JOUR. FAC. SCI., SHINSHU UNIV. Vol. 5, pp. 29—32, May 1970

Note on Cyclic Extensions of Rings

By KAZUO KISHIMOTO

Department of Mathematics, Faculty of Science
Shinshu University
(Received May 11, 1970)

Introduction. Let A be a $\mathfrak{G}$-Galois extension of B with $A_B = B_B \oplus B'_B$ where $\mathfrak{G}$ is a finite group of automorphisms of A.

In [4], Y. Miyashita has shown that if $\mathfrak{G}$ is completely outer, then V, the centralizer of B in A, coincides with the center C of A. In general, it is unknown that whether the outerlity of $\mathfrak{G}$ implies $V = C$ or not.

In the present paper, we shall show that the outerlity of $\mathfrak{G}$ implies $V = C$ for some type of cyclic extension and some related results. As to notations and terminologies used in this paper, we follow those of [2].

§ The case of characteristic p.

Throughout the present section, we assume that B is an algebra over $GF(p)$, $\mathfrak{G}$ a cyclic group of order p with a generator σ. If A is a $\mathfrak{G}$-Galois extension of B with $A_B = B_B \oplus B'_B$, then as is shown in [2], $A = B[\alpha] = B \oplus \alpha B \oplus \alpha^2 B \oplus \cdots\cdots \oplus \alpha^{p-1}B$, a free B-module of rank p with a B-basis $\{1, \alpha, \alpha^2, \cdots\cdots, \alpha^{p-1}\}$ with $\sigma(\alpha) = \alpha + 1$.

Let $D = \alpha_r - \alpha_l$. Then it is clear that D is a derivation in B and $b\alpha = \alpha b + Db$ for each $b \in B$.

Lemma 1. *Let A/B be a $\mathfrak{G}$-Galois extension with $\sigma = \tilde{v} \in \tilde{V}$ such that $A_B = B_B \oplus B'_B$. Then each order τ of $\mathfrak{G}(A/B)$ is p and $\mathfrak{G}(A/B)$ is abelian.*

Proof. Let $\tau \in \mathfrak{G}(A/B)$. Then $b \circ \tau(\alpha) = \tau(b\alpha) = \tau(\alpha b + Db) = \tau(\alpha)b + Db$ for each $b \in B$ shows that $\tau(\alpha) - \alpha$ is contained in V. Since $\mathfrak{G}$ is inner, $V = Z$, the center of B, by [2]. Thus $\tau(\alpha) = \alpha + z$ for some $z \in Z$. This means that the order of τ is p and $\mathfrak{G}(A/B)$ is abelian.

Theorem 1. *Let Z be a field. If A/B is a $\mathfrak{G}$-Galois extension with $A_B = B_B \oplus B'_B$ then the following conditions are equivalent.*

1) $\sigma = \tilde{v}$ *for some* $v \in V$.
2) $V = Z \supsetneqq C$.
3) $\mathfrak{G}(A/B) = \tilde{Z}$.

Proof. *1)* → *2)* has been shown in [*2*] and *3)* → *1)* is clear.

2) → *3)*. Let τ be an arbitrary element of $\mathfrak{G}(A/B)$. Then, by Lemma *1*, $\tau(\alpha)=\alpha+z$. Therefore $\tau(\alpha z^{-1})=\alpha z^{-1}+1$ and $\{1, \alpha z^{-1}, (\alpha z^{-1})^2, \cdots, (\alpha z^{-1})^{p-1}\}$ is a free B-basis of A. Hence $A^{\tau}=B$. Now, by β we denote αz^{-1}, and we set $Z_j=\tau^j(\beta)j^{-1}-j^{-1}(\beta)$ and $Z_j^{(k)}=\tau^j(\beta)\tau^k(j^{-1})-j^{-1}\tau^k(\beta)$, for each $j, k=1, 2, \cdots, p\text{-}1$. Then $Z_j=1$ and $Z_j^{(k)}=1-kj^{-1}$.

Hence we have $Z_1 \cdot Z_2 \cdots\cdots Z_{p-1}=1$ and $Z_1^{(k)} \cdot Z_2^{(k)} \cdots\cdots Z_{p-1}^{(k)}=0$ for each $0<k<p-1$. This shows that the existence of a (τ)-Galois coordinate system $\{x_1, \cdots\cdots, x_n; y_1, \cdots\cdots, y_n\}$. Thus we can see that A/B is a (τ)—Galois extension, and hence $V=C\oplus J_\tau\oplus\cdots\oplus J_{\tau^{p-1}}$ where $J_{\tau^i}=\{a\in A \mid ax=\tau^i(x)a, \forall x\in A\}$. If $a\in J_{\tau^i}$, $a\beta=\tau^i(\beta)a=\beta a+ia$, we have $Ea=ia$ where $E=\beta_r-\beta_l$ is a derivation in B. Since $Z\supsetneqq C$, we have $J_{\tau^i}\neq 0$ for some i $(0<i<p)$, and hence there exists an element $z(\neq 0)$ in Z satisfying $Ez=iz$. Thus we obtain $\tau^i=\tilde{z}$ by the same reasoning as that of [*2*]. This means that $\tau=\widetilde{z^k}$ for some k.

Lemma 2. *Let Z be a field, A/B a $\mathfrak{G}$-Galois extension with $A_B=B_B\oplus B'_B$ such that σ is outer. Then $Z\subseteqq C$.*

Proof. If there exists an element $z\notin C$ $(z\in Z)$, then $z\alpha z^{-1}=\alpha+(Dz)z^{-1}$ shows that $\tilde{z}\in\mathfrak{G}$ (A/B). If we set $w=(Dz)z^{-1}$, $zrz^{-1}=r+1$ where $r=\alpha w^{-1}$, and $\{1, r, \cdots\cdots, r^{p-1}\}$ is a B-basis for A. Thus, as is shown in the proof of Theorem *1*, A/B is a $(\tilde{z})$-Galois extesnion.

Therefore we have a contradiction that σ is inner by Theorem *1* again.

Lemma 3. *Under the assumptions of Lemma 2, $D^pV=0$.*

Proof. Let $v=\alpha^{p-1}b_{p-1}+\alpha^{p-2}b_{p-2}+\cdots\cdots+b_0$ be an arbitrary element of V $(b_i\in B)$. Then $bv=\alpha^{p-1}bb_{p-1}+\alpha^{p-2}d_{p-2}+\cdots\cdots+d_0=\alpha^{p-1}b_{p-1}b+\alpha^{p-2}b_{p-2}b+\cdots\cdots+b_0b$ $(d_i\in B)$ for each $b\in B$. Hence we obtain $b_{p-1}\in Z\subseteqq C$. Consequently, $Dv=\alpha^{p-2}Db_{p-2}+\alpha^{p-3}Db_{p-3}+\cdots\cdots+Db_0\in V$. Repeating the same procedure, we have $D^pv=0$.

Theorem 2. *Let A/B be a $\mathfrak{G}$-Galois extension with $A_B=B_B\oplus B'_B$, Z a fiel. The following conditions are equivalent.*

1) *σ is an outer automorphism.*

2) *$V=C$.*

3) *$\mathfrak{G}(A/B)$ is outer.*

Moreover, if A is a ring without proper central idempotents, $\mathfrak{G}=\mathfrak{G}(A/B)$.

Proof. *2)* → *3)* and *3)* → *1)* are clear.

1) → *2)*. Since $J_{\sigma^i}=\{a\in A \mid ax=\sigma^i(x)a, \forall x\in A\}\subseteqq\{a\in A \mid a\alpha=\sigma^i(\alpha)a=(\alpha+i)a\}=\{a\in A \mid Da=ia\}$, each element v of J_{σ^i} satisfies $D^pv=i^p v$. On the other hand, Lemma *3* yields that $D^pv=0$. Therefore $v=0$, that is, $J_{\sigma^i}=0$. Thus we obtain $V=C$.

If A is a ring without proper central idmepotents, the assertion is a direct consequence of Theorem *4.2* of [*4*].

§ Kummer case.

Throughout the present section, we assume that the center Z of B is a field which contains ζ a primitive n-th root of 1, $\mathfrak{G}$ a cyclic group of order n with a generator σ. If A is a strongly-$\mathfrak{G}$ Galois extension of B*) such that the center C of A contains ζ, then as is shown in [2], $A=B[\alpha]=B\oplus\alpha B\oplus\cdots\oplus\alpha^{n-1}B$, a free B-module of rank n with a B-basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, satisfying $\sigma(\alpha)=\alpha\zeta$ and $\alpha\in U(A)$. Hence, if we set $\rho=\tilde{\alpha}^{-1}$, ρ is an automorphism of B and $b\alpha=\alpha\cdot\rho(b)$ for each $b\in B$.

Theorem 1. *If A/B is strongly-$\mathfrak{G}$ Galois extension satisfying $C\ni\zeta$ and $A_B=B_B\oplus B'_B$, then the following conditions are equivalent.*

1) $\sigma=\tilde{v}$ *for some* $v\in V$.

2) $V=Z \supsetneqq C$.

3) $\mathfrak{G}(A/B)=\tilde{Z}$.

Proof. *1)* → *2)* has been shown in [3] and *3)* → *1)* is clear.

2) → *3)*. Let τ be an arbitrary element of $\mathfrak{G}(A/B)$. Then $b\tau(\alpha)=\tau(b\alpha)=\tau(\alpha\cdot\rho(b))=\tau(\alpha)\cdot\rho(b)$ for each $b\in B$ implies that $\tau(\alpha)=\alpha\, v$ for some $v\in V=Z$. Hence, if there exists an element $w\in Z$ satisfying $\rho(w)=wv$, $w\alpha w^{-1}=\alpha\cdot\rho(w)w^{-1}=\alpha v$ yields at once $\tau=\tilde{w}$. Now, since Z is a cyclic extension of C with the Galois group (ρ), $N_\rho(w)=1$ if and only if $w=\rho(x)x^{-1}$ for some $x\in Z$ by Hilbert Theorem [Cf. Théorém 3, P. 171 [1]]. If $\tau(\alpha)=\alpha w$, $\alpha^n=\tau(\alpha^n)=(\alpha w)^n=\alpha^n N_\rho(w)$ shows that the existence of $v\in Z$ such that $\rho(v)v^{-1}=w$, that is, $\rho(v)=vw$.

Let A/B be a strongly-$\mathfrak{G}$ Galois extension mentioned in Theorem *1*. If $v=\sum_{i=0}^{n-1}\alpha^i b_i$ is an element of V, $bv=vb$ for each $b\in B$ shows that each term $\alpha^i b_i$ of v is contained in V again and further, $\alpha^i b_i\in J_{\sigma^j}$ if and only if $\rho(b_i)=b_i\zeta^j$ since $\sigma^j(\alpha)\alpha^i b_i=(\alpha^i b_i)\alpha$.

Theorem 2. *Let B be an integral domain. If A is a strongly-$\mathfrak{G}$ Galois extension of B satisfying the conditions in Theorem 1, then the followings are equivalent.*

1) σ *is an outer automorphism.*

2) $V=C$.

3) $\mathfrak{G}(A/B)$ *is outer.*

Moreover, if this is the case, $\mathfrak{G}=\mathfrak{G}(A/B)$.

Proof. *3)* → *1)* and *2)* → *3)* are clear.

1) → *2)*. Let $v=\sum\alpha^i b_i$ $(b_i\in B)$ be an arbitrary element of $J_{\sigma j}$. Then each term

---

*) A $\mathfrak{G}$-Galois extansion A of B is called a *strongly-$\mathfrak{G}$ Galois extension* of B if A has no proper central idempotents, and further $j(u_1+\zeta u_\sigma+\cdots+\zeta^{n-1}u_{\sigma^{n-1}})(A)\cap U(A)\neq\phi$ where $U(A)$ is the group of units of A and ζ is a primitive n-th root of 1 which is contained in Z. If B is semi-local with $Z\ni\zeta$, any $\mathfrak{G}$-Galois extension without proper central idempotents is a strongly-$\mathfrak{G}$ Galois extension.

$\alpha^i b_i$ of v is contained in $J_{\sigma j}$ again, and $\alpha^i b_i$ is non regular since σ is outer. Now $N_\sigma(\alpha^i b_i)$ is contained in $V \cap B = Z$. Hence, if $N_\sigma(\alpha^i b_i) \neq 0$, we obtain that $\alpha^i b_i$ is regular. Consequently, we have $N_\sigma(\alpha^i b_i) = 0$. On the other hand, $N_\sigma(\alpha^i b_i) = \alpha^i b_i (\alpha^i \zeta^i b_i)(\alpha^i \zeta^{2i} b_i) \cdots (\alpha^i \zeta^{(n-1)i} b_i) = (\alpha^i)^n \rho^{(n-1)i}(b_i) \rho^{(n-2)i}(b_i) \cdots \rho^i(b_i) b_i (\zeta^i)^{n(n-1)/2} = 0$. Hence $b_i = 0$. This means that $J_{\sigma j} = 0$ if $j = 1, 2, \cdots, n\text{-}1$.

Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$. Then $\mathfrak{H} = (\sigma^m)$ for some divisor m of n, and $A^{\mathfrak{H}} = B \oplus (\alpha^{m'}) B \oplus (\alpha^{m'})^2 B \oplus \cdots \oplus (\alpha^{m'})^{m-1} B$ where $m' = n/m$. If $r \neq im'$ $(i = 0, 1, 2, \cdots, m\text{-}1)$, $0 < r < n$, then $r + jm' \neq lm'$ for each $j, l = 0, 1, 2, \cdots, m\text{-}1$, $A^{\mathfrak{H}}$ is an $A^{\mathfrak{H}}$-direct summand of A. Thus $\mathfrak{G} = \mathfrak{G}(A/B)$ by Theorem *4. 2* of [*4*].

References

[1] BOURBAKI, N. : ALGEBRE, Chap. 4–Chap. 5, HERMANN.

[2] KISHIMOTO, K. : On abelian extensions of rings I. (to appear in Okayama J. Math.).

[3] KISHIMOTO, K. : On abelian extensions of rings II. (to appear)

[4] MIYASHITA, Y. : Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., Vol. 19 (1966), 114–134.