Hokkaido Mathematical Journal Vol. 20 (1991) p. 123-133

On P-Galois extensions of rings of cyclic type

Dedicated to Professor Tosiro Tsuzuku on his 60th birthday

Kazuo KISHIMOTO

(Received August 31, 1989)

§ 1. A relative sequence of homomorphisms P and a P-Galois extension.

Let B be a ring with an identity 1 and A a subring of B with common identity 1 of B. In [6], the author studied on a relative sequence of homomorphisms P of $End(B_A)$ and a P-Galois extension B/A. In this paper we shall study on constructive P-Galois commutative extensions of cyclic type as an application of the works of [6].

For the convenience of readers, we shall summarized notions and several properties of a relative sequence of homomorphisms P and a P-Galois extension. The details and proofs will be seen in [6].

Let $P=\{D_0=1, D_1, \cdots, D_n\}$ be a finite subset of $End(B_A)$ and let P be a poset with respect to the order $\leq$. For D_i and D_j in P, $D_i \gg D_j$ means that D_i is a cover of D_j, that is, $D_i > D_j$ and no $D_k \in P$ such that $D_i > D_k > D_j$.

$P(min)$ (resp. $P(max)$) is the set of all minimal (resp. maximal) elements of P.

For $D_i \in P$, a chain of D_i means a descending chian in P such that
$D_i = D_{i_0} \gg \ldots\ldots \gg D_{i_m}$, $D_{i_m} \in P(min)$,
and $m+1$ is said to be the length of the chain.

(I) P is said to be a relative sequence of homomorphisms if it satisfies the following conditions (A. 1)-(A. 4) and (B. 1)-(B. 4):

(A. 1) $D_i \neq 0$ for all $D_i \in P$ and $P(min)$ coincides with all $D_i \in P$ such that D_i is a ring automorphism.

(A. 2) The length of each chain of D_i is unique and denotes it by $ht(D_i)$.

(A. 3) $D_iD_j \in P$ if $D_iD_j \neq 0$ and if $D_iD_j=0$ then $D_jD_i=0$.

(A. 4) Assume D_iD_j and D_iD_k are in P.

(i) $D_iD_j \geq D_iD_k$ (*resp.* $D_jD_i \geq D_kD_i$) if and only if $D_j \geq D_k$.

(ii) If $D_iD_j \geq D_m$ then $D_m = D_sD_t$ for some $D_s \leq D_i$ and $D_t \leq D_j$.

(B. 1) $D_i(1)=0$ for any $D_i \in P-P(min)$.

Let $D_i \in P$. Then there exists $g(D_i, D_j) \in End(B_A)$ for each $D_j \leq D_i$ such that

(B. 2) $D_i(xy)=\sum_{D_j} g(D_i, D_j)(x)D_j(y)$ for $x, y \in B$ where the sum runs over all D_j such that $D_j \leq D_i$.

(B. 3) Let $x, y \in B$.

(i) $g(D_i, D_j)(xy)=\sum_{D_k} g(D_i, D_k)(x)g(D_k, D_j)(y)$ where the sum runs over all D_k such that $D_j \leq D_k \leq D_i$.

(ii) Let $D_i > D_j$ and $D_jD_k \geq D_h$. Then $g(D_i, D_j)(x)g(D_jD_k, D_h)(y)= g(D_i, D_j)(x)\sum_{D'_j, D'_k} g(D_j, D'_j)(x)g(D_k, D'_k)(y)$ where the sum runs over all D'_j and D'_k such that $D'_jD'_k=D_h$.

(B. 4) (i) $g(D_i, D_i)$ is a ring automorphism.

(ii) $g(D_i, \Lambda)=D_i$ for any minimal Λ of P.

(iii) $g(D_i, D_k)(1)=0$ if $D_k < D_i$.

Since $P(min)$ is a finite multiplicative semigroup which is contained in the group of automorphisms of B, it forms a group.

A relative sequence of homomorphisms $P=\{D_0=1, D_1, \dots, D_n\}$ is said to be cyclic if $D_i=(D_1)^i$ for $i=1, 2, \dots, n$ and $D^i \geq D^j$ for $i \geq j$.

For the covenience, elements of P are some times denoted by Capital Greek.

The sum of all $\Delta_j \in P(max)$ is denoted by Δ and for $\Omega \in P$, $g(\Delta_j, \Omega)$ is the sum of all $g(\Delta_j, \Omega)$ such that $\Delta_j \geq \Omega$.

For $P(min)$, $B_1=B^{P(min)}=\{b \in B\,;\Omega(b)=b$ for all $\Omega \in P(min)\}$ and $B^P=B_1 \cap B_0$ where $B_0=\{b \in B\,;\Omega(b)=0$ for all $\Omega \in P-P(min)\}$.

(II) Assume a relative sequence of homomorphisms P satisfies the condition

(A. 5) $|P(min)|=|P(max)|$.

Then B/A is said to be a P-Galois extension if

(g. 1) $B^P=A$

(g. 2) There exists a system $\{x_i, y_i\,; i=1, 2, \dots, s\} \subseteq B$ such that $\sum_{i=1}^{s} x_i g(\Delta, \Omega)(y_i)=\delta_{1,\Omega}$ where $\delta_{1,\Omega}$ is the Kronecker's delta.

If P is cyclic then P satisfies (A. 5) since $|P(min)|=1=|P(max)|$, and in this case, a P-Galois extension B/A is said to be cyclic.

The system $\{x_i, y_i\,; i=1, 2, \dots, s\} \subseteq B$ which satisfies (g. 2) is said to be a P-Galois system for B/A.

Let $D(B, P)=\sum_{\Omega \in P} \oplus Bu_\Omega$ be a free left B-module with a B-basis $\{u_\Omega\,; \Omega \in P\}$. Then $D(B, P)$ forms a ring by the multiplication $(bu_\Omega)(cu_\Gamma)= b\sum_{\Lambda \leq \Omega} g(\Omega, \Lambda)(c)(u_{\Lambda\Gamma}$ where $u_{\Lambda\Gamma}=0$ if $\Lambda\Gamma=0$ (Theorem 2.2 [6].

Then the map j of $D(B, P)$ to $End(B_A)$ defined by

$$j(u_\Omega b)(x)=\Omega(bx) \text{ for } x\in B$$

is a ring homomorphism.

Assume a relative sequence of homomorphisms P satsifies the condition (A. 6). For each maximal element Δ_j, if $\Delta_j\geq\Omega$ then there exists $\Omega'\in P$(resp. Ω'') such that $\Delta_j=\Omega'\Omega$(resp. $\Delta_j=\Omega\Omega''$).

Then, under the assumption that $B^P=A$, (g. 2) is equivalent to (g. 2') B_A is a finitely generated projective module and j is an isomorphism (Theorem 3.8 [6].

In the rest of this paper, we assume that a relative sequence of homomorphisms satisfies (A. 5) and (A. 6).

(III) Let $P=P(min)$ (and hence $P=P(max)$). Then P is a finite group of automorphisms of B, and $g(\Delta, \Omega)=g(\Omega, \Omega)=\Omega$ by (B. 3), (iii). Hence the existence of a P-Galois system $\{x_i, y_i\,;\, i=1, 2, \dots, S\}$ means the existence of that of $\sum_{i=1}^{s} x_i\Omega(y_i)=\delta_{1,\Omega}$. Consequently, a P-Galois extension means a Galois extension of separable type which is studied in [2], [3] and the others.

Let B/A be a P-Galois extension. Then $B_A\oplus>A_A$, A_A is a direct summand of B_A, if and only if there exists $x\in B$ such that

$\Delta(x)=1$ (Theorem 3.3 [6]).

If B is commutative then $B_A\oplus>A_A$.

(IV) Let $P(min)=\{1\}$ and $P(max)=\{\Delta\}$. If B is commutative and $B^P=A$, then B/A is a P-Galois extension if and only if there exists a system $\{x_i, y_i\,;\, i=1, 2, \dots, s\}\subseteq B$ such that $\sum_{i=1}^{s}\Omega(x_i)y_i=\delta_{\Delta,\Omega}$, and if this is the case, $B=\sum_{i=1}^{s}Ay_i$.

Moreover, the existence of such a system $\{x_i, y_i\,;\, i=1, 2, \dots, s\}$ is equivalent to the existence of an element $x_\Omega\in B$ for each $\Omega\in P$ such that

(i) $\Omega(x_\Omega)=1$,
(ii) $\Gamma(x_\Omega)\neq 0$ if and only if $\Lambda\Gamma=\Omega$ for some $\Lambda\in P$
(iii) If $\Lambda\Gamma=\Omega$ then $\Gamma(x_\Omega)=x_\Lambda$ (Theorem 6.6 and Corollary 5.8 [6]).

Hereafter, we assume that all ring considered are commutative.

§ 2. Cyclic *P*-Galois extensions.

In this section we assume that $P=\{D^0=1, D, D^2, \dots, D^{p-1}\}$ is a cyclic relative sequence of homomorphisms of $End(B_A)$. Thus P is a linearly ordered set with $P(min)=\{1\}$ and $P(max)=\{D^{p-1}\}$. Moreover,

$$D(xy)=g(D, D)(x)D(y)+g(D, 1)(x)y$$
$$=g(D, D)(x)D(y)+D(x)y \text{ for } x,\ y\in B$$

shows that D is a $g(D, D)$-derivation of B.

The purpose of this section is to determine the structure of B when B is a P-Galois extension over A.

REMARK: Let A be an algebra of prime characteristic p and let σ be an A-automorphism of B of order p. Then $D=\sigma-1$ is a σ-derivation, $P=\{D^0=1, D, D^2, \ldots, D^{p-1}\}$ forms a cyclic relative sequence of homomorphisms and a P-Galois extension is a σ-cyclic extension which is studied in [4] and [7].

R is said to be a p-extension of A if $R\cong A[X]/(f(X))$ for some monic polynomial $f(X)=X^p-X\alpha-\beta(\alpha, \beta\in A)$ of degree p. Hence if R is a p-extension of A then it can be written
$R=A[x]=A\oplus xA\oplus x^2A\oplus\ldots\oplus x^{p-1}A$ and $x^p=x\alpha+\beta$ for some α, $\beta\in A$.

In the rest we assume that $P=\{D^0=1, D, D^2, \ldots, D^{p-1}=\Delta\}$ such that $Dg(D, D)=g(D, D)D$.

THEOREM 2.1. *Let A be an algebra over a prime field $GF(p)$ of prime characteristic p and let B be an extension ring of A. Then B/A is a P-Galois extension for some P if and only if $B=A[x]=\sum_{i=0}^{p-1}\oplus x^iA$ is a p-extension with $x^p=x\alpha+\beta$ for α, $\beta\in A$ and $\alpha\in A^{p-1}=\{a^{p-1}; a\in A\}$. More precisely, if this is the case,*

(i) *$g(D, D)(x)=x+c$ for some $c\in A$ and $c^{p-1}=\alpha$,*
(ii) *$D^k(x^k)=k!$ for $1\leq k\leq p-1$.*

PROOF. Assume B/A is P-Galois extension. Since $B_A\oplus>A_A$, there exists an element $w\in B$ such that $\Delta(w)=1$. Then $x=D^{p-2}(w)$ is a requested one. $D(g(D, D)(x)-x)=g(D, D)(D(x))-D(x)=1-1=0$ shows that

$$g(D, D)(x)-x=c\in B^P=A\ldots\ldots\ldots(*)$$

For this x, $D(x^2)=g(D, D)(x)D(x)+D(x)x=g(D, D)(x)+x=2x+c$. Hence we can see that

$$D(x^k)=\sum_{i=0}^{k-1}\binom{k}{i}x^ic^{k-1-i} \text{ by induction on } k. \text{ Thus,}$$
$$D(x^p)=c^{p-1}.$$

Since $D(x^p-xc^{p-1})=0$,

$$x^p-xc^{p-1}=\beta\in B^P=A\ldots\ldots\ldots(**)$$

Further, since $D^2(x^2)=2\,!$, we can see

$$D^k(x^k)=k\,!\,.........(***)$$

for $1\leq k\leq p-1$ by induction on k.
Since

$$D^j(x^{p-1})\cdot 1+D^j(x^{p-2}/(p-2)\,!)\cdot D^{p-2}(x^{p-1})=\begin{cases}1 \text{ if } D^j=\Delta\\ 0 \text{ if } D^j=D^{p-2},\end{cases}$$

we assume that there exist elements $u_1, u_2, \dots, u_t$ and $v_1, v_2, \dots, v_t$ of B such that $\sum_{i=1}^{t}\Omega(u_i)v_i=\delta_{\Delta,\Omega}$ for all $\Omega=D^j$, $j=k+1, \dots, p-1$ and each u_i, v_i are contained in $A[x]$. Then

$$\begin{aligned}&\textstyle\sum_{i=1}^{t} D^i(u_i)v_i-D^j(x^k/k\,!)\sum_{i=1}^{t} D^j(u_i)v_i\\ &=\begin{cases}1 \text{ if } j=p-1\\ 0 \text{ if } j=k,\ k+1, \dots, k-2.\end{cases}\end{aligned}$$

Thus there exists a system $\{u_i, v_i\,; i=1, 2, \dots, s\}$ such that $\sum_{i=1}^{s}\Omega(u_i)v_i=\delta_{\Delta,\Omega}$ for all $\Omega\in P$ and each u_i, $v_i\in A[x]$. Then $B=\sum_{i=0}^{p-1} x^iA$ by (IV) and (**)

Next, we shall show that $\{1, x, x^2, \dots, x^{p-1}\}$ is linearly independent over A. If $z=\sum_{i=0}^{p-1} x^ia_i=0$ $(a_i\in A)$, then $0=\Delta(z)=(p-1)\,!\,a_{p-1}$ by (***) and this means that $a_{p-1}=0$. Repeating this way we can see that $a_i=0$ for $i=0, 1, 2, \dots, p-1$. Consequently, we can see that B is a p-extension such that

$$B=A[x]=\textstyle\sum_{i=0}^{p-1}\oplus x^iA \text{ with } x^p=xc^{p-1}+d \text{ for } c,\ d\in A,$$

and further, this x satisfies (i) and (ii) by (*) and (**).

Conversely, assume that $B=A[x]=\sum_{i=0}^{p-1}\oplus x^iA$ is a p-extension such that $x^p=xc^{p-1}+d$ for c, $d\in A$. Then the map σ of a polynomial ring $A[X]$ over A defined by $\sigma(X)=x+c$ gives an A-automorphism *of* $A[X]$. Further the map D of $A[X]$ defined by (*i*) $D(Xa)=a$ for $a\in A$, (*ii*) $D(X^ka)=(\sigma(X)D(X^{k-1})+D(X)X^{k-1})a$ and (*iii*) $D(\sum_{i=0}^{k} X^ia_i)=\sum_{i=0}^{k} D(X^i)a_i$ gives a σ-derivation of $A[X]$. For, assume $D(X^k)=\sigma(X^i)D(X^{k-i})+D(X^i)X^{k-i}$ for all $k\leq n$ and $i\leq k$. Then

$$\begin{aligned}D(X^{n+1})&=\sigma(X)D(X^n)+X^n\\ &=\sigma(X)(\sigma(X^{i-1})D(X^{n+1-i})+D(X^{i-1})X^{n+1-i})+X^n\\ &=\sigma(X^i)D(X^{n+1-i})+(\sigma(X)D(X^{i-1})+X^{i-1})X^{n+i-1}\\ &=\sigma(X^i)D(X^{n+1-i})+D(X^i)X^{n+1-i}.\end{aligned}$$

Thus D is a σ-derivation. Since $D(X^p)=c^{p-1}$, $D(X^p-Xc^{p-1}-d)=0$ and this shows that D induces a σ-derivation of $A[X]/(X^p-Xc^{p-1}-d)\cong B$.

We denote it again by D. Then $P=\{D^0=1, D, D^2, \dots, D^{p-1}=\Delta\}$ is a relative sequence of homomorphism for B/A such that $P(min)=\{1\}$, $P(max)=\{\Delta\}$ and $Dg(D, D)=g(D, D)D$.

Let $z=\sum_{i=0}^{p-1} x^i a_i \in B^P (a_i \in A)$. Then $0=\Delta(z)=\sum_{i=0}^{p-1}\Delta(x^i)a_i=(p-1)!\, a_{p-1}$ yields $a_{p-1}=0$. Repeating the same way, we can see that $z=a_0$. Thus, $B^P=A$. Since $\Delta(x^{p-1})=(p-1)!=-1$, $x_{(Dj)}=D^{p-1-j}(x^{p-1})$ satisfies (i), (ii) and (iii) of (IV). Thus B/A is a P-Galois extension by (IV).

COROLLARY 2.2. *Let A be an algebra over $GF(p)$ and let $B=A[x]=\sum_{i=0}^{p-1}\oplus x^i A$ be a P-Galois extension over A such that $x^p=xc^{p-1}+d$ for some c, $d\in A$ and $D(x)=1$. Then*

(1) *A $g(D, D)$-derivation $g(D, D)-1$ is obtained by cD.*

(2) *$B^{g(D,D)}=\{b\in B\,;\, g(D, D)(b)=b\}=A$ if and only if c is a regular element (i. e, c is non-zero-divisor). In particular c is a unit element if and only if B/A is a $g(D, D)$-cyclic extension.*

(3) *$B^{g(D,D)}\supset A$ (i, e., A is a proper subset of $B^{g(D,D)}$) if and only if c is a zero divisor. In particular if c is nilpotent then there exists a positive integer k such that $B^{p^k}=\{b^{p^k}\,;\, b\in B\}\subseteq A$.*

(4) *$g(D, D)=1$ if and only if $c=0$. Moreover, if this is the case, $B^p\subseteq A$.*

PROOF. (1) $g(D,D)-1=cD$ if and only if $(g(D, D)-1)(x^i a)=cD(x^i a)$ for $a\in A$ and $0\le i\le p-1$. Since $(g(D, D)-1)(xa)=ca=cD(xa)$, we can easily see $(g(D, D)-1)x^i a)=cD(x^i a)$ by induction on i.

(2) Let c be regular and let $y=\sum_{i=0}^{p-1} x^i a_i\in B^{g(D,D)}$. Then $0=(g(D, D)-1)(y)=\sum_{i=0}^{p-1}(x+c)^i a_i-\sum_{i=0}^{p-1} x^i a_i$ yields $\binom{p-1}{p-2} ca_{p-1}=0$. Since c is regular, this means that $a_{p-1}=0$. Repeating this way, we can easily see that $y=a_0$, and hence $B^{g(D,D)}=A$. Conversely, assume that $B^{g(D,D)}=A$. If $ca=0$ for some $a(\neq 0)\in A$, then $g(D, D)(xa)=(x+c)a=xa$ shows that $xa\in A$ and this contradicts to linear independence of $\{1, x, x^2, \dots, x^{p-1}\}$.

Let c be a unit. Then $g(D, D)(y)=y+1$ for $y=xc^{-1}$. Moreover we can see that $B=\sum_{i=0}^{p-1}\oplus y^i A$ and $y^p=y+d$ for some $d\in A$. Thus B/A is a $g(D, D)$-cyclic extension, and the converse is also true [see [4]].

(3) $B^{g(D,D)}\supset A$ if and only if c is a zero divisor by (2). Since $D(x^s)=\sum_{i=0}^{s-1}\binom{s}{i} x^i c^{s-1-i}$ (see the proof of Theorem 2.1), $D(x^{p^t})=c^{p^t-1}$ for some $t\ge 1$. If c is nilpotent, we may assume $(c^{p-1})^{p^k}=0$ for some $k\ge 0$. Then $x^{p^{k+1}}=(x^p)^{p^k}=d^{p^k}$ shows that $B^{p^{k+1}}\subseteq A$.

(4) Since $g(D, D)(x)=x+c$, $g(D, D)=1$ if and only if $c=0$. Further

if this is the case, $x^p=d$ shows that $B^p \subseteq A$.

REMARK: (i) If A is an algebra over $GF(2)$, and B is a 2-extension of A, then $B=A[x]=A\oplus xA$ with $x^2=xc+d$ for some $c, d\in A$. Hence any 2-extension of A is a P-Galois extension by Theorem 2.1.

(ii) Let $B=A[x]=\sum_{i=0}^{p-1}\oplus x^iA$ be a p-extension such that $x^p=xc^{p-1}+d$. Corollary 2.2 of (2) shows that if c is a regular element but not a unit element then B/A is a P-Galois extension but not a $g(D, D)$-cyclic extension though $B^{g(D,D)}=A$.

In the rest we assume that $p>2$ is a prime and K is a field of characteristic p or of 0 and K contains a primitive $p-1$ the root ζ of 1 if the characteristic is 0. Further A is an algebra over K.

Let $C=A[y]=\sum_{i=0}^{p-2}\oplus y^iA$ be a ring with $y^{p-1}=c\in A$ (and hence, $A[y]\cong A[Y]/(Y^{p-1}-c)$). For a primitive $p-1$ th root ζ of 1 of K, we define two maps τ and E of C as follows:

$$\tau(\textstyle\sum_{i=0}^{p-2} y^ia_i)=\sum_{i=0}^{p-2}(y\zeta)^ia_i,$$
$$E(ya)=a,\ E(y^ka)=(\tau(y)E(y^{k-1})+E(y)y^{k-1})a \text{ and}$$
$$E(\textstyle\sum_{i=0}^{p-2} y^ia_i)=\sum_{i=0}^{p-2} E(y^ia_i)(a_i,\ a\in A).$$

Then τ is an A-automorphism of order $p-1$. Further, we have the following

LEMMA 2.3. *E is a τ-derivation of C such that*

(i) $E(y^k)=y^{k-1}(\zeta^{k-1}+\zeta^{k-2}+\dots\dots+\zeta+1)$

(ii) $E^i\begin{cases}=0 \text{ if } i=p-1\\ \neq 0 \text{ if } 0\leq i\leq p-2\end{cases}$

(iii) $E^k(y^k)=(\zeta+1)(\zeta^2+\zeta+1)\cdots(\zeta^{k-1}+\zeta^{k-2}+\dots\dots+\zeta+1)$ *for* $2\leq k\leq p-2$.

(iv) $E\tau=\tau E\zeta$.

PROOF. By the same way as in the proof of Theorem 2.1, we have $E(y^k)=\tau(y^i)E(y^{k-i})+E(y^i)y^{k-i}$ for $0\leq i\leq k$. Since $E(y^2)=\tau(y)+y=y(\zeta+1)$, we can easily see that $E(y^k)=y^{k-1}(\zeta^{k-1}+\zeta^{k-2}+\dots+\zeta+1)$ by induction on k. Further $E(y^{p-1})=y^{p-2}(\zeta^{p-2}+\zeta^{p-3}+\dots+\zeta+1)=0=E(c)$ shows that E is well-defined and is a τ-derivation. This proves (i).

Since any element of C is obtained by $\sum_{i=0}^{p-2} y^ia_i(a_i\in A)$, (ii) is clear by (i).

By induction on k, we can easily see (iii).

$E\tau(y^k)=E(y^k)\zeta^k=y^{k-1}(\zeta^{k-1}+\zeta^{k-2}+\dots+\zeta+1)\zeta^k$ and $\tau E\zeta(y^k)=\tau(E(y^k))\zeta=y^{k-1}\zeta^{k-1}(\zeta^{k-1}+\zeta^{k-2}+\dots+\zeta+1)\zeta$ for each $0\leq k\leq p-2$ shows that $E\tau=\tau E\zeta$

For $1\leq k\leq p-2$, we put $\eta_k=\zeta^k+\zeta^{k-1}+\cdots+\zeta+1$.

THEOREM 2.4. *Let C be an extension ring of A. Then C/A is a Q-Galois extension for some $Q=\{E^0=1, E, E^2, \ldots, E^{p-2}\}$ with $Eg(E, E)=g(E, E)E\zeta$ if and only if C is isomorphic to $A[Y]/(Y^{p-1}-c)$ for some $c\in A$.*

PROOF. Assume $C=A[y]=A\oplus\cdots\oplus y^{p-2}A$ with $y^{p-2}=c$. Then $Q=\{E^0=1, E, \ldots, E^{p-2}\}$ is a relative sequence of homomorphisms of C/A where E is a τ-derivation which is discussed in Lemma 2.3 and so $E\tau=\tau E\zeta$.

Let $\alpha=\sum_{i=0}^{p-2} y^i a_i\in C^E$. Then $0=E^{p-g}(\alpha)=a_{p-2}\eta_{p-3}\eta_{p-4}\cdots\eta_1$ shows that $a_{p-2}=0$. Repeating this way, we have $C^E=A$. For each $E^j=\Omega$, $y_\Omega=y^j/(\eta_1\eta_2\cdots\eta_{j-1})$ satisfies the conditions (i), (ii) and (iii) of (IV), and so C/A is a Q-Galois extension by (IV) again.

Conversely, assume that C/A is a Q-Galois extension. Since $C_A\oplus> A_A$, there exists $w\in C$ such that $E^{p-2}(w)=1$. Put $y=E^{p-3}(w)$. Then $E(y)=1$. Since $Eg(E, E)=g(E, E)E\zeta$, $E(g(E, E)(y)-y\zeta)=g(E, E)E(y\zeta)-E(y\zeta)=\zeta-\zeta=0$, and hence, $g(E, E)(y)-y\zeta=a\in C^E=A$. Then $g(E, E)(y+a/(\zeta-1))=(y+a/(\zeta-1))\zeta$. We denote this $y+a/(\zeta-1)$ by y again. Then $g(E, E)(y)=y\zeta$ and $E(y)=1$.

Let $\Omega=E^j$, $y_\Omega=y^j/\eta_1\eta_2\cdots\eta_{j-1}$ and $\Gamma=E^i$. Then $\Omega(y_\Omega)=1$ and $\Gamma(y_\Omega)\neq 0$ if and only if $i\leq j$, that is, $\Omega=\Gamma\Lambda$ where $\Lambda=E^{j-i}$. Further if this is the case, $\Gamma(y_\Omega)=y^{j-i}(\eta_{j-i}\eta_{j-i+1}\cdots\eta_{j-1})=y_\Lambda$. Thus y_Ω satisfies the conditions (i), (ii) and (iii) of (IV), and so $C=\sum_{j=0}^{p-2} y^jA$ by (IV). Let $\alpha=\sum_{j=0}^{p-2} y^j a_j=0$. Then $0=E^{p-2}(\alpha)=a_{p-2}(\eta_1\eta_2\cdots\eta_{p-3})$ implies $a_{p-2}=0$. Repeating this way we can obtain $a_{p-2}=a_{p-3}=\cdots=a_1=a_0=0$. Thus $\{1, y, y^2, \ldots, y^{p-2}\}$ is a linearly independent A-basis for C. Since $E(y^{p-1})=y^{p-2}\eta_{p-2}=0$, $y^{p-1}=c$ for some $c\in A$. Thus C is isomorphic to $A[Y]/(Y^{p-1}-c)$.

COROLLARY 2.5. *Let $C=A\oplus yA\oplus\cdots\oplus y^{p-2}A$ be a Q-Galois extension with $y^{p-1}=c\in A$, where $Q=\{E^0=1, E, E^2, \ldots, E^{p-2}\}$ and E is a τ-derivation such that $E\tau=\tau E\zeta$, Then*

(i) $C^{g(E,E)}=A$

(ii) *If c is a unit element then C/A is a $g(E, E)$-strongly cyclic extension.*

(iii) *If A is of prime characteristic p and c is nilpotent, then there exists a positive integer k such that $C^{p^k}\subseteq A$.*

PROOF. (i) Let $z=\sum_{i=0}^{p-2} y^i a_i \in C^{g(E,E)}$. Then $0=g(E, E)(z)-z=\sum_{i=0}^{p-2} y^i(\zeta^i a_i - a_i)$ implies $z\in A$.

(ii) This is proved in [5].

(iii) Since c is nilpotent, y is also nilpotent. Hence there exists an integer k such that $y^{p^k}=0$. Since $C=\sum_{i=0}^{p-2}\oplus y^i A$, $C^{p^k}=A^{p^k}\subseteq A$.

§ 3. Embedding of p-extensions.

Let A be an algebra over $GF(p)$ again. As is stated in Theorem 2.1, a p-extension $B\cong A[X]/(X^p - X\alpha - \beta)$ is a P-Galois extension over A for some $P=\{D^0=1, D, D^2, \dots, D^{p-1}\}$ if and only if $\alpha\in A^{p-1}$. Then it is natural to ask that whether a p-extension B/A can be embedded into an S-Galois extension T/A for some relative sequence of homomorphisms S. It seems like an open problem. But we can see that B/A can be embedded into such T/A that $T^S=A$ and T_A is finitely generated projective for some finite set S of $End(T_A)$ where T^S means $\{t\in T\,;\Lambda(t)=t$ for all $\Lambda\in S_a$, the set of all ring automorphism in $S\}\cap\{t\in T\,;\Omega(t)=0$ for all $\Omega\in S-S_a\}$.

Let $B=A[x]=\sum_{i=0}^{p-1}\oplus x^i A$ be a p-extension with $x^p=xc+d$ and let $C=A[y]=\sum_{j=0}^{p-2}\oplus y^i A$ be a Q-Galois extension with $y^{p-1}=c$ which is given in Theorem 2.4.

Let $T=B\otimes_A C=\sum_{i=0,j=0}^{p-1,p-2}\oplus(x^i\otimes y^j)A$. For the covenience, we denote $x^i\otimes y^j$ by $x^i y^j$. Hence $T=\sum_{i=0,j=0}^{p-1,p-2}\oplus x^i y^j A=\sum_{i=0}^{p-1}\oplus x^i C=\sum_{j=0}^{p-2}\oplus y^j B$.

Let σ be the map of T defined by $\sigma(\sum_{i=0}^{p-1} x^i c_i)=\sum_{i=0}^{p-1}(x+y)^i c_i (c_i\in C)$. Since $\sigma(x^p)=(x+y)^p=x^p+y^p=xc+d+yc=\sigma(xc+d)$, σ is well-defined and a C-automorphism of order p. For this σ the map D of T defined by

(i) $D(C)=0$ and $D(xd)=d$

(ii) $D(x^k d)=((\sigma(x)D(x^{k-1})+D(x)x^{k-1})d$

(iii) $D(\sum_{i=0}^{p-1} x^i d_i)=\sum_{i=0}^{p-1} D(x^i)d_i$, where d, $d_i\in C$

becomes a σ-derivation of T, and $P=\{D^0=1, D, \dots, D^{p-1}=\Delta_D\}$ is a relative sequence of homomorphisms with $P(max)=\{\Delta_D\}$ and $T^P=C$. Further, $x_{(D^k)}=x^k/k!$ satisfies the conditions (i), (ii) and (iii) of (IV). Therefore T/C is a P-Galois extension.

Next, an automorphism τ and a τ-derivation E of C which are discussed in Lemma 2.3 can be extended to that of T by $\tau(\sum_{j=0}^{p-1} y^j b_j)=\sum_{j=0}^{p-2}\tau(y)^j b_j$ and $E(\sum_{j=0}^{p-2} y^j b_j)=\sum_{j=0}^{p-2} E(y^j)b_j$ for $b_j\in B$, and T/B is a $Q=\{E^0=1, E, E^2, \dots, E^{p-2}=\Delta_E\}$-Galois extension.

Let $F(i, j)$ be $D^i E^j$ for $0\le i\le p-1$ and $0\le j\le p-2$. By S we denote the set of all nonzero finite products of $F(i, j)$, that is, $S=\{\prod_{s=1}^m F(i_s, j_s)\,; m\ge 1\}-\{0\}$. Then we have the following theorem.

THEOREM 3.1. *S is a finite set and $T^S=A$.*

PROOF. $F(i, j)(x^k y^h)=D^i(x^k)E^j(y^h)=\sum_{h=0}^{k-i} x^h c_h$, $c_h\in C=A[y]$ shows that $F(i_1, j_1)F(i_2, j_2)\cdots F(i_n, j_n)=0$ if $i_1+i_2+\cdots+i_n\geq p$. Hence if $F(i_1, j_1)F(i_2, j_2)\cdots F(i_m, j_m)\neq 0$ then it must be $i_1+i_2+\cdots+i_m\leq p-1$ and $j_k<p-1$ for all $k=1, 2, \dots, m$. Thus S must be a finite set. Since $S_a=\{1\}$, $T^S=A$ is clear.

Let $B=A[X]/(X^p-Xc-d)$ and let c be a unit element. Then B/A can be embedded into an S-Galois extension T/A for some $S=S(min)$ since B/A is strongly separable ([1]). As a corollary to Theorem 3.1, we can show that a non-abelian group of the order p^2-p can be choose as S if $p>2$. For, let $C\cong A[Y]/(Y^{p-1}-c)$ and let $T=B\otimes_A C=\sum_{i=0,j=0}^{p-1,p-2}\oplus x^i y^j A$. (Note that y is a unit element since so is c). As is seen in the begining of this section, $\sigma: x^i y^j \Longrightarrow (x+y)^i y^j$ and $\tau: x^i y^j \Longrightarrow x^i(y\nu)^j$, where $\nu\in GF(p)$ is a primitive $p-1$ th root of 1, are automorphisms of T respectively, and further, T/C is a σ-cyclic extension and T/B is a τ-cyclic extension. Put $z=xy^{-1}$. Then $T=\sum_{i=0}^{p-1}\oplus z^i C$, $\sigma(z)=z+1$ and $\tau(z)=z\nu^{-1}$. Hence $\sigma^\nu\tau(z^i y^j)=\sigma^\nu(z^i y^j \nu^{j-1})=(z+\nu)^i y^j \nu^{j-1}$ and $\nu\sigma(z^i y^j)=\tau(z+a)^i y^j)=(z\nu^{-1}+1)^i y^j \nu^j=(z+\nu^i y^j \nu^{j-i}$ show that $\sigma^\nu\tau=\tau\sigma$. Therefore $S=(\sigma, \tau)=\{\sigma^i\tau^j; i=0, 1, \dots, p-1$ and $j=0, 1, \dots, p-2\}$ is a non-abelian group of the order p^2-p and $T^S=A$. Let $\{x_i, y_i; i=1, 2, \dots, t\}$ be a σ-Galois system for T/C and let $\{u_j, v_j; j=1, 2, \dots, s\}$ be a τ-Galois system for T/B. Then we may choose the system $\{u_j, v_j; j=1, 2, \dots, s\}$ in C since C/A is a τ-cyclic extension, and hence, u_j and v_j are invariant under the action of σ. Consequently we have

$$\sum_{i=1}^{t}(x_i(\sum_{j=1}^{s}u_j\sigma^k\tau^h(v_j))\sigma^k(y_i)=\delta_{1,\sigma^k\tau^h}.$$

and this shows that T/A is an S-Galois extension. Thus we have

COROLLARY 3.2. *Let $p>2$ be a prime. If $B=A[x]=\sum_{i=0}^{p-1}\oplus x^i A$ is a p-extension such that $x^p=xc+d$ and c is a unit element, then B/A can be embedded into a G-Galois extension T/A where G is a non-abelian group of the order p^2-p.*

References

[1] M. AUSLANDER and O. GOLDMAN; The Brauer group of a commutative ring, Trans. A. M. S., Vol. 97 (1960), 367-409.

[2] S. U. CHASE, D. K. HARRISON and A. ROSENBERG; Galois theory and Galois cohomology of commutative rings, Mem. A. M. S., No. 52 (1965), 15-33.

[3] F. R. DEMEYER; Some notes on the general Galois theory of rings, Osaka Math. J., Vol. 2 (1970), 159-174.

[4] K. KISHIMOTO; On abelian extensions of rings I, Math. J. Okayama Univ., Vol. 14 (1970), 159-174.

[5] K. KISHIMOTO; On abelian extensions of rings II, Math. J. Okayama Univ., Vol. 15 (1971), 57-70.

[6] K. KISHIMOTO; Finite posets P and P-Galois extensions of rings, (to appear).

[7] T. NAGAHARA and A. NAKAJIMA; On cyclic extensions of commutative rings, Math. J. Okayama Univ., Vol. 15 (1971), 81-90.

Department of Mathematics
Shinshu University
Matsumoto 390, Japan