda/\mathfrak{m}\Lambda\cong R/\mathfrak{m}G$ as $R/\mathfrak{m}$ G-module. Since mRG is a radical ideal of the group ring RG, and Λ is a RG-projective module, by Lemma 3.14 in [11] Λ and RG are isomorphic RG-modules.

Corolary 1. *Let Λ be an abelian Galois algebra over R with abelian group G. Then Λ is a finitely generated rank 1 RG-projective module, and therefore Λ is a rank $|G|$ R-projective module ($|G|$ denotes tne order of G).*

Proof. Since RG is a commutative ring, for any prime ideal P of RG

$$\Lambda\otimes_{RG}(RG)_P = (\Lambda\otimes_R R_p)\otimes_{R_pG}(RG)_P$$

where $p=R\cap P$. By Theorem 1, $\Lambda\otimes_P R_p\cong R_pG$ as R_pG-module, hence $\Lambda\otimes_{RG}(RG)_p\cong(RG)_p$ as $(RG)_p$-module. Therefore, by p. 138, Theorem 1 in [2], Λ is an RG-projective module with rank 1.

Corollary 2. *Let R be a semi-local ring, Λ an abelian Galois algebra over R with aberian group G. Then Λ is isomorphic to RG as RG-module.*

Proof. By Corollary 1, Λ is a finitely generated rank 1 RG-projective module. If R is a semi-local ring, then RG is also semi-local, therefore by p. 143, Proposition 5 in [2], Λ is RG-free module with rank 1.

Therem 2. *Let Λ be an algebra over a commutative ring R with* *unit element, and G a finite abelian group of R-algebra automorphisms of Λ. If Λ is isomorphic to the group ring RG as RC-module, and if Λ is a strongly separable algebra over R (see [9]), then Λ is a Galois algebra over R with group G.*

Before proving the Theorem, we prove the following lemma.

Lemma 1. *Let Λ be an algebra over R, and G a finite group of R-algebra automorphisms of Λ. If Λ is strongly separable over R and $Tr(\Lambda)\ni 1$, where $Tr(x) = \sum_{\sigma\in G}\sigma(x)$ for $x\in\Lambda$, then a crossed product $\Delta(\Lambda, G)$ of Λ and G with trivial factor set is separable over R.*

Prof. Let $\Delta(\Lambda, G)=\sum_{\sigma\in G}\oplus\Lambda u_\sigma$, $u_\sigma u_\tau=u_{\sigma\tau}$, and $u_\sigma\lambda=\sigma(\lambda)u_\sigma$ for $\lambda\in\Lambda$. We set $\boldsymbol{A}$=right annihilator of ker φ in $\Delta(\Lambda, G)^e=\Delta(\Lambda,G)\otimes_R(\Delta(\Lambda, G))^0$, where $\varphi:\Delta(\Lambda, G)\otimes_R(\Delta(\Lambda, G))^0\to\Delta(\Lambda, G)$ is defined by $\varphi(x\otimes y)=xy$, and set A=right annihilator of ker φ in $\Lambda^e=\Lambda\otimes_R\Lambda^0$, where $\varphi:\Lambda\otimes_R\Lambda^0\to\Lambda$ is defined by $\varphi(x\otimes y)=xy$. From the proof of Theorem 4 in [7], it follows that $\boldsymbol{A}$ contains the elements $\sum_{\gamma\in G}\gamma\times\gamma(a)u_\gamma\otimes u^0_{\gamma^{-1}}$ in $\Delta(\Lambda, G)^e$ for every a in A. Therefore, $\varphi(\sum\gamma\times\gamma(a)\,u_\gamma\otimes u^0_{\gamma^{-1}})=Tr\,(\varphi(a))$ is contained in $\varphi(\boldsymbol{A})$. Since Λ is strongly separable over R, Λ is separable over R and $\Lambda=C\oplus[\Lambda, \Lambda]$. Thus $\varphi(\boldsymbol{A})\supset Tr(\varphi(A))=Tr(C)$. Since $Tr(\Lambda)\ni 1$, there exists $a=c+b$ in $\Lambda=C\oplus[\Lambda, \Lambda]$ such that $Tr(a)=Tr(c)+Tr(b)=1$, $c\in C$, $b\in[\Lambda, \Lambda]$, therefore $Tr(C)\ni Tr(c)=1$. Accordingly, $\varphi(\boldsymbol{A})\ni 1$, $\Delta(\Lambda, G)$ is separable over R.

We have easily the following lemma.

Lemma 2. *Let Λ be a faithful algebra over R, G a finite abelian group of R-algebra automorphisms of Λ, and let $\Lambda^G=R$. Then an element $\sum_{\sigma\in G}\lambda_\sigma u_\sigma$ of the crossed product $\Delta(\Lambda, G)$ is contained in its center if and only if λ_σ is in R for ever $\sigma\in G$ and satisfies $\lambda_\sigma\sigma(\lambda)=\lambda\lambda_\sigma$ for every $\lambda\in\Lambda$ and $\sigma\in G$.*

Proof of Theorem 2. We suppose $\Lambda=\sum_{\sigma\in G}\oplus R\sigma(\vartheta)$ for some element ϑ in Λ. We have easily $\Lambda^G=RTr(\vartheta)=Tr(\Lambda)$. Since Λ^G is a ring and contains R, $Tr(\vartheta)$ is contained in R, therefore $\Lambda^G=Tr(\Lambda)=R$. By Lemma 1, the crossed product $\Delta(\Lambda, G)$ is separable over R, and by Lemma 2, the center of $\Delta(\Lambda, G)$ is R. Because, if $\sum_{\sigma\in G}\lambda_\sigma u_\sigma$ is any element of the center of $\Delta(\Lambda, G)$, tnen $\lambda_\sigma\in R$ and $\lambda_\sigma\sigma(\vartheta)=\lambda_\sigma\vartheta$ for every $\sigma\in G$, hence $\lambda_\sigma=0$ for $\sigma\neq 1$. Therefore, $\Delta(\Lambda, G)$ is a central separable algebra over

R. Now, we consider the natural homomorphism $\delta: \Delta(\Lambda, G) \to \mathrm{Hom}_R(\Lambda, \Lambda)$. By [1], $\mathrm{Hom}_R(\Lambda, \Lambda)$ and $\mathrm{Im}\,\delta$ are central separable algebras over R. Since the commutor ring $V_{\mathrm{Hom}_R(\Lambda, \Lambda)}(\mathrm{Im}\,\delta)$ of $\mathrm{Im}\,\delta$ in $\mathrm{Hom}_R(\Lambda, \Lambda)$ is R, by Lemma 2.3 in [4], δ is an isomorphism. Therefore, Λ is a Galois extension of R with group G.

REMARK. By Proposition 8 in [10], an abelian Galoif algebra Λ over any commutative ring R with abelian group G is strongly separable over R. Therefore if R is a semi-local ring, then Λ is a Galois algebra over R with aberian group G if and only if Λ is a strongly separable algebra and a Galois algebra over R with abelian group G in the sense of Hasse [6] or Wolf [13].

2. Splitting ring. In this section, we shall show that an abelian Galois algebra over a local ring has a splitting ring.

Theorem 3. *Let Λ be an abelian Galois algebra over a commutative ring R with abelian grou G. If R is indecomposable, then there exist a maximal commutative subalgebra S of Λ and a subgroup G_1 of G such that $\Lambda^{G_1}=S$. Therefore, S is a commutative Galois extension of R with group G/G_1 and Λ is a finitely generated projective S-module. Thus, if C is the center of Λ then central separable algebra Λ over C is split by S in the sense of [1]. In particular, if R is a local ring, then $\Lambda\otimes_R R$ is isomorphic to the full matrix ring of degree $|G_1|$ over the commutative ring $C\otimes_R S=\sum_{\bar\sigma\in G/H}\oplus Se_{\bar\sigma}$ where $H=\{\sigma\in G:\sigma|C=identity\}$, $\{e_{\bar\sigma}:\bar\sigma\in G/H\}$ are orthogonal idempotent elements and $\sum_{\bar\sigma\in G/H} e_{\bar\sigma}=1$.*

Proof. For the first part, we prove by the induction on the order $|G|$. If $|G|$ is prime, then by [5], Λ is commutative, i.e. $\Lambda=S$. We suppose Λ is non-commutative. Since R is indecomposable, by [10], Λ is a Galois extension of the center C with group H, and $\Lambda=\sum_{\sigma\in H}\oplus J_\sigma$, $J_\sigma=\{a\in\Lambda:\sigma(x)a=ax \text{ for all } x\in\Lambda\}$. By [5], we may assume that H is not cyclic. For an element σ in H, we denote the σ-fixed subring of Λ by $\Lambda^{(\sigma)}$, then the commutor ring $V_\Lambda(\Lambda^{(\sigma)})=\sum_i\oplus J_{\sigma^i}$ is the center of Λ (cf. [10]). Since $\Lambda^{(\sigma)}$ is a Galois extension of R with group $G/(\sigma)$, using the inductive assumption on roder $|G/(\sigma)|$, there exist a maximal commutative subalgebra S of Λ and a subgroup $\bar G_1=G_1/(\sigma)$ of $G/(\sigma)$ such that $(\Lambda^{(\sigma)})^{G_1}=\Lambda^{G_1}=S$. But $\Lambda^{(\sigma)}\supset S\supset V_\Lambda(\Lambda^{(\sigma)})$, hence $V_\Lambda(S)\subset(\Lambda^{(\sigma)})$, therefore $V_\Lambda(S)=S$. Accordingly, S is a maximal commutative subalgebra of Λ. Since S is a Galois extension of R with group G/G_1, S is separable over

R, therefore Λ is a finitely generated projective S-module (see [7]). By Proposition 2.4 in [4], central separable algebra Λ over C is split by S. Thus we have the first part. For the last part, we assume R is local. Then S is a semi-local ring and by §5, Proposition 5 in [2], Λ is a S-free module with rank $|G_1|=m$. By Proposition 2.4 in [4], $\Lambda\otimes_C S=\mathrm{Hom}_S(\Lambda, \Lambda)=(S)_m$. On the other hand, by [3], $C\otimes_R C=\sum_{\bar\sigma\in G/H}\oplus Ce_{\bar\sigma}$, and therefore

$$\begin{aligned}\Lambda\otimes_R S &= (\Lambda\otimes_C S)\otimes_C(C\otimes_R C) = (S)_m\otimes_C(C\otimes_R C) = (S)_m\otimes_S(S\otimes_R C)\\ &= (\sum_{\bar\sigma\in G/H}\oplus Se_{\bar\sigma})_m .\end{aligned}$$

3. Central Galois extenlsion

Lemma 3. *Let C be any commutative ring, and G a finite group such that the order $|G|$ is unit in C. Then for any CG-module M, $M^G=\{x\in M: \sigma x=x$ for all $\sigma\in G\}$ is a direct summund of M as C-module.*

Proof. $Tr'(x)=\frac{1}{|G|}\sum_{\sigma\in G}\sigma(x)$ for $x\in M$. Then $Tr'; M\to M^G$ is a C-epimorphism, and $Tr'|M^G=$identity, therefore, M^G is a direct summund of M as C-module.

Theorem 4. *Let Λ be a central abelian Galois extension of the center C with abelian group G, and C an indecomposable ring. Then*

1) *for every subgroup H of G, there exists a subgroup H' of G such that $\Lambda^H=\sum_{\sigma\in H'}\oplus J_\sigma$,*

2) *if $\Lambda^H=\sum_{\sigma\in H'}\oplus J_\sigma$* then *then* $\Lambda^H=V_\Lambda(\Lambda^{H'})$ and *and* $\Lambda^{H'}=V_\Lambda(\Lambda^H)$.

Proof. By [10], $\Lambda=\sum_{\sigma\in G}\oplus J_\sigma$ and $|G|$ is unit in C. Since $\sigma(J_\tau)=J_{\sigma\tau\sigma^{-1}}=J_\sigma$ (see [10], J_τ is CG-module. For any subgroup H of G, by Lemma 3, J_τ^H is a finitely generated projective C-module. Since C is indecomposable, for every maximal ideal p of C, rank of $J_\tau^H\otimes_C C_p$ over C_p is constant (see p. 138, Theorem 1 in [2]), hence $J_\tau^H\otimes_C C_p\neq 0$ for every maximal ideal p of C if $J_\tau^H\neq 0$. Since J_τ is a rank 1 projective C-module (see [12]), we have $J_\tau^H\otimes_C C_p=J_\tau\otimes_C C_p$ for every maximal ideal p of C if $J_\tau^H\neq 0$. Therefore, we have either $J_\tau^H=0$ or $J_\tau^H=J_\tau$ for each $\tau\in G$. Accordingly, $\Lambda^H=\sum_{\sigma\in G}\oplus J_\tau^H=\sum_{\tau\in H'}\oplus J_\tau$, where $H'=\{\tau\in G: J_\tau^H=J_\tau\}$. Since Λ^H is a subring, by [10], H' is a subgroup of G. Since $\Lambda^{H'}$ is separable over C, $T_\Lambda(\Lambda^{H'})=\sum_{\tau\in H'}\oplus J_\tau=\Lambda^H$ is separable over C, and $V_\Lambda(V_\Lambda(\Lambda^{H'}))=\Lambda^{H'}$ (see [7]). Therefore, $V_\Lambda(\Lambda^H)=\Lambda^{H'}$ and $V_\Lambda(\Lambda^{H'})=\Lambda^H$.

OSAKA GAKUGEI DAIGAKU

References

[1] M. Auslander and O. Goldman : *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960) 1–24.

[2] N. Bourbaki : Algebre commutative, Chap. I–II, 1964.

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

[4] S. U. Chase and A. Rosenberg : *Amitsur cohomology and the Brauer group*, Memoirs Amer. Math. Soc. 52 (1965).

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

[6] H. Hasse : *Invariant Kennzeichnung galoissche Körper mit vorgegebener Galois Gruppe*, J. reine angew. Math. **187** (1950) 14–43.

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

[8] ———— : *On Galois extension of rings*, Nagoya Math. J. **27** (1966), 43–49.

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

[10] ———— : *On Galois algebra over a commutative ring*, Osaka J. Math. **2** (1965) 309–317.

[11] A. Rosenberg and D. Zelinsky : *On Amitsur complex*, Trans. Amer. Math. Soc. **97** (1960) 327–356.

[12] ———————— : *Automorphisms of separable algebras*, Pacific. J. Math. **11** (1961) 1109–1129.

[13] P. Wolf : Algebraische Theorie der galoisschen Algebren, Berlin, 1965.