Mathematical Journal of Okayama University

Volume 25, *Issue* 2 1983 *Article* 2

DECEMBER 1983

On connectedness of p-Galois extensions of rings

Miguel Ferrero* Kazuo Kishimoto†

*Universidade Federal

†Shinshu University

Math. J. Okayama Univ. 25 (1983), 103—121

ON CONNECTEDNESS OF p-GALOIS EXTENSIONS OF RINGS

MIGUEL FERRERO and KAZUO KISHIMOTO

Let A be an algebra over a prime field GF(p) of prime characteristic p with an identity 1 and G a finite p-group. A ring is said to be *connected* if the center contains no nontrivial idempotents.

In this paper, we study the connectedness of G-Galois extensions over a connected ring A. The study contains the extensions of several results cited in [7], [8] and [11] to the non-commutative case.

Our study starts with the preliminary section §1, which is devoted to notations and some general remarks about a skew polynomial ring of derivation type and abelian extensions of rings which have been noted in [5] and [6].

In §2, G is assumed to be cyclic and we will give necessary and sufficient conditions for A to have a connected G-Galois extension B for the case $|G|=p$. Further, if B is a G-Galois extension for $G=(\sigma)$ with $|\sigma|=p^e$, we can prove that B is connected if and only if $T=B^{\sigma^p}$, the fixed subring of B under σ^p, is connected. In §§3 and 4, we shall extend the results of §2 to the case in which G is a noncyclic abelian group and to the case in which G is a non abelian group.

1. Preliminaries. Let A be a ring with an identity 1 which has derivations $\{D_i\,;\,i=1,\cdots,n\}$ and a family $\mathcal{A}=\{a_{ij}: i,j=1,\cdots,n\}$ of elements in A such that

(1) $a_{ij}+a_{ji}=a_{ii}=0$,

(2) $[D_i,D_j]=D_iD_j-D_jD_i=I_{a_{ji}}$, an inner derivation $(a_{ji})_r-(a_{ji})_l$,

(3) $D_i(a_{jk})+D_k(a_{ij})+D_j(a_{ki})=0$

for all $i,j,k=1,\cdots,n$.

The set of all polynomials

$$\{\sum X_1^{\nu_1}X_2^{\nu_2}\cdots X_n^{\nu_n}\ a_{\nu_1\nu_2\cdots\nu_n}\,;\, a_{\nu_1\nu_2\cdots\nu_n}\in A\}$$

becomes an associative ring by the rules

$$aX_i=X_ia+D_i(a) \text{ for all } a\in A \text{ and } X_iX_j=X_jX_i+a_{ij}.$$

The first named author was supported by a fellowship awarded by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Brazil.

This ring is denoted by $R_n=A[X_1,\cdots,X_n\,;D_1,\cdots,D_n,\mathcal{A}]$ or $R_n=A[X_1,\cdots,X_n\,;D_1,\cdots,D_n,\{a_{ij}\,;i,j=1,\cdots,n\}]$ and is called a skew polynomial ring of derivation type (see [5]). Moreover, by $R_m(0\leqq m\leqq n)$, we denote the skew polynomial ring $A[X_1,\cdots,X_m\,;D_1,\cdots,D_m,\{a_{ij}\,;i,j=1,\cdots,m\}]$ which is a subring of R_n, where $R_0=A$. In particular, if $n=1$, we denote it by

$$R=A[X;D]=\{\sum X^i a_i\,;a_i\in A\}$$

and its multiplication is given by $aX=Xa+D(a)$ for $a\in A$.

Further, by D_m^*, we denote the derivation of R_{m-1} defined by $D_m^*(h)=hX_m-X_mh\,(h\in R_{m-1})$, where $1\leqq m\leqq n$. Clearly $D_m^*\,|\,A=D_m$, and $D_m^*(X_k)=a_{km}$.

Remark 1.0. For a permutation π of m letters $1,\cdots,m$ $(m\leqq n)$, we have an A-ring isomorphism

$$R_m\cong A[X_{\pi(1)},\cdots,X_{\pi(m)}\,;D_{\pi(1)},\cdots,D_{\pi(m)},\{a_{\pi(i)\pi(j)}\,;i,j=1,\cdots,m\}]$$

which maps X_i to $X_{\pi(i)}$ $(i=1,\cdots,m)$. Moreover, there holds

$$R_m\cong R_{m-1}[X_m\,;D_m^*]\ (1\leqq m\leqq n).$$

Definition 1.1. Let g be a monic polynomial in $R_{m-1}[X_m\,;D_m^*]=R_m$ where $1\leqq m\leqq n$. g is called a *generator* in R_n if $gR_n=R_ng$. Moreover, a generator g in $A[X;D]$ is called *weakly irreducible* (abbreviate *w-irreducible*) if g has no proper monic factors of degree $\geqq 1$ which is a generator.

Remark 1.2. The notion of w-irreducibility of g in $A[X]$ coincides with irreducibility of g in $C(A)\,[X]$ where $C(A)$ is the center of A since each generator in $A[X]$ is contained in $C(A)\,[X]$.

Remark 1.3. Let $R_m=R_{m-1}[X_m\,;D_m^*]\,(1\leqq m\leqq n)$. Then, there exists a generator $g=X_m-f$ $(f\in R_{m-1})$ in R_m if and only if there exists an element $Y\in R_m$ such that $R_m=R_{m-1}[Y]$ (i.e., R_m is a free R_{m-1}-module with the basis $\{1,\ Y,\ Y^2,\cdots\}$ such that $hY=Yh$ for all $h\in R_{m-1}$).

For, if $g=X_m-f$ $(f\in R_{m-1})$ is a generator in $R_m=R_{m-1}[X_m\,;D_m^*]$ then D_m^* is the inner derivation I_f of R_{m-1} effected by f(that is, $D_m^*(h)=I_f(h)=hf-fh$ for all $h\in R_{m-1}$), which implies $R_m=R_{m-1}[g]$. Conversely, if $R_m=R_{m-1}[Y]$ and $X_m=\sum Y_jf_j$ $(f_j\in R_{m-1})$ then, for $h\in R_{m-1}$, $D_m^*(h)=hX_m-X_mh=\sum Y^j(hf_j-f_jh)$, and whence $D_m^*(h)=hf_0-f_0h$, which implies that X_m-f_0 is a generator in R_m.

Definition 1.4. Let B be a ring extension of A with the common identity 1 and G a finite group of automorphisms of B. Then B is said to be a *G-Galois extension* of A if $A=B^G(=\{b\in B\,;\,\tau(b)=b$ for all $\tau\in G\})$, A_A is a direct summand of B_A and there exist elements r_i, s_i $(1\leqq i\leqq k)$ such that $\sum_{i=1}^k r_i\tau(s_i)=\delta_{1,\tau}$ for all $\tau\in G$ (cf. [10]). Moreover, a G-Galois extension B/A is called a *p^e-cyclic extension* if G is a cyclic group of order p^e.

Remark 1.5. Let $G=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_n)$ be an elementary abelian group of order p^n. Then, A has a G-Galois extension B if and only if there exist derivations $\{D_i\,;\,i=1,\cdots,n\}$ of A, a family $\mathscr{A}$ of elements in A which satisfy conditions (1)—(3) and there exist elements $\alpha_1,\cdots,\alpha_n$ of A such that $X_i^{\mathfrak{p}}-\alpha_i=X_i^p-X_i-\alpha_i$ is a generator in $R_n=A[X_1,\cdots,X_n\,;\,D_1,\cdots,D_n,\mathscr{A}]$ for $i=1,\cdots,n$. Moreover, if this is the case, B is isomorphic to the factor ring R_n/M, $M=(X_1^{\mathfrak{p}}-\alpha_1,\cdots,X_n^{\mathfrak{p}}-\alpha_n)$ and $\sigma_i(x_j)=x_j+\delta_{ij}$ where x_j is the coset of X_j and δ_{ij} is the Kronecker's delta (see [4, Corollary 2.1]). Hence we may write

$$B=\sum\oplus(x_1^{\nu_1}x_2^{\nu_2}\cdots x_n^{\nu_n})A\quad(0\leqq\nu_i\leqq p-1)$$

with $ax_i=x_ia+D_i(a)$ for $a\in A$, $x_ix_j=x_jx_i+a_{ij}$ and $x_i^{\mathfrak{p}}=\alpha_i\in A$.

Moreover, in this paper, we shall use the following conventions:

$$A_m=A[x_1,\cdots,x_m\,;\,D_1,\cdots,D_m,\{a_{ij}\,;\,1\leqq i,j\leqq m\}]\ (1\leqq m\leqq n)$$

which is a subring of B (as in Remark 1.5) generated by elements $x_1,\cdots,x_m$ over A.

$$A'_m=A[x_1,\cdot\cdot,x_{m-1},x_{m+1},\cdot\cdot,x_n\,;\,D_1,\cdots,D_{m-1},D_{m+1},\cdots,D_n,\{a_{ij}\,;\,i,j\neq m\}].$$

In case $a_{ij}=0$ $(1\leqq i,\ j\ \leqq m)$, abbreviate

$$A_m=A[x_1,\cdots,x_m\,;\,D_1,\cdots,D_m],$$

and further

$$R_m=A[X_1,\cdots,X_m\,;\,D_1,\cdots,D_m].$$

Remark 1.6. Let $R_n=A[X_1,\cdots,X_n\,;\,D_1,\cdots,D_n]$. Then, $X_i^{\mathfrak{p}}-\alpha(\alpha\in A)$ is a generator in R_n if and only if $\alpha\in A_0=\bigcap_{j=1}^n A^{D_j}$ and $I_\alpha=D_i^{\mathfrak{p}}=D_i^p-D_i$, where $A^{D_j}=\{a\in A\,;\,D_j(a)=0\}$ ([5, Theorem 2.1]).

Now, the rest of this section is devoted to generalize some results in [7] to the non-commutative case. These results are not only useful in our study, but also, interesting of themselves.

Definition 1.7. Let H be a group and N a normal subgroup of H. Then, we say that N is a *small subgroup* (abbreviate an s-subgroup) of H if $NH' \neq H$ for any proper subgroup H' of H.

If $H=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_n)$ is an abelian group with $|\sigma_i|=p^{e_i}$ (p is prime and $e_i \geqq 1$), then $N=(\sigma_1^p)\times(\sigma_2^p)\times\cdots\times(\sigma_n^p)$ is an s-subgroup of H. Moreover, if H is a finite p-group then the Frattini subgroup $\Phi(H)$ of H is an s-subgroup of H.

The following Lemma and Theorem are proved in [7] when the rings considered are commutative. But the validity of them can be shown by the same way for the non-commutative case. For the convenience of readers, we will prove them here again.

Lemma 1.8. *Let A be connected and let B/A be an H-Galois extension for a finite group H. If B is disconnected, then there exists a nontrivial idempotent $e \in C(B)$ such that $e\tau(e)=0$ or $\tau(e)=e$ for every $\tau \in H$.*

Proof. Let f be a nontrivial idempotent of $C(B)$. Then H-norm $N(f)$ is either 1 or 0. If $N(f)=1$, then f is invertible and this leads to a contradiction $f=1$. Thus $N(f)=0$. Let e be a product $\tau_1(f)\tau_2(f)\cdots\tau_r(f)$ of maximal length such that $e\neq 0$, and such that $\tau_i(f)'s$ are distinct. For an element τ of H, assume $e\tau(e)\neq 0$. Then each $\tau(\tau_i(f))$ appears among the $\tau_i(f)'s$ and so $\tau(e)=e$.

Theorem 1.9. *Let A be connected and let B/A be an H-Galois extension for a finite group H. If B^N is connected for an s-subgroup N of H, then B is connected.*

Proof. Suppose B is disconnected. For any idempotent e as in Lemma 1.8, we set $H'=\{\tau\in H\,;\,\tau(e)=e\}$. Choose $\tau_1,\cdots,\tau_s$ to be the right coset representatives in NH'/H'. Then all $\tau_i(e)$'s are distinct. Hence, for each pair $i\neq j$, we have $\tau_i^{-1}\tau_j(e)=\tau_k(e)\neq e$ for some k, and whence $e\tau_i^{-1}\tau_j(e)=0$ (Lemma 1.8), which implies $\tau_i(e)\tau_j(e)=0$. Therefore, $e'=\tau_1(e)+\cdots+\tau_s(e)$ is an idempotent which is fixed by N, and hence, e' is 1 or 0. If $e'=0$, then all $\tau_i(e)$'s are zero, a contradiction. Hence $e'=1$. It follows that $\{\tau_i(e)\,;\,i=1,\cdots,s\}$ is the full H-orbit of e. Since $\phi: H/H'\to NH'/H'$ such that $\phi(\sigma H')=\tau_i H'$ for $\sigma(e)=\tau_i(e)$ is a bijection, this means that $H'N=H$. Since N is an s-subgroup of H, we have $H'=H$, which is a contradiction.

2. Connected cyclic extensions. The purpose of this section is to give a necessary and sufficient condition for a connected ring A to have a connected p-cyclic extension and some related results.

The map $'$ defined in $R=A[X;D]$ by $g'(X)=\sum_{i=1}^{n} iX^{i-1}a_i$ for all $g(X)=\sum_{i=0}^{n} X^i a_i$, satisfies $(D^*(g(X))'=D^*(g'(X))$ and so is a derivation in R, where $D^*=I_X$.

Let $f(X)$ be a generator in R. Then $f(X)$ is contained in the commutative ring $C(A^D)[X]$ (cf. [1, Lemma 1.6]). Hence, if $f(X)$ is separable in $C(A^D)[X]$, then $f'(x)$ is invertible in $C(A^D)[x]\cong C(A^D)[X]/(f(X))$ ([7, Theorem 1]). Under these remarks we can prove the following

Lemma 2.1. *Let $f(X)=\sum_{i=0}^{n}(X^p)^i a_i$ be a generator in $R=A[X;D]$, and assume that $R/(f(X))$ is connected. Then*

(i) *A is connected.*

(ii) *If $f(X)$ is separable in $C(A^D)[X]$, then $f(X)$ is w-irreducible.*

Proof. (i) We set $B=A[x;D]=R/(f(X))$. Now let e be an idempotent of $C(A)$. Then $ea=ae$ for all $a\in A$. Hence $e\in C(B)$ if and only if $D(e)=ex-xe=0$. $D(e)=D(e^2)=2eD(e)$ implies $(2e-1)D(e)=0$. Multiplying by e, we have $eD(e)=0$ and so $D(e)=0$.

(ii) If $f(X)$ is separable in $C(A^D)[X]$ then $f'(x)=a_0$ is invertible in $C(A^D)$. Assume $f(X)$ is not w-irreducible. Then $f(X)=g(X)h(X)$ for some proper monic factors $g(X)$ and $h(X)$ which are generators. Hence $a_0=f'(X)=g(X)h(X)+g(X)h'(X)$ shows that $(g(X))+(h(X))=R$. Since $g(X)$ and $h(X)$ are central polynomials, $(g(X))(h(X))=(h(X))(g(X))$ and hence $(f(X))=(g(X))(h(X))=(g(X))\cap(h(X))$. Thus $R/(f(X))\cong R/(g(X))\oplus R/(f(X))$ is disconnected.

As is noted in Remark 1.5, a polynomial $X_i^p-a_i$ which is a generator in $R_n=A[X_1,\cdots,X_n;D_1,\cdots,D_n,\mathcal{A}]$ plays a key role to construct an abelian extension of A. In the following we shall give an important property of X^p-a.

Theorem 2.2. *Let A be connected. Then a generator $f(X)=X^p-a$ in $R=A[X;D]$ is either w-irreducible or a product of generators of degree* 1.

Proof. Suppose $f(X)$ is not w-irreducible. Then there exists a proper factor $g(X)$ of $f(X)$ which is a generator. Let $g(X)=X^n+\sum_{i=0}^{n-1}X^i a_i$. Then $n<p$ and $ag(X)=g(X)a$ for $a\in A$ implies $nD(a)=a_{n-1}a-aa_{n-1}$ ([1, Lemma 1.6]) and so D is inner. Hence we may assume that $R=A[X]$ and $X^p-a\in C(R)=C(A)[X]$. Hence X^p-a is reducible in $C(A)[X]$

and it is a product of linear factors which are generators by [7, Lemma 2.1].

Corollary 2.3. *Let $R=A[X;D]$. If D is outer then a generator $X^p-\alpha$ is w-irreducible.*

Now, in the rest of this section, B/A will mean a p-cyclic extension (cf. Definition 1.4). Then, by Remark 1.5, B is obtained by $A[X;D]/(X^p-\alpha)$ for some derivation D of A and a generator $X^p-\alpha$ in $R=A[X;D]$. Hence, we may write

$$B=A[x;D]=A[x;D/\alpha]=\textstyle\sum_{i=0}^{p-1}\oplus x^iA$$

where $x=X+(X^p-\alpha)$.

Lemma 2.4. *Let $B=A[x;D]$ and $f=\sum_{i=0}^{s} x^i a_i$ be an element of $V_B(A)$, the centralizer of A in B, where $1\leqq s\leqq p-1$ and $a_s\neq 0$. Then*

(i) *$a_s\in C(A)$, and $sD(a)a_s=a_{s-1}a-aa_{s-1}$ for all $a\in A$.*

(ii) *If a_s is invertible in A then D is inner.*

(iii) *If $f\in C(B)$ then $D(a_i)=0$ for all i.*

Proof. For any $a\in A$, we have

$$0=af-fa=x^s(aa_s-a_sa)+x^{s-1}(sD(a)a_s+aa_{s-1}-a_{s-1}a)+\textstyle\sum_{i=0}^{s-2} x^ic_i$$

where $c_i\in A$, $i=1,\cdots,s-2$. This implies (i). The other assertions will be be easily seen.

Now, let $A_0(D)=\{a\in A_0\,;\,I_a=D\}$ where $A_0=A^D$. Then $A_0(D)=C(A_0)(D)$, and $X-c$ is a generator in $R=A[X;D]$ if and only if $c\in A_0(D)$ (Remark 1.3). Moreover, let $A(D^p)=\{a\in A_0\,;\,I_a=D^p\}$. Then $A_0(D^p)=C(A_0)(D^p)$, and X^p-c is a generator in R if and only if $c\in A_0(D^p)$ (Remark 1.6). Further, we shall write $A_0(D)^p=\{a^p\,;\,a\in A_0(D)\}$.

Next, we shall prove the following theorem which is one of our main results.

Theorem 2.5. *Let A be connected. Then, for $B=A[x;D/\alpha]$, the following conditions are equivalent.*

(1) *B is connected.*

(2) *$X^p-\alpha$ is w-irreducible in R.*

(3) *$\alpha\in A_0(D^p)\backslash A_0(D)^p$.*

Proof. (1)⇒(2) is clear from Lemma 2.1(ii), and (2)⇔(3) is clear from Theorem 2.2.

(2)⇒(1). Let $e=\sum_{i=0}^{s} x^i a_i$ be an idempotent of $C(B)$, and assume that $1 \leqq s \leqq p-1$ and $a_s \neq 0$. Then e is a nontrivial idempotent in $C(B)$. Now, by Lemma 2.4, we have

(a) $D(a_i)=0$ for all i,

(b) $a_s \in C(A)^D$,

(c) $sD(a)a_s=a_{s-1}a-aa_{s-1}$ $(a \in A)$.

From (a), we see that

$$e^p=\sum_{i=0}^{s} (x^p)^i a_i^p=\sum_{i=0}^{s}(x+\alpha)^i a_i^p=e=\sum_{i=0}^{s} x^i a_i.$$

This implies $a_s^p=a_s$. Since X^p is separable in $C(A)[X]$ ([9, Lemma 2.1]) and $a_s^p=a_s \in C(A)$ (connected) by (b), it follows that $a_s \in \mathrm{GF}(p)$ and is invertible. Hence D is inner by (c). Thus we may assume that $R=A[X]$ and $C(B) \cong C(A)[X]/(X^p-\alpha)$. Since $X^p-\alpha$ is irreducible in $C(A)[X]$ (Remark 1.2), $C(B)$ is connected by [8, Theorem 1.6], a contradiction. Therefore, we obtain $e=a_0 \in C(A)$.

As a consequence of Theorem 2.5, we have

Corollary 2.6. *Let A be connected. Then A has a connected p-cyclic extension if and only if one of the following conditions* (a) *and* (b) *is satisfied.*

(a) $p \leqq (C(A):C(A)^p)$, *the index of the subgroup $C(A)^p$ in the additive group $(C(A),+)$.*

(b) *A has an outer derivation D such that $C(A_0)(D^p) \neq \emptyset$.*

Proof. First, we assume that A has a connected p-cyclic extension B. Then, there exists a derivation D of A and an element $\alpha \in A$ such that $X^p-\alpha$ is a w-irreducible generator in $R=A[X;D]$ (Remark 1.5 and Theorem 2.5). In this case, there holds $\alpha \in A_0(D^p)=C(A_0)(D^p)$ and $\alpha \notin A_0(D)^p$. If it is possible to choose D as inner, we may assume $D=0$ and so $A_0(D^p)$ $C(A)$ and $\alpha \in C(A)\backslash C(A)^p$. Since $\nu\alpha+C(A)^p$, $\nu=0,1,\cdots,p-1$, are distinct cosets in $C(A)/C(A)^p$, $(C(A):C(A)^p) \geqq p$. Conversely, if (a) is satisfied, then $C(A)$ has a connected commutative p-cyclic extension C ([8, Lemma 1.2 and Theorem 1.6]) and $B=A\otimes_{C(A)}C$ is a requested one. If (b) is satisfied, $A_0(D)=\emptyset$, and so $X^p-\alpha$ is w-irreducible for any $\alpha \in A_0(D^p)$ (Theorem 2.5).

A p-cyclic extension B/A is said to be *inner* (resp. *outer*) if its Galois group can be choosen as an inner automorphism group (resp. an outer automorphism group). In [5, Corollary 1.3], it is proved that if $B=A[x;D]$ is a p-cyclic extesnion of A, then B/A is inner if and only if there exists

Mathematical Journal of Okayama University, Vol. 25 [1983], Iss. 2, Art. 2

an elemet $c \in U = U(C(A))$, the group of invertible elements in $C(A)$, such that $D(c) = c$. Further, if $C(A)$ is a field and B/A is inner, then each A-automorphism of B is inner and $V_B(A) = C(A) \supsetneqq C(B)$ ([6, Theorem 1]). On the other hand, if $C(A)$ is a field and B/A is outer, then each A-automorphism of B is outer and $V_B(A) = C(B)$ ([6, Theorem 2]). Combining this with Corollary 2.6, we have the following

Corollary 2.7. (I) *Let A be connected. Then A has a connected inner p-cyclic extension if and only if there exists a derivation D of A such that*

(i) $A_0(D^p) \neq \emptyset$,

(ii) $D(U) \cap U \neq \emptyset$, *where* $U = U(C(A))$.

(II) *Let $C(A)$ be a field and $B = A[x;D]$ a connected p-cyclic extension. Then $C(B)$ is a field and further,*

(i) *B/A is outer if and only if $D(C(A)) = 0$,*

(ii) *B/A is inner if and only if $D(C(A)) \neq 0$.*

Proof. (I) Assume that A has a derivation D which satisfies (i) and (ii). Then D is outer by (ii). Hence, by Corollary 2.6, A has a connected p-cyclic extension $B = A[x;D]$. Further, by (ii), there exists an element $c \in U$ such that $D(c) \in U$. Then $c(xD(c)^{-1}c)c^{-1} = (cxc^{-1})$. $D(c)^{-1}c = xD(c)^{-1}c + 1$. Put $y = xD(c)^{-1}c$. Then $B = A[y\,; D(c)^{-1}cD]$ shows that B is an inner p-cyclic extension with a Galois group $(\tilde{c})$, a cyclic group generated by an inner automorphism $\tilde{c}(= c_l c_r^{-1})$. The converse is clear by [5, Corollary 1.3].

(II) If D is inner, then we may assume that $C(B) = C(A)\,[x]$ and so $C(B)$ is a field. On the other hand, if D is outer, then $C(B) \subseteqq V_B(A) \cap A = C(A)$ (by Lemma 2.4), which implies $C(B) = C(A)^D \subseteqq C(A)$. Finally, if B/A is outer, $C(B) \supseteqq C(A)$ and then $D(C(A)) = I_x(C(A)) = 0$. If B/A is inner then $C(A) \supsetneqq C(B)$ and hence $D(C(A) = I_x(C(A)) \neq 0$. This completes the proof of (II).

Let $J(A)$ be Jacobson radical of A. We say that A is a *quasi local ring* (resp. a *primary ring* (see [2, p.56]) if $A/J(A)$ is a two sided simple ring (resp. a simple artinian ring).

Let A be a two sided simple ring. Then each proper ideal of $R = A[X;D]$ is generated by a generator in R and an ideal of R is maximal if and only if it is generated by a w-irreducible polynomial (see [4, p. 76]).

Corollary 2.8. (I) *If A is a two sided simple ring* (*resp. a simple* *artinian ring) then, for $B=A[x;D/\alpha]$, the following conditions are equivalent.*

(1) *B is a two sided simple ring (resp. a simple artinian ring).*

(2) *B is connected.*

(3) *$X^p-\alpha$ is w-irreducible in R.*

(II) *If A is a quasi local ring (resp. a primary ring) with $D(J(A))\subseteqq J(A)$ then, for $B=A[x;D/\alpha]$, the following conditions are equivalent.*

(1) *B is a quasi local ring (resp. a primary ring).*

(2) *$B/J(B)$ is connected.*

(3) *$X^p-\bar{\alpha}$ is w-irreducible in $A/J(A)[X;\bar{D}]$ where $\bar{\alpha}$ is the coset of α modulo $J(A)$ and $\bar{D}$ is a derivation of $A/J(A)$ defined by $\bar{D}(\bar{a})=\overline{D(a)}$.*

Proof. (I) is clear from the above remark and Theorem 2.5.

(II) If $D(J(A))\subseteqq J(A)$ then $J(A)[x;D]=\{\sum_{i=0}^{p-1} x^i a_i\,;\, a_i\in J(A)\}$ is an ideal of B. Hence $J(B)=J(A)[x;D]$ by [10, Proposition 7.8] and $B/J(B)$ is a p-cyclic extension of $A/J(A)$ by [10, Theorem 5.6]. The rest is clear from (I).

Corollary 2.9. *Let A be a finite dimensional central simple algebra and $B=A[x;D]$ a connected p-cyclic extension of A. Then B/A is inner if and only if D is outer.*

Proof. If B/A is inner then D is outer by Corollary 2.7. Conversely, if D is outer then $D(C(A))\neq 0$. For, if $D(C(A))=0$ then D is an inner derivation of A ([2, Theorem 6.13.2]), a contradiction. Thus B/A is inner by Corollary 2.7.

Lemma 2.10. *Let $B=A[x;D]$ be a p-cyclic extension with a Galois group (σ). Then $T_\sigma(y)=\sum_{i=0}^{p-1}\sigma^i(y)=1$ for $y\in B$ if and only if $y=-x^{p-1}+f(x)$ for $f(x)=\sum_{i=0}^{p-2} x^i a_i$.*

Proof.
$$\begin{aligned}T_\sigma(x^i a)&=(x^i+(x+1)^i+\cdots+(x+p-1)^i)a\\ &=[px^i+\binom{i}{i-1}(x^{i-1}(1+\cdots+(p-1))+\cdots\\ &\quad+\binom{i}{j}x^j(1^{i-j}+\cdots+(p-1)^{i-j}+\cdots+(1^i+\cdots+(p-1)^i]a.\end{aligned}$$

Since $\{1,\cdots,p-1\}$ is a cyclic group generated by some element c, we see that, if $1\leqq s\leqq p-2$, then

$$\sum_{k=1}^{p-1} c^s=\sum_{k=0}^{p-2}(c^k)^s=\sum_{k=0}^{p-2}(c^s)^k=(1-(c^s)^{p-1})(1-c^s)^{-1}=0.$$

Hence $T_\sigma(x^i a)=\begin{cases}0 \text{ if } i\leqq p-2\\ -a \text{ if } i=p-1.\end{cases}$

This shows that $T_\sigma(y)=1$ if and only if $y=-x^{p-1}+\sum_{i=0}^{p-2} x^i a_i$.

Let B be a p^e-cyclic extension of A for a cyclic group (σ). If we put $\tau_i=\sigma^{p^i}$ $(i \leqq e)$ and $B_i=B^{\tau_i}$, then B_{i+1}/B_i is a p-cyclic extension with a cyclic group $(\tau_i \mid B_{i+1})$ such that B_i is a B_i-direct summand of B_{i+1}. Hence $B_{i+1}=B_i[x_{i+1}\,;\partial_i]$ for some derivation ∂_i of B_i and an element $x_{i+1}\in B_{i+1}$ such that $\tau_i(x_{i+1})=x_{i+1}+1$. A p^e-cyclic extension B of A is said to be a trivail extension if B is obtained by $C\otimes_{C(A)}A$ for some commutative p^e-cyclic extension C of $C(A)$. Hence B_{i+1}/B_i is a trivial extension if and only if ∂_i is inner. Then we have the following

Corollary 2.11. *Let A be connected.*

(i) *B is connected if and only if B_1 is connected.*

(ii) *B/A is a trivial extension if and only if B_{i+1}/B_i is a trivial extension for every i.*

Proof. (i) Since $B_1=B^{\tau_1}$ and (τ_1) is an s-subgroup of (σ), the connectedness of B_1 implies that of B by Theorem 1.9. The converse is also clear by Lemma 2.1.

(ii) It is clear that B/A is a trivial extension if each B_{i+1}/B_i is a trivial extension. To prove the converse, it is enough to prove that if ∂_i is inner, then ∂_{i-1} is also inner. Now, we assume that ∂_i is inner. Then $\partial_i=I_C$ for some $c\in B_i$. We write $y=x_{i+1}-c$, $x_i=x$, $\tau_i=\tau$ and $\tau_{i-1}=\rho$. Then $\tau(y)=y+1$ and $B_{i+1}=B_i[y]$ (that is, $y\in C(B_{i+1})$). Let $t=\rho(y)-y$. Then $t\in B_i$ since $\tau(\rho(y)-y)=\rho(y+1)-(y+1)=\rho(y)-y=t$, and further, $T_\rho(t)=\sum_{i=0}^{p-1}\rho^i(t)=\sum_{i=0}^{p-1}\rho^i(\rho(y)-y)=\tau(y)-y=1$. Hence $t=-x^{p-1}+\sum_{i=0}^{p-1}x^i d_i$ $(d_i\in B_{i-1})$ by Lemma 2.10 and $\rho(y)-y=t\in C(B_{i+1})\cap B_i=V_{B_i}(B_{i+1})\subseteqq V_{B_i}(B_{i-1})$. Hence, by Lemma 2.4, ∂_{i-1} is the inner derivation effected by $-d_{p-2}$.

As a direct consequence of Corollary 2.8 and Corollary 2.11, we obtain the following

Corollary 2.12. *When A is a two sided simple ring (resp. a simple artinian ring), B is a two sided simple ring (resp. a simple artinian ring) if and only if so is B_1.*

3. Connected Abelian extensions. Let $G=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_n)$ be an elementary abelian group of order p^n. In this section, we assume that B is a G-Galois extension. Hence $B=A[x_1,\cdots,x_n\,;D_1,\cdots,D_n,\mathcal{A}]=\sum\oplus(x_1^{\nu_1}x_2^{\nu_2}\cdots x_n^{\nu_n})A$

with $x_i^p = a_i \in A$, $ax_i = x_i a + D_i(a)$ for $a \in A$ and $x_i x_j = x_j x_i + a_{ij}$. Unless otherwise stated, B means one which is obtained by the free A-basis $\{x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}\,;\, 0 \leqq \nu_i \leqq p-1\}$, and as to notations A_k, etc., we follow Remark 1.5 and others.

The following lemma is easy to obtain by induction, using Lemma 2.1 and Corollary 2.7(2).

Lemma 3.1. *If B is connected then A_k is connected, and if $C(A)$ is a field then $C(A_k)$ is a field for $0 \leqq k \leqq n$.*

It is clear that the converse of Lemma 3.1 is not true. For this reason, the main interest of this section is to study sufficient conditions for B to be connected.

In virtue of Theorem 2.5, we can easily see that if $X_i^p - a_i$ is w-irreducible in $A_i'[X_i\,;\,D_i^*]$ for $i = 1, \cdots, n$, then B is connected. Now we shall study some types of intermediate subrings of B/A which depend on properties of derivations D_i's.

Let S_n be the set of all permutations of $\{1, \cdots, n\}$ and for $\pi \in S_n$, let $A_{\pi(k)}$ be a subring of B generated by elements $x_{\pi(1)}, \cdots, x_{\pi(k)}$ over A. Then, there exists an element $\pi \in S_n$ and $m \geqq 0$ such that $D_{\pi(i)}^*$ is inner (resp. outer) in $A_{\pi(i-1)}$ for each $i \leqq m$, and for each $\nu \in S_n$, $D_{\nu(j)}^*$ is not inner (resp. outer) in $A_{\nu(j-1)}$ for some $1 \leqq j \leqq m+1$ (cf. Remark 1.0 and Remark 1.5).

For the inner (resp. outer) case, we set

$$\mathcal{I} = \{D_{\pi(1)}, \cdots, D_{\pi(m)}\} \text{ (resp. } \mathcal{O} = \{D_{\pi(1)}, \cdots, D_{\pi(m)}\}).$$

Then, $\mathcal{I}$ (resp. $\mathcal{O}$) will be called a maximal inner (resp. outer) subset of $\{D_1, \cdots, D_n\}$ over A. Moreover, we denote $A_{\pi(m)}$ by $A(\mathcal{I})$ (resp. $A(\mathcal{O})$). Clearly, $\mathcal{I}$ (resp. $\mathcal{O}$) might be $\emptyset$, or not $\emptyset$, and it seems that $\mathcal{I}$ (resp. $\mathcal{O}$) does not determine uniquely. As to our study, we shall distiguish two cases.

Case 1. D_i is inner for some i.

In this case, there is a maximal inner subset $\mathcal{I}_1$ of $\{D_1, \cdots, D_n\}$ over A which is not empty. Next, let $\mathcal{O}_1$ be a maximal outer subset of $\{D_1, \cdots, D_n\} \backslash \mathcal{I}_1$ over $A(\mathcal{I}_1)$. Clearly $\mathcal{I}_1 \neq \{D_1, \cdots, D_n\}$ if and only if $\mathcal{O}_1 \neq \emptyset$. We shall now write

$$A(\mathcal{I}_1, \mathcal{O}_1) = A(\mathcal{I}_1)\ (\mathcal{O}_1).$$

If $\mathcal{I}_1 \cup \mathcal{O}_1 \neq \{D_1, \cdots, D_n\}$ then we can see

$$B = A(\mathcal{I}_1, \mathcal{O}_1)\ (\mathcal{I}_2, \mathcal{O}_2) \cdots (\mathcal{I}_k, \mathcal{O}_k)$$

for some k by repetition of this procedure, where $\mathscr{I}_k \neq \emptyset$.

Case 2. Each D_i is outer.

In this case, there is a maximal outer subset $\mathcal{O}'_1$ of $\{D_1,\cdots,D_n\}$ over A which is not empty. Next, let $\mathscr{I}'_1$ be a maximal inner subset of $\{D_1,\cdots,D_n\}\backslash\mathcal{O}'_1$ over $A(\mathcal{O}'_1)$, and we write

$$A(\mathcal{O}'_1,\mathscr{I}'_1)=A(\mathcal{O}'_1)\ (\mathscr{I}'_1).$$

If $\mathcal{O}'_1 \cup \mathscr{I}'_1 \neq \{D_1,\cdots,D_n\}$ then we can see

$$B=A(\mathcal{O}'_1,\mathscr{I}'_1)\ (\mathcal{O}'_2,\mathscr{I}'_2)\cdots(\mathcal{O}'_h,\mathscr{I}'_h)$$

for some h by repetition of this procedure, where $\mathcal{O}'_h \neq \emptyset$.

Now, in the rest of this section, we shall write as folows:

In Case 1, $\mathscr{I}_1=\{D_1,\cdots,D_{m_1}\}$, $\mathcal{O}_1=\{D_{m_1+1}\cdots,D_{m_1+n_1}\},\cdots$.

In Case 2, $\mathcal{O}'_1=\{D_1,\cdots,D_{m_1}\}$, $\mathscr{I}'_1=\{D_{m_1+1},\cdots,D_{m_1+n_1}\},\cdots$.

If $m_1 < n$ then, it is obvious that in Case 1 (resp. in Case 2), D_j^* is outer (resp. inner) in A_{m_1} for $j=m_1+1,\cdots,n$, and $A_{q_1}=A(\mathscr{I}_1,\mathcal{O}_1)$ (resp. $A_{q_1}=A(\mathcal{O}'_1,\mathscr{I}'_1)$) for $q_1=m_1+n_1$.

Lemma 3.2. *Let D_1 be inner.*

(i) *If D_j^* is inner A_1 then D_j is inner.*

(ii) *In case $D_1=0$, D_j^* is inner in A_1 if and only if D_j is inner and $x_jx_1=x_1x_j$.*

Proof. Let $D_1=I_c$. Then, for $y=x_1-c$, we have $A_1=A[y]$. Now, we assume that D_j^* is inner in A_1. Then, there exists an element $f=\sum_{i=0}^{p-1} y^i a_i$ ($a_i\in A$) in A_1 such that $D_j^*(g)=gf-fg$ for all $g\in A_1$. Since y is central in A_1, it follows that $A\ni D_j(a)=D_j^*(a)=aa_0-a_0a$ for all $a\in A$. Clearly $D_j^*(x_1)=D_j(c)$. Hence, if, in particular, $c=0$ (that is $D_1=0$) then $x_jx_1=x_1x_j$. The rest of the assertions will be easily seen.

Lemma 3.3. (i) *Let $A_{q_1}=A(\mathscr{I}_1,\mathcal{O}_1)$. Then we may assume $D_i=0$, $a_i\in C(A)$ for $i=1,\cdots,m_1$ and $A_{q_1}=A[x_1,\cdots,x_{m_1},x_{m_1+1},\cdots,x_{m_1+n_1}\,;D_{m_1+1},\cdots,D_{m_1+n_1},\{a_{ij}\}]$ where $ax_i=x_ia$, $x_ix_j=x_jx_i$ for $i,j \leqq m_1$, $ax_j=x_ja+D_j(a)$ and $x_ix_j=x_jx_i+a_{ij}$ for $j > m_1$.*

(ii) *Let $A_{q_1}=A(\mathcal{O}'_1,\mathscr{I}'_1)$. Then we may assume $D_i^*=0$ in A_{i-1} for $i=m_1+1,\cdots,m_1+n_1$ and $A_{q_1}=A[x_1,\cdots,x_{m_1},y_{m_1+1},\cdots,y_{m_1+n_1}\,;D_1,\cdots,D_{m_1},\{a_{ij}\}]$ where $ax_i=x_ia+D_i(a)$, $x_ix_j=x_jx_i+a_{ij}$ for $i,j \leqq m_1$, $y_j=x_j-f_j$ for $f_j\in A_{m_1}$ such that $y_j\in C(A_{q_1})$ and $y_j^p\in C(A_{m_1})$.*

Proof. (i) $A_{m_1}=A[x_1,\cdots,x_{m_1}]$ is clear from Lemma 3.2 and the rest can be easily seen.

(ii) Replace A by $A_{m_1}=A(\mathcal{O}_1')$. Then we can see the assertion by the same reason as in (i).

In what follows, let A_{q_1} be as follows:

i) If $A_{q_1}=A(\mathcal{I}_1,\mathcal{O}_1)$ then

$$A_{q_1}=A[x_1,\cdots,x_{m_1},x_{m_1+1},\cdots,x_{m_1+n_1}\,;\,D_{m_1+1},\cdots,D_{m_1+n_1},\{a_{ij}\}],$$

where $x_i^p=a_i\in C(A)$, $i=1,\cdots,m_1$.

ii) If $A_{q_1}=A(\mathcal{O}_1',\mathcal{I}_1')$ then

$$A_{q_1}=A[x_1,\cdots,x_{m_1},y_{m_1+1},\cdots,y_{m_1+n_1}\,;\,D_1,\cdots,D_{m_1},\{a_{ij}\}],$$

where $y_j=x_j-f_j\in C(A_{q_1})$ for $f_j\in A_{m_1}$ and $y_j^p=a_j-f_j^p\in C(A_{m_1})$. Moreover, a derivation D of A is said to be *completely outer* if cD is outer for all nonzero $c\in C(A)$. If $C(A)$ is a field then any outer derivation of A is completely outer.

Lemma 3.4. *If $B=A[x_1,\cdots,x_n\,;\,D_1,\cdots,D_n]$ and each outer derivation among $\{D_1,\cdots,D_n\}$ is completely outer, then B is either $A(\mathcal{I}_1,\mathcal{O}_1)$ or $A(\mathcal{O}_1')$. More precisely, $\mathcal{I}_1$ is the set of all inner derivations and $\mathcal{O}_1$ is the set of all outer derivations among $\{D_1,\cdots,D_n\}$.*

Proof. Since $\mathcal{A}=\{0\}$, $\mathcal{I}_1$ is the set of all inner derivations in $\{D_1,\cdots,D_n\}$ by Lemma 3.2. Suppose that there exists D_j such that $D_j\notin\mathcal{I}_1\cup\mathcal{O}_1$. Then D_j is outer and D_j^* is inner in A_{q_1}. Hence $D_j^*=I_f$ for $f=\sum x_{q_1}^{\nu_{q_1}}\cdots x_1^{\nu_1}a_{\nu_{q_1}\cdots\nu_1}$. Then $A\ni D_j(a)=af-fa$ implies $a_{(p-1)\cdots(p-1)}\in C(A)$ and $(p-1)D_{q_1}(a)a_{(p-1)\cdots(p-1)}=a_{(p-2)(p-1)\cdots(p-1)}a-aa_{(p-2)(p-1)\cdots(p-1)}$. Since $D_{q_1}^*$ is outer in A_{m_1}, D_{q_1} is outer. Further since D_{q_1} is completely outer, $a_{(p-1)(p-1)\cdots(p-1)}$ must be 0 and hence $a_{(p-2)(p-1)\cdots(p-1)}\in C(A)$. Then, by the same way, we have $(p-2)D_{q_1}(a)\cdot a_{(p-2)(p-1)\cdots(p-1)}=a_{(p-3)(p-1)\cdots(p-1)}a-aa_{(p-3)(p-1)\cdots(p-1)}$. Repeating this, we can see $\nu_{q_1}=\nu_{q_1-1}=\cdots=\nu_{m_1+1}=0$. Consequently, $f\in A_{m_1}$ and D_j^* is inner in A_{m_1}, a contradiction. Thus $\mathcal{O}_1$ is the set of all outer derivations in $\{D_1,\cdots,D_n\}$.

Lemma 3.5. (i) *Let $A_{q_1}=A(\mathcal{I}_1,\mathcal{O}_1)$. If A_{q_1} is connected then $(C(A_{m_1})^p\cap A)/C(A)^p$ is an m_1-dimensional* GF(p)*-space with a basis $\{a_i+C(A)^p\,;\,i=1,\cdots,m_1\}$.*

(ii) *Let $A_{q_1}=A(\mathcal{O}_1',\mathcal{I}_1')$. If A_{q_1} is connected then $(C(A_{q_1})^p\cap A_{m_1})/C(A_{m_1})^p$ is an n_1-dimensional* GF(p)*-space with a basis $\{a_i-f_i^p+C(A_{m_1})^p\,;\,i=m_1+1,\cdots,m_1+n_1\}$.*

Mathematical Journal of Okayama University, Vol. 25 [1983], Iss. 2, Art. 2

Proof. (i) Let $f \in C(A_{m_1})$ and $f^p \in A$. First, we shall prove that

$$f = \sum_{i=1}^{m_1} x_i \mu_i + c \text{ for some } \mu_i \in \mathrm{GF}(p) \text{ and } c \in C(A).$$

Now, we set $m_1 = r$ and assume that $f = \sum_{i=1}^{s} x_r^i a_i$ where $a_i \in A_{r-1}$, $a_s \neq 0$ and $2 \leqq s \leqq p-1$. Then $a_i \in C(A_{r-1})$ for $i=0, 1, \cdots, s$ and

$$f^p = \sum_{i=0}^{s} (x_r + \alpha_r)^i a_i^p - \sum_{i=0}^{s} x_r^i a_i.$$

Hence we obtain $a_s^p = 0$ and $s\alpha_r a_s^p = (-a_{s-1})^p$. Since A_{q_1} is connected, A_r is connected by Lemma 3.1. Then, noting $a_s^p = 0$, we have $a_s \in \mathrm{GF}(p)$, and whence $\alpha_r = (-a_{s-1} s^{-1} a_s^{-1})^p$. This implies that $X_r^p - \alpha_r$ is reducible in $C(A_{r-1})[X_r]$, a contradiction. Hence, it follows that $f = x_r a_1 + a_0$. Clearly $a_1^p = 0$ and so, $a_1 = \mu_r \in \mathrm{GF}(p)$. Moreover $f^p - (x_r \mu_r)^p = a_0^p \in A \cap C(A_{r-1})^p$. Therefore, by induction methods, we obtain $f = \sum_{i=1}^{m_1} x_i \mu_i + c$ for $\mu_i \in \mathrm{GF}(p)$ and $c \in C(A)$. Now, noting $x_i^p = \alpha_i$, we have $f^p = \sum_{i=1}^{m_1} \alpha_i \mu_i + c^p$. Clearly $C(A_{m_1})^p \supset C(A)^p$ and they are $\mathrm{GF}(p)$-modules. Since $\alpha_i \in C(A_{m_1})^p \cap A$, it follows that

$$(C(A_{m_1})^p \cap A)/C(A)^p = \sum_{i=1}^{m_1} (\alpha_i + C(A)^p)\mathrm{GF}(p).$$

If $\alpha_i = \alpha_1 \nu_1 + \dots \alpha_{i-1}\nu_{i-1} + \alpha_{i+1}\nu_{i+1} + \dots + \alpha_{m_1}\nu_{m_1} + c^p (\nu_i \in \mathrm{GF}(p)$ and $c^p \in C(A)^p)$ then $X_i^p - \alpha_i$ has a factor $X_i - (x_1\nu_1 + \cdots + x_{i-1}\nu_{i-1} + x_{i+1}\nu_{i+1} + \cdots + x_{m_1}\nu_{m_1} + c)$ which is a generator in $A[x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{m_1}][X_i]$. But this is a contradiction since A_{m_1} is connected by Lemma 3.1.

(ii) Since $A_{q_1} = A_{m_1}[y_{m_1+1}, \cdots, y_{m_1+n_1}]$, we can see the validity of the assertion by the same way as in (i) by replacing A to A_{m_1}.

Theorem 3.6. *Let A be connected.*

(I) *If $B = A(\mathcal{I}_1, \mathcal{O}_1)$, then the following conditions are equivalent.*

(1) *B is connected.*

(2) *$\{\alpha_i + C(A)^p ; i = 1, \cdots, m_1\}$ is linearly independent over $\mathrm{GF}(p)$ in $C(A)/C(A)^p$.*

(II) *If $B = A(\mathcal{O}_1', \mathcal{I}_1')$, then the following conditions are equivalent.*

(1) *B is connected.*

(2) *$\{\alpha_i - f_i^p + C(A_{m_1})^p ; i = m_1+1, \cdots, m_1+n_1\}$ is linearly independent over $\mathrm{GF}(p)$ in $C(A_{m_1})/C(A_{m_1})^p$.*

Proof. (I) (1)⇒(2). Since $C(A_{m_1})^p \cap A \subset C(A)$, this is clear from Lemma 3.5(i).

(2)⇒(1). Let A_{k-1} be connected for $k \leqq m_1$. If $X_k^p - \alpha_k$ is reducible in $C(A_{k-1})[X_k]$, then there exists $f \in C(A_{k-1})$ such that $f^p = \alpha_k (\in A)$, and so $f = x_1\mu_1 + \dots + x_{k-1}\mu_{k-1} + c$ by making use of the same methods as in the proof of Lemma 3.5 (i), where $\mu_i \in GF(p)$ and $c \in C(A)$. Hence $f^p = a_k = a_1\mu_1 + \ldots + a_{k-1}\mu_{k-1} + c^p$ and this contradicts to the linear independence of $\{a_i + C(A)^p ; i=1,\cdots,m_1\}$. Thus A_k is connected. By inductive argument, we can see that A_{m_1} is connected. Since $A_{m_1}[x_{m_1+1} : D^*_{m_1+1}]/A_{m_1}$ is a (σ_{i+1})-cyclic extension and $D^*_{m_1-1}$ is outer in A_{m_1}, $A_{m_1+1} = A_{m_1}[x_{m_1+1} ; D^*_{m_1+1}]$ is connected by Corollary 2.3. Repeating this we can see the connectedness of B.

(II) This can be prove by the similar way as in (I).

Lemma 3.7. *If $C(A)$ is a field and B is connected then B is either $A(\mathscr{I}_1,\mathscr{O}_1)$ or $A(\mathscr{O}'_1)$.*

Proof. If D^*_j is inner in A_1, then D_j is inner. For, if D_1 is inner, it follows from Lemma 3.2. On the other hand, if D_1 is outer, it is a consequence of the fact that D_1 is completely outer. Since $C(A_k)$ is a field by Lemma 3.1, continuing this way, we can see that $\mathscr{I}_1$ is the set of all inner derivations and $\mathscr{O}_1$ is the set of all outer derivations in $\{D_1,\cdots,D_n\}$(cf. the proof of Lemma 3.4).

Combining Theorem 3.6 with Lemma 3.7, we have the following

Corollary 3.8. *Let $C(A)$ be a field. Then A has a connected G-Galois extension B such that $\mathscr{A}=\{0\}$ if and only if one the following conditions* (a) *and* (b) *is satisfied.*

(a) *There exist outer derivations $D_{m_1},\cdots,D_{m_1+n_1}$ of A and elements $a_i \in A$ $(i=1,\cdots,n)$ such that*

(1) $[D_i,D_j]=0$.

(2) $a_1,\cdots,a_{m_1} \in C(A)_0$ *and* $\{a_i + C(A)^p ; i=1,\cdots,m_1\}$ *is linearly independent over* $GF(p)$ *in* $C(A)/C(A)^p$.

(3) $a_j \in A^{D_j}(D^p_j)$ *for* $j > m_1$.

(b) *There exist outer derivations $D_1,\cdots,D_n$ and elements $a_i \in A$ $(i=1,\cdots,n)$ such that*

(1) $[D_i,D_j]=0$,

(2) $a_i \in A^{D_i}(D^p_i)$ *for all* $i,j=1,\cdots,n$.

Proof. If B is a connected G-Galois extension such that $\mathscr{A}=\{0\}$, then $B=A(\mathscr{I}_1,\mathscr{O}_1)$ or $A(\mathscr{O}'_1)$ by Lemma 3.4. Thus we can easily see that A satisfies conditions (a) or (b) by Theorem 3.6. Conversely, if A satisfies (b), then $B=A[X_1,\cdots,X_n ; D_1,\cdots,D_n] / (X^p_1 - a_1,\cdots,X^p_n - a_n)$ is a G-Galois extension of A and $X^p_i - a_i$ is w-irreducible in A'_i. While, if A satisfies (a), then $B=A[X_1,\cdots,X_{m_1},X_{m_1+1},\cdots,X_n\,;D_{m_1+1},\cdots,D_n]/(X_1^p-\alpha_1,\cdots,X_n^p-\alpha_n)$ is a G-Galois extension of A such that A_{m_1} is connected by Theorem 3.6. Since D_j^* is outer in A_{j-1} by Lemma 3.4, this means that B is connected.

Corollary 3.9. *Let A be a two sided simple ring (resp. a simple artinian ring) and B a G-Galois extension of A. Then B is a two sided simple ring (resp. a simple artinian ring) if and only if B is connected, and if this is the case, B is either $A(\mathscr{I}_1,\mathcal{O}_1)$ or $A(\mathcal{O}_1')$.*

Proof. By Corollary 2.8, B is a two sided simple ring (resp. a simple artinian ring) if and only if B is connected. The rest is clear from Lemma 3.7.

Corollary 3.10. *Let $H=(\tau_1)\times(\tau_2)\times\cdots(\tau_n)$ be an abelain group such that $|\tau_i|=p^{e_i}$ $(e_i\geqq 1)$, B/A an H-Galois extension and $T=B^{G'}$ for $G'=(\tau_1^p)\times(\tau_2^p)\times\cdots\times(\tau_n^p)$.*

(i) *Let A be connected. Then B is connected if and only if so is T.*

(ii) *Let A be a two sided simple ring (resp. a simple artinian ring). Then B is a two sided simple ring (resp. a simple artinian ring) if and only if so is T.*

Proof. Since G' is an s-subgroup of H, these are direct consequences of Theorem 1.9 and Corollary 3.9.

4. Connected p-extensions. In this section, we will deal with the connectedness of a G-Galois extension over a connected ring A when G is a nonabelian p-group of order p^e. Thus we assume here B/A is a G-Galois extension and $T=B^{\Phi(G)}$ where $\Phi(G)$ is the Frattini subgroup of G which is an s-subgroup of G (cf. Definition 1.7). Then we can readily see the following

Theorem 4.1. (i) *Let A be connected. Then B is connected if and only if so is T.*

(ii) *Let A be a two sided simple ring (resp. a simple artinian ring). Then B is a two sided simple ring (resp. a simple artinian ring) if and only if so is T.*

Proof. By Theorem 1.9, B is connected if so is T. Conversely, assume B is connected, $\Phi(G)=G_0\supsetneqq G_1\supsetneqq\cdots\supsetneqq G_t=\{1\}$ is a composition series of $\Phi(G)$ and $B_i=B^{G_i}$. Then B_i/B_{i-1} is a p-cyclic extension and so the connectedness of $B=B_t$ implies that of $T=B_0$ by Lemma 3.1. This completes the proof of (i).

Since $H=G/\Phi(G)$ is an elementary abelian group and T/A is a connected H-Galois extension, T is two sided simple if so is B by Corollary 3.9. The converse is an immediate conseqeunce of Corollary 2.8.

Let C be a central subgroup of order p of G which is contained in $\Phi(G)$ and let P be a p-group which is isomorphic to G/C. If all rings considered are supposed commutative, then a P-Galois extension M/A can be embedded into a G-Galois extension B/A ([7] and [11]). In the following we shall give a necessry and sufficient condition for M/A can be embedded into B/A in general case.

Let $C=(\sigma)$. Then as same as in [11], we choose representatives $u(\tau) \in G$ for $\tau \in P$. Define the group cohomology of 2-cocycles $g(\tau,\rho)$ by

$$u(\tau)u(\rho)=g(\tau,\rho)u(\tau\rho).$$

$u(\tau)\sigma=\sigma u(\tau)$ is clear for $\tau \in P$ since C is central.

Let $\chi: C \to \mathrm{GF}(p)$ be the homomorphism defined by $\chi(\sigma^i)=i$. $\chi(g(\tau,\rho))$ is a 2-cocycle of P into $\mathrm{GF}(p)$.

For a derivation D of M, we put $\Delta_0(u)=1$ and $\Delta_i(u)=D(\Delta_{i-1}(u))+\Delta_{i-1}(u)u$ for $u \in M$.

Under these notations, we have the following

Theorem 4.2. *Let M/A be a P-Galois extension. Then M/A can be embedded into a G-Galois extension B/A if and only if there exist a derivation D of M, elements $t \in M^D$ and $t_\tau \in M$ $(\tau \in P)$ such that*

(1) $D^p=I_t$,

(2) $[\tau,D]=I_{t_\tau}\cdot\tau$,

(3) $t_\tau+\tau(t_\rho)=t_{\tau\rho}+\chi(g(\tau,\rho))$,

(4) $T_\tau(t_\tau)=\sum_{i=0}^{|\tau|-1}\tau^i(t_\tau)=\chi(g)$ *where* $g \in C$ *such that* $u(\tau)^{|\tau|}=g$,

(5) $(\tau-1)(t)=\Delta_p(t_\tau)-t_\tau$ *for* $\tau \in P$.

Proof. Let B/A be a G-Galois extension. Then $B^C=M$. Since B possessess an element $y \in B$ such that $T_G(y)=1$ (since $B_A \oplus > A_A$), we can see that $T_C(T_P(y))=1$. Hence B/M is a C-Galois extension with $B_M \oplus > M_M$. Therefore there is an element $x \in B$ such that $\{1,x,\cdots,x^{p-1}\}$ is a free M-basis for B, $x^p=t \in M$ and $\sigma(x)=x+\chi(\sigma)$.

Let c be an arbitrary element of M. Then $\sigma(I_x(c))=\sigma(cx-xc)=c\sigma(x)-\sigma(x)c=I_x(c)$ shows that $D=I_x|M$ is a derivation of M satisfying (1).

Let $u(\tau)(x)=\sum x^i c_{i\tau}$ for $c_{i\tau}\in M$. Since $\sigma u(\tau)=u(\tau)\sigma$, $\sum(x+1)^i c_{i\tau}$ $=\sigma u(\tau)(x)=u(\tau)\sigma(x)=\sum x^i c_{i\tau}+1=u(\tau)(x)+1=u(\tau)(x)-x+\sigma(x)$, and whence, $u(\tau)(x)=x+t_\tau$ for some $t_\tau\in M$.

$$\begin{aligned}[\tau,D]\,(c)&=\tau(cx-xc)-(\tau(c)x-x\tau(c))=u(\tau)\,(cx-xc)-(\tau(c)x-x\tau(c))\\&=\tau(c)\,(x+t_\tau)-(x+t_\tau)\tau(c)-(\tau(c)x-x\tau(c))\\&=\tau(c)t_\tau-t_\tau\tau(c)+I_t\,.\tau(c).\end{aligned}$$

Since $u(\tau)u(\rho)=g(\tau,\rho)u(\tau\rho)$, $x+t_\tau+\tau(t_\rho)=u(\tau)\,(x+t_\rho)=u(\tau)u(\rho)\,(x)$ $=g(\tau,\rho)u(\tau\rho)(x)=g(\tau,\rho)(x+t_{\tau\rho})=x+t_{\tau\rho}+\chi(g(\tau,\rho))$ and $x+T_\tau(t_\tau)=u(\tau)^{|\tau|}(x)$ $=g(x)=x+\chi(g)$ shows that $t_\tau+\tau(t_\rho)=t_{\tau\rho}+\chi(g(\tau,\rho))$ and $T_\tau(t_\tau)=\chi(g)$ for $g=u(\tau)^{|\tau|}$.

Noting that $(x+t_\tau)^p=x^p+\Delta_p(t_\tau)$([5, p. 163]), $t+\Delta_p(t_\tau)-t_\tau=x^p+\Delta_p(t_\tau)$ $-t_\tau=x^p+\Delta_p(t_\tau)-(x+t_\tau)=u(\tau)\,(x^p)=\tau(t)$ means that $(\tau-1)\,(t)=\Delta_p(t_\tau)$ $-t_\tau$.

Conversely, assume that there exist a derivation D, elements t and t_τ $(\tau\in P)$ which satisfy the conditions (1)–(5).

By (1), X^p-t is a generator in $R=M[X;D]$. Let $B=R/(X^p-t)$ and let x be the coset of X. We define the action of σ on B by

$$\sigma(\sum x^i c_i)=\sum (x+\chi(\sigma))^i c_i \ (c_i\in M).$$

Then $\sigma(x^p)=(x^p+\chi(\sigma)^p)=x^p=t=\sigma(t)$ and $\sigma(cx)=\sigma(xc+D(c))=xc+\chi(\sigma)c$ $+D(c)=c(x+\chi(\sigma))=\sigma(c)\sigma(x)$. This shows that σ acts on B as an M-automorphism of order p.

Next we extend $u(\tau)$ $(\tau\in P)$ to an automorphism of B by

$$u(\tau):\sum x^i r_i\to\sum (x+t_\tau)^i\tau(r_i)\ (r_i\in M).$$

Then $u(\tau)\,(x^p)=x^p+\Delta_p(t_\tau)-t_\tau=t+\Delta_p(t_\tau)-t_\tau=u(\tau)\,(t)$ by (5) and $u(\tau)\,(rx)$ $=u(\tau)\,(xr+D(r))=(x+t_\tau)\tau(r)+\tau D(r)=x\tau(r)+\tau(r)t_\tau+D\tau(r)=\tau(r)\,(x+t_\tau)=$ $\tau(r)\tau(x)$ by (2). Thus τ is a ring homomorphism of B. Moreover $u(\tau)^{|\tau|}$ $(x)=x+T_\tau(t_\tau)=x+\chi(g)$ by (4), and whence $g^p(x)=x$. Thus $u(\tau)$ acts as an automorphism on B and $u(\tau)\,|\,M=\tau$. $\sigma u(\tau)=u(\tau)\sigma$ is clear and $u(\tau)u(\rho)\,(xr)=(x+t_\tau+\tau(t_\rho))\tau\rho(r)=(x+t_{\tau\rho}+\chi(g(\tau,\rho))\tau\rho(r)=g(\tau,\rho)u(\tau\rho)(xr)$ show that $u(\tau)u(\rho)=g(\tau,\rho)u(\tau\rho)$. Now it is clear that $A\subseteqq B^G\subseteqq M^G\subseteqq$ $M^P=A$.

Let $\{y_i,z_i\,;\,i=1,\cdots,n\}$ and $\{u_i,v_i\,;\,i=1,\cdots,m\}$ be a (σ)-Galois coordinate system for B/M and a P-Galois coordinate system for M/A respectively. Then $\sum_i y_i(\sum_j u_j\tau\sigma^k(v_j))\tau\sigma^k(z_i)=\delta_{1,\tau\sigma^k}$ for all $\tau\sigma^k\in G=\bigcup_\tau \tau(\sigma)$, where τ runs over all the elements of a complete representatives of G modulo (σ).

Noting that C is an s-subgroup of G, we have the following

Corollary 4.3. *Let A be connected and B/A a G-Galois extension. Then the following conditions are equivalent.*

(1) *B is connected.*

(2) *M is connected.*

(3) *T is connected.*

REFERENCES

[1] S. IKEHATA: On separable polynomials and Frobenius polynomials in skew polynomial rings, Math. J. Okayama Univ 22 (1980), 115—129.

[2] N. JACOBSON: Structure of Rings, Amer. Math. Soc. Colloq. Publ. 37, Rev. Ed., Providence, 1968.

[3] G.J. JANUSZ: Separable algebras over commutative rings, Trans. Amer. Math. Soc., 122 (1966), 461—479.

[4] K. KISHIMOTO: On cyclic extensions of simple rings, J. Fac. Sci. Hokkaido Univ. 19 (1966), 74—85.

[5] K. KISHIMOTO: On abelian extensions of rings I, Math. J. Okayama Univ. 14 (1970), 159—174.

[6] K. KISHIMOTO: Note on cyclic extensions of rings, J. Fac. Sci. Shinshu Univ. 5 (1970), 29—32.

[7] K. KISHIMITO: On p-extensions of an algebra of characteristic p, to appear in J. Algebra.

[8] T. NAGAHARA and A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ. 15 (1971), 81—90.

[9] T. NAGAHARA: Characterization of separable polynomials over a commutative rings, Proc. Japan. Acad. 46 (1970), 1011—1015.

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

[11] D.J. SALTMAN: Noncrossed product p-algebra and Galois p-extensions, J. Algebra, 52 (1978), 302—314.

INSTITUTO DE MATEMATICA
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY

(*Received April 28, 1983*)