A Note on Submodules of a Galois Extension of a Ring with a Cyclic Galois Group of Order $p^e$

By KAZUO KISHIMOTO

Department of Mathematics, Faculty of Science, Shinshu University

(Received November, 16, 1976)

Let $B$ be an algebra over $GF(p)$ with 1, $A$ an extension ring of $B$. If a group $G$ acts on $A$ as a group of $B$-automorphisms, then $D_\sigma = \sigma - 1$ becomes a $\sigma$-derivation in $A$ for each $\sigma \in G$, i.e., $D_\sigma (x+y) = D_\sigma (x) + D_\sigma (y)$ and $D_\sigma (xy) = \sigma (x)D_\sigma (y) + D_\sigma (x)y$ for each $x, y \in A$. If we set $D_0 = 1$, then the $D_\sigma^k$-constant $A(k) = \{a \in A | D_\sigma^k(a) = 0\}$ is a right $B$-submodule of $A$ for each non negative integer $k$, and if $k = p^j$, $A(k)$ coincides with the fixed subring $A^\eta$ with $\eta = \sigma^k$ since $D_\sigma^k = \sigma^k - 1$. Hence, if $G$ is a cyclic group of order $p^e$ with a generator $\sigma$ and $A/B$ is a $G$-cyclic extension with $A_B \oplus > B_B$, then the $D_\sigma^k$-constant $A(k)$ is a free right ($\sigma$-as well as left) $B$-module with a basis $\{x_i | i = 1, 2, \cdots, k\}$ by [2] if $k = p^j$. In this note, we shall show that $A(n)$ is also a free right $B$-module with a basis $\{w_i | i = 1, 2, \cdots, n\}$ for each $1 \leq n \leq p^e$ and some related results. These are obtained in [1] when $A$ is a division ring.

Now, we shall begin our study from the following

**Lemma 1.** Let $D = D_\sigma$ for some $\sigma \neq 1 \in G$.

1. $D^n(xY) = \sum_{i=0}^n \binom{n}{i} \sigma^i D^{n-i}(x) D^i(y)$ for each $x, y \in A$.

2. If $D(y) = 1$ then $D^k(y^k) = k!$.

**Proof.** We shall prove the assertions by the induction on $n$.

1. Since $D(xY) = \sigma(x)D(y) + D(x)y$, we assume that $D^k(xY) = \sum_{i=0}^k \binom{k}{i} \sigma^i D^{k-i}(x) D^i(y)$ for $k \geq 1$. Then,

\[
D^{k+1}(xY) = D(\sum_{i=0}^k \binom{k}{i} \sigma^i D^{k-i}(x) D^i(y)) \\
= \sum_{i=0}^k \binom{k}{i} [\sigma^{i+1} D^{k-i}(x) D^{i+1}(y) + \sigma^i D^{k+1-i}(x) D^i(y)] \\
= D^{k+1}(xY) + \sum_{i=1}^k \binom{k}{i-1} \sigma^i D^{k-i}(x) D^i(y) + \sigma^{k+1}(x) D^{k+1}(y) \\
= \sum_{i=0}^{k+1} \binom{k+1}{i} \sigma^i D^{k+1-i}(x) D^i(y).
\]
(2) Since \( D(Y) = 1 \), we assume that \( D^k(Y) = k! \). Then
\[
D^{k+1}(Yk+1) = D(D^k(Yk)) = D\left(\sum_{i=0}^{k} \binom{k}{i} a^i D^{k-i}(Y) D^i(Y)\right)
\]
\[= D(k! y + k a D^{k-1}(Y)) \]
\[= k! + k k! = (k + 1)!. \]

In all that follows, we assume that \( G \) is a cyclic group of order \( p^e \) with a generator \( \sigma \), \( A/B \) is a \( G \)-cyclic extension with \( A_B \oplus B_B \), \( D = D_\sigma \) and \( A(k) \) is the \( D \)-constant of \( A \) for each \( 0 \leq k \leq p^e \). Further, we put \( m = p^n \), \( m' = p^{n+1} \) and \( \eta = \sigma^m \). Then \( A(m')/A(m) \) is a \( (\eta)/(\eta p) \)-cyclic extension with \( A(m')_{A(m')} \oplus A(m)_{A(m)} \).

Therefore there exists an \( (m) \)-basis \( \{1, y_{n+1}, y_{n+1}^2, \ldots, y_{n+1}^{p-1}\} \) for \( A(m') \) such that \( D^m(Y_{n+1}) = 1 \) by [2]. Since \( \eta(D(Y_{n+1})) = D(\eta(y_{n+1})) = D(D^m(Y_{n+1}) + y_{n+1}) = D(y_{n+1}) \), we have \( D(y_{n+1}) \in A(m) \).

By \( \{1, y_{n+1}, y_{n+1}^2, \ldots, y_{n+1}^{p-1}\} \), we denote an \( A(m') \)-basis for \( A(m') \) such that \( D(Y_{n+1}) \in A(m \oplus A(m)_{A(m)}) \). Hence, if we put \( E = D^m \), then \( E^i(y_{n+1}) = i! \) if \( i = j \) by Lemma 1 (2).

**Lemma 2.** \( D^{k-1}(A(k)) \) coincides with \( B \) for each \( 1 \leq k \leq p^e \).

**Proof.** Since \( A(1) = B = D^o(A(1)) \), we assume that \( D^{k-1}(A(k)) = B \) for \( k \geq 1 \).

Let \( k = a p^n + \sum_{i=0}^{n-1} a_i p^i \) be a \( p \)-expansion of \( k \) with \( a \neq 0 \) and \( y = y_{n+1} \).

(i) \( k + 1 = a p^n + \sum_{i=0}^{n-1} (a_i + 1) p^i \) for some \( j < n \): For any \( i < p^n \), \( E(x) = 0 \) for each \( x \in A(i) \) shows that \( E^i(yx) = a! x \). Hence \( D^k(a p^n(A(k + 1) + a p^n)) = D^{k+1-\alpha} E^i(yx(A(k + 1) + a p^n)) = D^{k+1-\alpha} E^i(yx(A(k + 1) + a p^n)) = 0 \). Thus \( A(k + 1) \) contains \( y^k A(k + 1) + a p^n \), and hence \( D^k(A(k + 1)) \supseteq D^k(y^k A(k + 1) + a p^n) = D^{k-\alpha} E^i(yx(A(k + 1) + a p^n)) = B \) by the induction hypothesis. On the other hand, \( B = A(1) \supseteq D^k(A(k + 1)) \) is clear. Therefore \( D^k(A(k + 1)) = B \).

This Lemma enable us to prove the following

**Theorem.** (1) \( D(A(k)) \) coincides with \( A(k-1) \) for each \( 1 \leq k \leq p^e \). In particular, if \( A(k) \) is a free right \( B \)-module with a basis \( \{x_1, x_2, \ldots, x_k \mid k \geq 1\} \) then \( A(k-1) \) is a free right \( B \)-module with a basis \( \{D(x_k), D(x_k), \ldots, D(x_k) \} \).

(2) There exists an element \( x_k \) in \( A(k) \) such that \( D^{k-1}(x_k) = 1 \) and \( \{D^i(x_k) \mid i = 0, 1, \ldots, k-1\} \) is a free right \( B \)-basis for \( A(k) \).

**Proof.** (1) Since \( D(A(k+1)) \supseteq A(k) \), it suffices to prove \( D(A(k+1)) \supseteq A(k) \). Now \( 0 = A(0) \subseteq D(A(1)) \) is clear, and hence, we assume that \( D(A(k)) \supseteq A(k-1) \).
A Note on Submodules of a Galois Extension of a Ring.

for $k \geq 1$. Let $x$ be an element of $A(k)$. Then $D^{k-1}(x) = D^k(y)$ for some $y \in A(k+1)$ by Lemma 2. Hence $D(y) - x \in \text{Ker } D^{k-1} = A(k-1)$, and hence, $x \in D(A(k+1)) + A(k-1) \subseteq D(A(k+1)) + D(A(k)) = D(A(k+1))$.

If $A(k) = \sum_{i=1}^{k} x_i B$ then $A(k-1) = D(A(k)) = \sum_{i=2}^{k} D(x_i) B$. Moreover, if $\sum_{i=2}^{k} D(x_i) b_i = 0$ then $0 = \sum_{i=2}^{k} D(x_i b_i)$ implies $\sum_{i=2}^{k} x_i b_i \in A(1) = B$. Consequently $b_i = 0$ for $i = 2, 3, \ldots, k$.

(2) Noting that $A(y)/B$ is a $(\sigma)/(\sigma y)$-cyclic extension with $A(y) B \supseteq B y$, $A(y) = B \oplus y_1 B \oplus \cdots \oplus y_{k-1} B$ with $D(y_i) = 1$. Hence $A(2) \supseteq B \oplus y_1 B$. On the other hand, if $a \in A(2) \subseteq A(y)$, $a = \sum_{i=0}^{b-1} y_i b_i$. But $D^2(a) = 0$ shows that $a = b_0 + y_1 b_1$ by Lemma 1 (2). Consequently, $A(2) = B \oplus y_1 B$ and $D(y_1) = 1$ is a $B$-basis for $A(1) = B$. Hence, assume that $x_k$ has been chosen as desired in $A(k)$. Since $D(A(k+1)) = A(k)$, there exists an element $x_{k+1} \in A(k+1)$ with $D(x_{k+1}) = x_k$. Then $\{D^i(x_k), x_{k+i} ; i = 0, 1, \ldots, k\}$ is right linearly independent over $B$.

Let $T = A(k) \oplus x_{k+1} B$. Then $T \subseteq A(k+1)$ and $D(T) = D(A(k)) + x_k B = \sum_{i=0}^{b-1} D^i(x_k) B = A(k) = D(A(k+1))$. Hence, for any $a \in A(k+1)$, there exists an element $t \in T$ such that $D(a) = D(t)$. Consequently $a - t \in \text{Ker } D = B$, and this means that $a \in T + B = T$. Thus we have $T = A(k+1)$.

As immediate consequences of Theorem, we have the following

**Corollary 1.** There exists an element $x \in A$ such that

(1) $A = \sum_{i=0}^{\sigma^k-1} \oplus D^i(x) B$

(2) $A = \sum_{i=0}^{\sigma^k-1} \oplus \sigma^i(x) B$, i.e., $A$ possesses a $G$-normal basis.

**Proof.** (1) is clear.

(2) It is clear that $\sum_{i=0}^{k} \oplus D^i(x) B = \sum_{i=0}^{k} \sigma^i(x) B$ for each $0 \leq k \leq \sigma^k - 1$. Let $x b + \sigma(x) c = 0$ for $b, c \in B$. Then $-x c = x b + (\sigma(x) - x) c = x b + D(x) c$ shows that $c = b = 0$. Hence we assume that $\sum_{i=0}^{k} \oplus D^i(x) B = \sum_{i=0}^{k} \sigma^i(x) B$ for $k \geq 0$. If $k + 1 < \sigma^k - 1$ and $\sigma^{k+1}(x) b \in \sum_{i=0}^{k} \oplus \sigma^i(x) B$ for some $b \neq 0 \in B$, we have a contradiction $D^{k+1}(x) b \in \sum_{i=0}^{k} \oplus D^i(x) B$ since $D^{k+1} = (\sigma - 1)^{k+1} = \sum_{i=0}^{k+1} \sigma^i(x) B$ for $k \geq 0$. Thus $A = \sum_{i=0}^{\sigma^k-1} \oplus \sigma^i(x) B$.

**Corollary 2.** If $M$ is a right $B$-submodule of $A$ satisfying $D(M) \subseteq M$ and $D^k(M) = B$ for some $k \geq 0$, then $M = A(k+1)$.

**Proof.** If a right $B$-submodule $M$ of $A$ satisfies $D(M) \supseteq M$ and $D^0(M) = B$, then $M = B = A(1)$. Hence we assume that $M = A(k)$ if $D(M) \subseteq M$ and $D^{k-1}(M)$
= B for \( k \geq 1 \).

Let \( D(M) \subseteq M \) and \( D^k(M) = B \) for some right \( B \)-submodule \( M \). Then \( D^{k-1}(D(M)) = B \). Noting that \( D(D(M)) \subseteq D(M) \), \( D(M) = A(k) = D(A(k + 1)) \) by the induction hypothesis. Thus \( A(k + 1) = M + \ker D = M + B = M \).

References
