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 $\sigma$. If $A$ is a $\mathfrak{G}$-Galois extension of $B$ with $A_B = B_B \oplus B'_B$, then as is shown in [2], $A = B[\sigma] = B \oplus \alpha B \oplus \alpha^2 B \oplus \cdots \cdots \cdots \oplus \alpha^{p-1} B$, a free $B$-module of rank $p$ with a $B$-basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{p-1}\}$ with $\sigma(\alpha) = \alpha + 1$.

Let $D = a_1 - \alpha_i$. Then it is clear that $D$ is a derivation in $B$ and $b\sigma = ab + Db$ for each $b \in B$.

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

Proof. Let $\tau \in \mathfrak{G}(A/B)$. Then $b \cdot \tau(\alpha) = \tau(b\alpha) = \tau(ab + Db) = \tau(\alpha)b + Db$ 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 $\tau$ 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) $\sigma = \tilde{\alpha}$ for some $\nu \in \tilde{V}$.
2) $V = Z \cong C$.
3) $\mathfrak{G}(A/B) = \tilde{Z}$. 
Proof. \(1) \Rightarrow 2\) has been shown in \([2]\) and \(3) \Rightarrow 1\) is clear.

\(2) \Rightarrow 3\). Let \(\tau\) be an arbitrary element of \(\mathcal{G}(A/B)\). Then, by Lemma 1, 
\(\tau(\alpha) = \alpha + z\). Therefore \(\tau(\alpha z^{-1}) = \alpha z^{-1} + 1\) and \(\{1, \alpha z^{-1}, (\alpha z^{-1})^2, \ldots, (\alpha z^{-1})^{p-1}\}\) is a free 
\(B\)-basis of \(A\). Hence \(A^\tau = B\). Now, by \(\beta\) we denote \(\alpha z^{-1}\), and we set 
\(Z_j = \tau^j(\beta)j^{-1} - j^{-1}(\beta)\) and \(Z_j^{(k)} = \tau^j(\beta)j^{-1} - j^{-1}(\beta)\), for each \(j, k = 1, 2, \ldots, p-1\). 
Then \(Z_j = 1\) and \(Z_j^{(k)} = 1 - k j^{-1}\).

Hence we have \(Z_1 Z_2 \cdots Z_{p-1} = 1\) and \(Z_j^{(k)} Z_2^{(k)} \cdots Z_{p-1}^{(k)} = 0\) for each \(0 < k < p-1\). This shows that the existence of a \((\tau)\)-Galois coordinate system \(\{x_1, \ldots, x_i, y_1, \ldots, y_n\}\). Thus we can see that \(A/B\) is a \((\tau)\)-Galois extension, and hence 
\(V = C \oplus J_1 \oplus \cdots \oplus J_{p-1}\) where \(J_i = \{a \in A \mid ax = \tau^i(x)a, \forall x \in A\}\). If \(a \in J_i\), \(\alpha = \tau^i(a) = \beta a + ia\) where \(E = \beta - \beta_i\) is a derivation in \(B\). Since 
\(Z \subseteq C\), we have \(J_i \neq 0\) for some \(i\) \((0 < i < p)\), and hence there exists an element 
\(z \neq 0\) in \(Z\) satisfying \(Ez = iz\). Thus we obtain \(\tau = \tilde{z}\) by the same reasoning as 
that of \([2]\). This means that \(\tau = \tilde{z}^k\) for some \(k\).

Lemma 2. Let \(Z\) be a field, \(A/B\) a \(\mathcal{G}\)-Galois extension with \(A_B = B_B \oplus B'_B\) such 
that \(\sigma\) is outer. Then \(Z \subseteq C\).

Proof. If there exists an element \(z \in C\) \((z \in Z)\), then \(zax^{-1} = a + (Dz)x^{-1}\) shows 
that \(z \in \mathcal{G}(A/B)\). If we set \(w = (Dz)x^{-1}, zrx^{-1} = r + 1\) where \(r = ax^{-1}\), and \(\{1, r, 
\ldots, r^{p-1}\}\) is a \(B\)-basis for \(A\). Thus, as is shown in the proof of Theorem 1, 
\(A/B\) is a \((\tilde{z})\)-Galois extension.

Therefore we have a contradiction that \(\sigma\) is inner by Theorem 1 again.

Lemma 3. Under the assumptions of Lemma 2, \(D^p V = 0\).

Proof. Let \(v = a^{p-1}b_{p-1} + a^{p-2}b_{p-2} + \cdots + b_0\) be an arbitrary element of \(V\) \((b_i \in B)\). Then 
\(bv = a^{p-1}b_{p-1} + a^{p-2}d_{p-2} + \cdots + b_0\) \(= \alpha^{p-1}b_{p-1} + \alpha^{p-2}b_{p-2} + \cdots + b_0\) \(= d_1 \in B\) for 
each \(b \in B\). Hence we obtain \(b_{p-1} \in Z \subseteq C\). Consequently, \(Dv = a^{p-2}Db_{p-2} + a^{p-3}Db_{p-3} 
\cdots + Db_0 \in V\). Repeating the same procedure, we have \(D^p v = 0\).

Theorem 2. Let \(A/B\) be a \(\mathcal{G}\)-Galois extension with \(A_B = B_B \oplus B'_B\), \(Z\) a field. The 
following conditions are equivalent.

1) \(\sigma\) is an outer automorphism.
2) \(V = C\).
3) \(\mathcal{G}(A/B)\) is outer.

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

Proof. \(2) \Rightarrow 3)\) and \(3) \Rightarrow 1)\) are clear.

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

If \(A\) is a ring without proper central idempotents, 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, Ø a cyclic group of order n with a generator σ. If A is a strongly-Ø Galois extension of B\(^{\sigma}\) such that the center C of A contains ζ, then as is shown in [2], A = B[ζ] = B ⊕ aB ⊕ ⋯ ⊕ a\(^{n-1}\)B, a free \(B\)-module of rank n with a \(B\)-basis \(\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}\), satisfying \(σ(α) = α^n\) and \(α ∈ U(A)\). Hence, if we set \(ρ = α^{-1}\), ρ is an automorphism of \(B\) and \(ba = α⋅ρ(b)\) for each \(b ∈ B\).

**Theorem 1.** If \(A/B\) is a strongly-Ø Galois extension satisfying \(C ∋ ζ\) and \(A_B = B_B \oplus B'_B\), then the following conditions are equivalent.

1) \(σ = \emptyset\) for some \(v ∈ V\).
2) \(V = Z \oplus C\).
3) \(Ø(A/B) = \emptyset\).

**Proof.** 1) → 2) has been shown in [3] and 3) → 1) is clear.
2) → 3). Let \(τ\) be an arbitrary element of \(Ø(A/B)\). Then \(bτ(α) = τ(bα) = τ(α⋅ρ(b)) = τ(α)⋅ρ(b)\) for each \(b ∈ B\) implies that \(τ(α) = α v\) for some \(v ∈ V = Z\). Hence, if there exists an element \(w ∈ Z\) satisfying \(ρ(w) = vw\), \(waw^{-1} = α⋅ρ(w)w^{-1} = αv\) yields at once \(τ = \bar{w}\). Now, since \(Z\) is a cyclic extension of \(C\) with the Galois group \(\langle ρ \rangle\), \(N_ρ(w) = 1\) if and only if \(w = ρ(x)x^{-1}\) for some \(x ∈ Z\) by Hilbert Theorem [Cf. Théorème 3, P.171 [1]]. If \(τ(α) = αw\), \(α^n = τ(α^n) = (αw)^n = α^nN_ρ(w)\) shows that the existence of \(v ∈ Z\) such that \(ρ(v)v^{-1} = w\), that is, \(ρ(v) = vw\).

Let \(A/B\) be a strongly-Ø Galois extension mentioned in Theorem 1. If \(v = \sum_{i=0}^{n-1} α^ib_i\) is an element of \(V\), \(bv = vb\) for each \(b ∈ B\) shows that each term \(α^ib_i\) of \(v\) is contained in \(V\) again and further, \(α^ib_i ∈ J_i\) if and only if \(ρ(b_i) = b_i\xi^i\) since \(α^i(α)α^ib_i = (α^ib_i)α\).

**Theorem 2.** Let \(B\) be an integral domain. If \(A\) is a strongly-Ø 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) \(Ø(A/B)\) is outer.

Moreover, if this is the case, \(Ø = Ø(A/B)\).

**Proof.** 3) → 1) and 2) → 3) are clear.
1) → 2). Let \(v = \sum_0^{n-1} α^ib_i\) be an arbitrary element of \(J_i\). Then each term
Let $S$ be a subgroup of $S$. Then $S = (a^m)$ for some divisor $m$ of $n$, and $A^\varnothing = B \oplus (a^{m'})B \oplus (a^{m''})B \oplus \cdots \oplus (a^{m''})^{m-1}B$ where $m' = n/m$. If $r \neq im'$ ($i = 0, 1, 2, \ldots, m-1$), $0 < r < n$, then $r + jm' \neq lm'$ for each $j, l = 0, 1, 2, \ldots, m-1, A^\varnothing$ is an $A^\varnothing$-direct summand of $A$. Thus $S = (A/B)$ by Theorem 4.2 of [4].

References