JOUR. FAC. SCI., SHINSHU UNIVERSITY, Vol. 12, No.1 June, 1977

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

(Recieved 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 σ-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 $D_\sigma{}^0 = 1$, then the $D_\sigma{}^k$-constant $A(k) = \{a \in A \mid D_\sigma{}^k(a) = 0\}$ is a right B-submodule of A for each non negative integer k, and if $k = p^f$, $A(k)$ coincides with the fixed subring A^η 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 σ 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 (as well as left) B-module with a basis $\{x_i \mid i = 1, 2, \cdots, k\}$ by [2] if $k = p^f$. In this note, we shall show that $A(n)$ is also a free right B-module with a basis $\{w_i \mid i = 1, 2, \cdots, n\}$ for each $1 \leqq n \leqq p^e$ 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 $k \geqq 1$. Then,

$$\begin{aligned} D^{k+1}(xy) &= D\Big(\sum_{i=0}^{k} \binom{k}{i} \sigma^i D^{k-i}(x) D^i(y)\Big) \\ &= \sum_{i=0}^{k} \binom{k}{i} [\sigma^{i+1} D^{k-i}(x) D^{i+1}(y) + \sigma^i D^{k+1-i}(x) D^i(y)] \\ &= D^{k+1}(x)y + \sum_{i=1}^{k} \Big(\binom{k}{i-1} \sigma^i D^{k-(i-1)}(x) D^i(y) \\ &\quad + \binom{k}{i} \sigma^i D^{k+1-i}(x) D^i(y)\Big) + \sigma^{k+1}(x) D^{k+1}(y) \\ &= \sum_{i=0}^{k+1} \binom{k+1}{i} \sigma^i D^{k+1-i}(x) D^i(y). \end{aligned}$$

(2) Since $D(y)=1$, we assume that $D^k(y^k)=k!$. Then

$$D^{k+1}(y^{k+1})=D(D^k(y^k)y)=D(\textstyle\sum_{i=0}^{k}\binom{k}{i}\sigma^i D^{k-i}(y^k)D^i(y))$$
$$=D(k!y+k\sigma D^{k-1}(y^k))$$
$$=k!+kk!=(k+1)!.$$

In all that follows, we assume that G is a cyclic group of order p^e with a generator σ, A/B is a G-cyclic extension with $A_B \oplus > B_B$, $D=D_\sigma$ and $A(k)$ is the D^k-constant of A for each $0 \leqq k \leqq p^e$. 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 $A(m)$-basis $\{1, y_{n+1}, y_{n+1}^2, \cdots, y_{n+1}^{p-1}\}$ 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 $\{1, y_{n+1}, y_{n+1}^2, \cdots, y_{n+1}^{p-1}\}$, we denote an $A(m)$-basis for $A(m')$ such that $D(y_{n+1}) \in A(m)$ and $D^m(y_{n+1})=1$. Hence, if we put $E=D^m$, then $E^j(y_{n+1}^i)=\begin{cases} i! & \text{if } i=j \\ 0 & \text{if } i<j \end{cases}$ by Lemma 1 (2).

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

Proof. Since $A(1)=B=D^0(A(1))$, we assume that $D^{k-1}(A(k))=B$ for $k \geqq 1$. Let $k=ap^n+\sum_{i=0}^{n-1}a_i p^i$ be a p-expansion of k with $a \neq 0$ and $y=y_{n+1}$.

(i) case $k+1=p^{n+1}(=m')$: $A(k+1)=A(m')=A(m) \oplus yA(m) \oplus y^2A(m) \oplus \cdots \oplus y^{p-1}A(m)$. Hence $E^{p-1}(A(k+1))=A(m)$ yields $D^k(A(m'))=D^{m-1}E^{p-1}(A(k+1))=D^{m-1}(A(m))=B$ by the induction hypothesis.

(ii) case $k+1=ap^n+\cdots+(a_j+1)p^j$ for some $j<n$: For any $i<p^n$, $E(x)=0$ for each $x \in A(i)$ shows that $E^a(y^a x)=a!x$. Hence $D^{k+1}(y^a A(k+1-ap^n))=D^{k+1-ap^n}E^a(y^a A(k+1-ap^n))=D^{k+1-ap^n}(A(k+1-ap^n))=0$. Thus $A(k+1)$ contains $y^a A(k+1-ap^n)$, and hence $D^k(A(k+1)) \supseteqq D^k(y^a A(k+1-ap^n))=D^{k-ap^n}E^a A(k+1-ap^n))=D^{k-ap^n}(A(k+1-ap^n))=B$ by the induction hypothesis. On the other hand, $B=A(1) \supseteqq D^k(A(k+1))$ 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 $1 \leqq k \leqq p^e$. In particular, if $A(k)$ is a free right B-module with a basis $\{x_1=1, x_2, \cdots, x_k\,;\, k>1\}$ then $A(k-1)$ is a free right B-module with a basis $\{D(x_2), D(x_3), \cdots, D(x_k)\}$.*

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

Proof. (1) Since $D(A(k+1)) \subseteqq A(k)$, it suffices to prove $D(A(k+1)) \supseteqq A(k)$. Now $0=A(0) \subseteqq D(A(1))$ is clear, and hence, we assume that $D(A(k)) \supseteqq A(k-1)$

for $k \geqq 1$. 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 $D(y) - x \in Ker\, D^{k-1} = A(k-1)$, and hence, $x \in D(A(k+1)) + A(k-1) \subseteqq D(A(k+1)) + D(A(k)) = D(A(k+1))$.

If $A(k) = \sum_{i=1}^{k} \oplus x_i B$ 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 $i = 2, 3, \cdots, k$.

(2) Noting that $A(p)/B$ is a $(\sigma)/(\sigma^p)$-cyclic extension with $A(p)_B \oplus > B_B$, $A(p) = B \oplus y_1 B \oplus \cdots \oplus y_1^{p-1} B$ with $D(y_1) = 1$. Hence $A(2) \supseteqq B \oplus y_1 B$. On the other hand, if $a \in A(2) \subseteqq A(p)$, $a = \sum_{i=0}^{p-1} y_1{}^i b_i$. 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 choosen 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 $\{D^i(x_k), x_{k+1}\,;\, i = 0, 1, \cdots, k-1\}$ is right linearly independent over B.

Let $T = A(k) \oplus x_{k+1}B$. Then $T \subseteqq A(k+1)$ and $D(T) = D(A(k)) + x_k B = \sum_{i=0}^{k-1} \oplus D^i(x_k)B = A(k) = D(A(k+1))$. Hence, for any $a \in A(k+1)$, there exists an element $t \in T$ such that $D(a) = D(t)$. Consequently $a - t \in Ker\, D = B$, 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) $A = \sum_{i=0}^{p^e-1} \oplus D^i(x)B$

(2) $A = \sum_{i=0}^{p^e-1} \oplus \sigma^i(x)B$, *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 $0 \leqq k \leqq p^e - 1$. Let $xb + \sigma(x)c = 0$ for $b, c \in B$. Then $-xc = xb + (\sigma(x) - x)c = xb + D(x)c$ shows that $c = b = 0$. Hence we assume that $\sum_{i=0}^{k} \oplus D^i(x)B = \sum_{i=0}^{k} \oplus \sigma^i(x)B$ for $k \geqq 0$. If $k + 1 < p^e - 1$ 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 $D^{k+1} = (\sigma - 1)^{k+1} = \sum_{i=0}^{k+1} \binom{k+1}{i} (-1)^i \sigma^{k+1-i}$. Thus $A = \sum_{i=0}^{p^e-1} \oplus \sigma^i(x)B$.

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

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

$= B$ for $k \geqq 1$.

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

References

[1] A. S. AMITSUR : Non-commutative cyclic fields, *Duke Math. Jour.* **vol.** 21 (1954), 87–105.

[2] K. KISHIMOTO : On abelian extensions of rings I, *Math. Jour. Okayama Univ.*, **vol.** 14 (1970), 150–174.