A note on abelian Galois algebra over a commutative ring

Kanzaki, Teruo

Osaka Journal of Mathematics. 3(1) P.1-P.6

1966

publisher

https://doi.org/10.18910/6309

10.18910/6309

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/repo/ouka/all/
A NOTE ON ABELIAN GALOIS ALGEBRA OVER A COMMUTATIVE RING

TERUO KANZAKI

(Received September 6, 1965)

Let $\Lambda$ be a faithful algebra over a commutative ring $R$ with unit element 1, and $G$ a finite group of $R$-algebra automorphisms of $\Lambda$. In the following we shall identify $R \cdot 1$ with $R$. We shall call $\Lambda$ a (central, abelian) Galois algebra over $R$ with group $G$, if $\Lambda$ 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 normal basis theorem for a commutative Galois algebra over a semi-local ring, and in [5], De Meyer proved it for a central abelian Galois algebra $\Lambda$ over its center with group of inner automorphisms of $\Lambda$. In this note, in §1, we shall prove the normal basis theorem for any abelian Galois algebra over a semi-local ring. Furthermore, we show that if the normal basis theorem holds for an $R$-algebra $\Lambda$ with a finite abelian group $G$ of $R$-algebra automorphisms of $\Lambda$, and if $\Lambda$ is a strongly separable algebra (see [9]) then $\Lambda$ 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 ring has a unit element.

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

Theorem 1. Let $R$ be a local ring, and $\Lambda$ an abelian Galois algebra over $R$ with abelian group $G$. Then $\Lambda$ 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], $\Lambda$ 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 $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_r\}$ be a representative system of the residue class group
By [3], \( C \otimes_R C = \sum_{i=1}^{r} \bigoplus C e_i = \sum_{i=1}^{r} C \sigma_i(e_i) \), where \( e_1, e_2, \ldots, e_r \) are orthogonal idempotent elements in \( C \otimes_R C \) and \( \sum e_i = 1 \), and hence \( \Lambda \otimes_R C = \sum_{i=1}^{r} \bigoplus (\Lambda \otimes_R C) \sigma_i(e_i) = \sum_{i=1}^{r} \sigma_i (\Lambda \otimes_R C) e_i \). On the other hand, \( (\Lambda \otimes_R C) e_i \) is a central Galois extension of \( C e_i \) with group \( H \). Since \( C \) is semi-local, by Lemma 1 in [10], \( H \) is a group of inner automorphisms of \( (\Lambda \otimes_R C) e_i \). By [5], there is an element \( \theta \) in \( (\Lambda \otimes_R C) e_i \) such that \( (\Lambda \otimes_R C) e_i = \sum_{\theta \in H} C \tau(\theta) \). Therefore, we have

\[
\Lambda \otimes_R C = \sum_{i=1}^{r} \bigoplus \sigma_i (\Lambda \otimes_R C) e_i = \sum_{i=1}^{r} \bigoplus C \sigma_i(\theta) = \sum_{\theta \in H} C \sigma(\theta).
\]

Hence \( \Lambda \otimes_R C \) is isomorphic to the group ring \( C[G] \) 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 \( RG \)-projective module. Since \( R \) is a direct summand of \( C \) as \( R \)-module, \( \Lambda \) 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 \( m \) of \( R \), we have \( \Lambda \otimes_R C/mC \cong RG \otimes_R R/mC \). Using the Krull-Schmidt Theorem, we obtain \( \Lambda/m\Lambda \cong R/mG \) as \( R/m \) \( G \)-module. Since \( mRG \) is a radical ideal of the group ring \( RG \), and \( \Lambda \) is a \( RG \)-module, by Lemma 3.14 in [11] \( \Lambda \) and \( RG \) are isomorphic \( RG \)-modules.

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

**Proof.** Since \( RG \) is a commutative ring, for any prime ideal \( P \) of \( RG \)

\[
\Lambda \otimes_{RG}(RG) \big|_P = (\Lambda \otimes_{p} R_p) \otimes_{R_p} (RG) \big|_P
\]

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

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

**Proof.** By Corollary 1, \( \Lambda \) 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], \( \Lambda \) is \( RG \)-free module with rank 1.

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

Before proving the Theorem, we prove the following lemma.

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

Proof. Let \( \Delta(\Lambda, G) = \sum_{\gamma \in G} \Lambda_{\gamma}u_{\gamma} \), where \( \varphi : \Delta(\Lambda, G) \otimes_R (\Delta(\Lambda, G))^\circ \to \Delta(\Lambda, G) \) is defined by \( \varphi(x \otimes y) = xy \), and set \( A = \text{right annihilator of ker } \varphi \) in \( \Lambda \). For every \( a \) in \( A \), therefore, \( \varphi(\sum_{\gamma \in G} \gamma(x \otimes u_{\gamma}) = Tr(\varphi(a)) \) is contained in \( \varphi(A) \). Since \( \Lambda \) is strongly separable over \( R \), \( \Lambda \) is separable over \( R \) and \( \Lambda = \mathbb{C}[\Lambda, \Lambda] \). Thus \( \varphi(A) = Tr(\varphi(A)) = Tr(C) \). Since \( Tr(\Lambda) \equiv 1 \), there exists \( a = c + b \) in \( \Lambda = \mathbb{C}[\Lambda, \Lambda] \) such that \( Tr(a) = Tr(c) + Tr(b) = 1 \), \( c \in \mathbb{C}, \ b \in [\Lambda, \Lambda] \), therefore \( Tr(C) \equiv Tr(c) = 1 \). Accordingly, \( \varphi(A) \equiv 1 \), \( \Delta(\Lambda, G) \) is separable over \( R \).

We have easily the following lemma.

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

Proof of Theorem 2. We suppose \( \Lambda = \sum_{\delta \in \Delta} \oplus R\sigma(\delta) \) for some element \( \delta \) in \( \Lambda \). We have easily \( \Lambda^G = RTr(\delta) = Tr(\Lambda) \). Since \( \Lambda^G \) is a ring and contains \( R \), \( Tr(\delta) \) 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 \( \sum_{\sigma \in G} \chi_{\sigma}u_{\sigma} \) is any element of the center of \( \Delta(\Lambda, G) \), then \( \chi_{\sigma} \in R \) and \( \chi_{\sigma}(\delta) = \lambda_{\sigma}(\delta) \) for every \( \sigma \in G \), hence \( \lambda_{\sigma} = 0 \) for \( \sigma \neq 1 \). Therefore, \( \Delta(\Lambda, G) \) is a central separable algebra over
Now, we consider the natural homomorphism $\delta: \Delta(\Lambda, G) \to \text{Hom}_R(\Lambda, \Lambda)$. By [1], $\text{Hom}_R(\Lambda, \Lambda)$ and $\text{Im} \delta$ are central separable algebras over $R$. Since the commutor ring $V_{\text{Hom}_R(\Lambda, \Lambda)}(\text{Im} \delta)$ of $\text{Im} \delta$ in $\text{Hom}_R(\Lambda, \Lambda)$ is $R$, by Lemma 2.3 in [4], $\delta$ is an isomorphism. Therefore, $\Lambda$ is a Galois extension of $R$ with group $G$.

**Remark.** By Proposition 8 in [10], an abelian Galois algebra $\Lambda$ over any commutative ring $R$ with abelian group $G$ is strongly separable over $R$. Therefore if $R$ is a semi-local ring, then $\Lambda$ is a Galois algebra over $R$ with abelian group $G$ if and only if $\Lambda$ 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 $\Lambda$ be an abelian Galois algebra over a commutative ring $R$ with abelian group $G$. If $R$ is indecomposable, then there exist a maximal commutative subalgebra $S$ of $\Lambda$ and a subgroup $G_1$ of $G$ such that $\Lambda^{G_1}=S$. Therefore, $\Lambda$ is a commutative Galois extension of $R$ with group $G/G_1$, and $\Lambda$ is a finitely generated projective $S$-module. Thus, if $C$ is the center of $\Lambda$ then central separable algebra $\Lambda$ over $C$ is split by $S$ in the sense of [1]. In particular, if $R$ is a local ring, then $\Lambda \otimes_R S$ is isomorphic to the full matrix ring of degree $|G|$ over the commutative ring $C \otimes_R S = \sum_{\sigma \in G/H} e_{\sigma}$ where $H = \{\sigma \in G : \sigma | C = \text{identity}\}$, $\{e_{\sigma} : \sigma \in G/H\}$ are orthogonal idempotent elements and $\sum_{\sigma \in G/H} e_{\sigma} = 1$.

Proof. For the first part, we prove by the induction on the order $|G|$. If $|G|$ is prime, then by [5], $\Lambda$ is commutative, i.e. $\Lambda = S$. We suppose $\Lambda$ is non-commutative. Since $R$ is indecomposable, by [10], $\Lambda$ is a Galois extension of the center $C$ with group $H$, and $\Lambda = \sum_{\sigma \in H} J_\sigma$, $J_\sigma = \{a \in \Lambda : \sigma(x)a = ax \text{ for all } x \in \Lambda\}$. By [5], we may assume that $H$ is not cyclic. For an element $\sigma$ in $H$, we denote the $\sigma$-fixed subring of $\Lambda$ by $\Lambda^{(\sigma)}$, then the commutor ring $V_{\Lambda}(\Lambda^{(\sigma)}) = \sum_i J_\sigma^i$ is the center of $\Lambda$ (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 $\Lambda$ and a subgroup $G_1 = G/(\sigma)$ of $G/(\sigma)$ such that $(\Lambda^{(\sigma)}) = \Lambda = S$. 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 $\Lambda$. Since $S$ is a Galois extension of $R$ with group $G/G_1$, $S$ is separable over
ABELIAN GALOIS ALGEBRA

5

i?, 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 \(|G| = m\). By Proposition 2.4 in [4], \(\text{Hom}_S(Λ, A) = (S)_m\). On the other hand, by [3], C \(\otimes K C = \sum \oplus C \epsilon\), and therefore

\[\Lambda \otimes_R S = (\Lambda \otimes_C S) \otimes_C (C \otimes_R C) = (S)_m \otimes_C (C \otimes_R C) = (S)_m \otimes_S (S \otimes_R C)\]

3. Central Galois extension

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, \(M^G = \{x \in M : \sigma x = x \text{ for all } \sigma \in G\}\) is a direct summand of M as C-module.

Proof. \(Tr'\left(x\right) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma(x)\) for \(x \in M\). Then \(Tr \colon M \to M^G\) is a C-epimorphism, and \(Tr' \mid M^G = \text{identity}\), therefore, \(M^G\) is a direct summand 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 \(\Lambda^H = \sum_{\sigma \in H'} \oplus J\),

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

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

Since \(\Lambda^H\) 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 \(V_\Lambda(\Lambda^{H'}) = \Lambda^H\).
References


