Journal of the Faculty of Environmental Science and Technology,
Okayama University
Vol.9, No.1, pp.27-36, February 2004

Commutative quartic P-Galois extensions over a field of characteristic 2

Atsushi Nakajima *

(Received November 27, 2003)

Abstract

Let A/R be a ring extension and P a subset of $\mathrm{Hom}(A_R, A_R)$. In his paper [5], K.Kishimoto introduced the notion of a P-Galois extension and gave several basic properties of these extensions. The author showed that these extensions are closely related to Hopf Galois extensions and the strucutre of quadratic or cubic P-Galois extensions over a field were given in [9] and [10]. Recently, the author classify commutative quartic P-Galois extensions over a field of characteristic not 2 in [11]. Continuing [11], we treat commutative quartic P-Galois extensions over a field of characteristic 2.

Keywords : Cyclic extension, P-Galois extension, Hopf Galois extension.

0. Introduction

Let A/R be a ring extension with common identity 1 and $\mathrm{Hom}(A_R, A_R)$ the set of all right R-module homomorphisms of A. For a subset P of $\mathrm{Hom}(A_R, A_R)$, the notion of a P- Galois extension was introduced by Kishimoto and gave several basic properties of these extensions in [5]. It closely relates a Hopf Galois extension, and a relation of these two Galois extensions was given in [9]. Although there are various types of the structure of P in general, but if the cardinality $\mid P \mid$ is very small, we can classify the types of P and determine the structure of P-Galois extensions. In fact, the author completely classified the P-Galois extensions over a field with $|P| = 2,\ 3$ in [9] and [10], and in case of $\mid P \mid = 4$, the structure of these commutative P-Galois extensions over a field of characteristic not 2 determined in [11].

In this paper, continuing [11], we classify commutative quartic P-Galois extensions over a field k of characteristic 2. A quartic extension means $|P| = 4$. If P is a group of order 4, then a P- Galois extension is a Galois extension with Galois group P, and if P is cyclic (cf. [4]) then these P-Galois extensions were discussed in [4] and [8]. Therefore, we treat the other cases of P-Galois extensions, that is, P is neither a group nor a cyclic type.

1. Preliminaries

The notion of a P-Galois extension is not familiar to the reader, so we begin by definition of a P-Galois extension.

Let A/R be a ring extension with common identity 1 and let P be a subset of $\mathrm{Hom}(A_R, A_R)$, which is a partially ordered set with respect to an order $\leq$. In the following, we denote the elements of P by *Capital Greek Letters* according to [5]. The set of all mininal (resp. maximal) elements of P under this order is denoted by $P(min)$ (resp. $P(max)$). A *chain* of Λ $(\in P)$ means a descending chain

$$\Lambda = \Lambda_0 >> \Lambda_1 >> \ldots >> \Lambda_m,$$

where Λ_m is a minimal element and $\Lambda_t >> \Lambda_s$ means that there does not exists Λ_u such that $\Lambda_t > \Lambda_u > \Lambda_s$. In this case, we say that Λ has *length* $m+1$. For a finite partially ordered subset $P \subseteq \mathrm{Hom}(A_R, A_R)$ is called a *relative sequence of homomorphisms* if the following conditions (A.1) - (A.4) and (B.1) - (B.4) are satisfied:

*Department of Environmental and Mathematical Sciences, Faculty of Environmental Science and Technology, Okayama University, Tsushima, Okayama 700-8530, Japan.

(A.1) $\Lambda \neq 0$ for all $\Lambda \in P$ and $P(min)$ coincides with all $\Lambda \in P$ such that Λ is a ring automorphism.
(A.2) Any two chains of Λ have the same length.
(A.3) If $\Lambda\Gamma \neq 0$, then $\Lambda\Gamma \in P$ and if $\Lambda\Gamma = 0$, then $\Gamma\Lambda = 0$.
(A.4) Assume that $\Lambda\Gamma$, $\Lambda\Omega \in P$ (resp. $\Gamma\Lambda$, $\Omega\Lambda \in P$). Then
(i) $\Lambda\Gamma \geq \Lambda\Omega$ (resp. $\Gamma\Lambda \geq \Omega\Lambda$) if and only if $\Gamma \geq \Omega$.
(ii) If $\Lambda\Gamma \geq \Omega$, then $\Omega = \Lambda_1\Gamma_1$ for some $\Lambda \geq \Lambda_1$ and $\Gamma \geq \Gamma_1$.
Let x, $y \in A$.
(B.1) $\Lambda(1) = 0$ for any $\Lambda \in P - P(min)$.
(B.2) For any $\Lambda \geq \Gamma$, there exists $g(\Lambda, \Gamma) \in \mathrm{Hom}(A_R, A_R)$ such that

$$\Lambda(xy) = \sum_{\Lambda \geq \Omega} g(\Lambda, \Omega)(x)\Omega(y).$$

If $\Lambda \not\geq \Gamma$, then we set $g(\Lambda, \Gamma) = 0$.
(B.3) (i) For the above $g(\Lambda, \Gamma)$, there holds

$$g(\Lambda, \Gamma)(xy) = \sum_{\Lambda \geq \Omega \geq \Gamma} g(\Lambda, \Omega)(x)g(\Omega, \Gamma)(y).$$

(ii) If $\Lambda\Gamma \geq \Omega$, then

$$g(\Lambda\Gamma, \Omega)(x) = \sum_{\Lambda \geq \Lambda', \Gamma \geq \Gamma', \Lambda'\Gamma' = \Omega} g(\Lambda, \Lambda')g(\Gamma, \Gamma')(x).$$

(B.4) (i) $g(\Lambda, \Lambda)$ is a ring automorphism.
(ii) $g(\Lambda, \Omega) = \Lambda$ for any $\Omega \in P(min)$ for $\Omega \leq \Lambda$.
(iii) If $\Lambda > \Gamma$, then $g(\Lambda, \Gamma)(1) = 0$.

Since $P(min)$ is a group by (A.1)–(A.4) (cf.[5, section 1, Remark]), P always contains the identity map from A to A and so we denote it by 1. We do not mistake the identity element 1 of A for the identity map 1. If $P = \{1 < \Lambda\}$, then by (B.2) and (B.4) we see

$$\Lambda(xy) = \Lambda(x)y + \lambda(x)\Lambda(y),$$

which shows that Λ is a $(1, \lambda)$-derivation, where $\lambda = g(\Lambda, \Lambda)$. For further details, see [4] and [5].

In [5], Kishimoto added the following two conditions for characterizing the P-Galois extensions:

(A.5) $|P(min)| = |P(max)|$.
(A.6) For any $\Gamma \in P(max)$, if $\Omega \leq \Gamma$, then there exist Ω_1 and $\Omega_2 \in P$ such that $\Gamma = \Omega\Omega_1 = \Omega_2\Omega$.

Now for a relative sequence of homomorphisms P, we set

$$A_1 = \{a \in A \mid \Lambda(a) = a \text{ for all } \Lambda \in P(min)\}$$

and

$$A_0 = \{a \in A \mid \Lambda(a) = 0 \text{ for all } \Lambda \in P - P(min)\}.$$

Since $P(min)$ is a group, A_1 is a subring of A. On the other hand, if a, $b \in A_0$ then by (B.2) we have

$$\Lambda(ab) = \sum_{\Lambda \geq \Gamma} g(\Lambda, \Gamma)(a)\Gamma(b) = \sum_{\Lambda \geq \Gamma, \Gamma \in P(min)} \Lambda(a)\Gamma(b) = 0$$

for any $\Lambda \in P - P(min)$ and thus A_0 is also a subring of A. We call that

$$A^P = A_1 \cap A_0$$

the *invariant subring* of P. Next we compose an algebra from A and P.

Let $D(A, P) = \sum_{\Lambda \in P} \oplus Au_\Lambda$ be a free left A-module with A-basis $\{u_\Lambda \mid \Lambda \in P\}$. Define a multiplication on $D(A, P)$ by

$$(au_\Lambda)(bu_\Gamma) = \sum_{\Lambda \geq \Omega} ag(\Lambda, \Omega)(b)u_{\Omega\Gamma},$$

where $u_{\Omega\Gamma} = 0$ if $\Omega\Gamma = 0$. Then it is easy to see that $D(A, P)$ is an R-algebra, which is called the *trivial crossed product* ([5, Theorem 2.2]). Under these circumstances we define the following

Definition 1.1. A/R is called a *P-Galois extension* if it satisfies the following three conditions:
(P.1) $A^P = R$.
(P.2) A is a finitely generated projective right R-module.
(P.3) The map $j : D(A, P) \to \mathrm{Hom}(A_R, A_R)$ defined by $j(au_\Lambda)(x) = a\Lambda(x)$ is an isomorphism.

If $P = P(min)$, then $D(A, P)$ is the usual crossed product and thus a P-Galois extension is a Galois extension with Galois group P. If

$$P = \{1 < \Lambda < \Lambda^2 < \cdots < \Lambda^n \mid \Lambda^n = 0,\ g(\Lambda, \Lambda) = \lambda\},$$

then the P-Galois extension is called *cyclic*. In case of $\mathrm{char}(R) = p$ and $\Lambda^p = 0$ with $g(\Lambda, \Lambda) = 1$, then the P-Galois extension is a purely inseparable extension.

Two P-Galois extensions A and B are *isomorphic* if there exists a ring isomorphism $\varphi : A \to B$ such that $\varphi(\Omega a) = \Omega\varphi(a)$ for any $a \in A$ and $\Omega \in P$.

Now we classify the types of P in case of $| P | = 4$. The cardinality of P is only four, but there are various types of P.

The following classification of P is given by [11, Lemmas 1.3 and 1.4].

Lemma 1.2. *Let A/R be a ring extension with common identity and let P be a relative sequence of homomorphisms of* $\mathrm{Hom}(A_R, A_R)$ *such that $| P | = 4$ and satisfies* (A.6). *Assume that P is neither a group nor cyclic. Then P is one of the following types.*

(1) $P = \{1 < \Gamma\ ;\ \Lambda < \Lambda\Gamma \mid \Lambda\Gamma = \Gamma\Lambda,\ \Lambda^2 = 1$ and $\Gamma^2 = 0\}$, *where $g(\Gamma, \Gamma) = \gamma$ and Γ is a $(1, \gamma)$-derivation.*

(2) $P = \{1 < \Lambda\ ;\ 1 < \Gamma\ ;\ 1 < \Omega \mid \Lambda^2 = \Gamma^2 = \Omega^2 = \Lambda\Gamma = \Lambda\Omega = \Gamma\Omega = 0\}$, *where $g(\Omega, \Omega) = \omega$ and Λ* (resp. Γ, Ω) *is a $(1, \lambda)$* (resp. $(1, \gamma)$, $(1, \omega)$)*-derivation.*

(3) $P = \{1 < \Gamma\ ;\ 1 < \Lambda < \Lambda^2 \mid \Lambda^3 = \Gamma^2 = \Lambda\Gamma = 0\}$, *where Λ* (resp. Γ) *is a $(1, \lambda)$* (resp. $(1, \gamma)$)*-derivation.*

(4) $P = \{1 < \Lambda,\ \Gamma < \Gamma\Lambda \mid \Lambda\Gamma = \Gamma\Lambda,\ \Lambda^2 = \Gamma^2 = 0\}$, *where Λ* (resp. Γ) *is a $(1, \lambda)$* (resp. $(1, \gamma)$)*-derivation.*

(5) $P = \{1 < \Lambda < \Gamma < \Gamma\Lambda \mid \Lambda\Gamma = \Gamma\Lambda,\ \Lambda^2 = \Gamma^2 = 0\}$, *where Λ is a $(1, \lambda)$-derivation.*

Proof. We give an outline of the proof. The proof is divided by the cardinality of $| P(min) |$.

First, let $| P(min) | = 4$. Then P is a group and so we exclude this case. Next, let $| P(min) | = 3$. Then we can set

$$P = \{1,\ \Lambda,\ \Lambda^2,\ \Gamma \mid \Lambda^3 = 1,\ \Gamma \text{ is not minimal}\}.$$

If Γ is the only maximal element in P, then by $1 < \Gamma$ we have a contradiction $\Lambda < \Lambda\Gamma = \Gamma$. For the other cases $\{1, \Gamma\} = P(max)$ etc., we also have contradictions. Therefore the case $| P(min) | = 3$ does not happen under our conditions.

Assume $P(min) = 2$. Then P contains a group of order 2, and so we can set $P = \{1,\ \Lambda,\ \Gamma,\ \Omega \mid \Lambda^2 = 1\}$. By the cardinality of $P(max)$, P is divided as the following cases:

(1) $P(max) = 1$.
  (i) $\{1 < \Gamma < \Omega\ ;\ \Lambda < \Gamma < \Omega\}$.
(2) $P(max) = 2$.
  (ii) $\{1\ ;\ \Lambda < \Gamma < \Omega\}$, (iii) $\{1 < \Gamma < \Omega\ ;\ \Lambda\}$, (iv) $\{1 < \Gamma,\ \Omega\ ;\ \Lambda < \Gamma,\ \Omega\}$,
  (v) $\{1 < \Gamma\ ;\ \Lambda < \Gamma,\ \Omega\}$, (vi) $\{1 < \Gamma,\ \Omega\ ;\ \Lambda < \Omega\}$, (vii) $\{1 < \Gamma\ ;\ \Lambda < \Omega\}$.
(3) $P(max) = 3$.
  (viii) $\{1 < \Gamma,\ \Omega\ ;\ \Lambda\}$, (ix) $\{\Lambda < \Gamma,\ \Omega\ ;\ 1\}$.

Then we note that

$$\Lambda\Theta \neq 0 \text{ for any } \Theta \in P, \text{ and } \Gamma < \Omega \text{ implies } \Gamma\Lambda < \Omega\Lambda, \qquad (*)$$

because Λ is an automorphism.

If P is type (1), then multiplying Λ we have $\Lambda < \Lambda\Gamma < \Lambda\Omega$. Comparing this chain with $\Lambda < \Gamma < \Omega$, we have a contradiction. Similarly, the types (ii) or (iii) in (2), and (viii) or (ix) in (3) do not happen under our conditions.

For the types (iv), (v) and (vi) in (2), since Γ has two minimal elements 1 and Λ, then by (B.2) we have

$$\begin{aligned}\Gamma(xy) &= g(\Gamma,\Gamma)(x)\Gamma(y) + g(\Gamma,1)(x)y + g(\Gamma,\Lambda)(x)\Lambda(y)\\ &= \gamma(x)\Gamma(y) + \Gamma(x)y + \Gamma(x)\Lambda(y),\end{aligned}$$

where $g(\Gamma,\Gamma) = \gamma$, and so $\Gamma(x) = \gamma(x)\Gamma(1) + \Gamma(x) + \Gamma(x)$. Since Γ is not minimal, we see $\Gamma(1) = 0$ by (B.1), which shows $\Gamma(x) = 0$ for all $x \in A$. This contradicts to (A.1). Since $\Lambda < \Lambda\Gamma = \Omega$, the type (vii) in (2) is the case (1) in our lemma.

Finally, let $\mid P(min) \mid = 1$. Then we can set

$$P = \{1,\ \Lambda,\ \Gamma,\ \Omega \mid 1 \text{ is the unique minimal}\}.$$

According to the cardinarity of $P(max)$, we can divide P as the following cases.

(i) $\{1 < \Lambda\ ;\ 1 < \Gamma\ ;\ 1 < \Omega\}$, (ii) $\{1 < \Gamma\ ;\ 1 < \Lambda < \Omega\}$, (iii) $\{1 < \Lambda < \Gamma,\ \Omega\}$,

(iv) $\{1 < \Lambda,\ \Gamma < \Omega\}$, (v) $\{1 < \Lambda < \Gamma < \Omega\}$.

If P is type (i), then $\Lambda < \Lambda^2$, $\Lambda < \Lambda\Gamma$ and $\Lambda < \Lambda\Omega$. Using (*) and the maximality of Λ, we see $\Lambda^2 = \Lambda\Gamma = \Lambda\Omega = 0$. Similarly, $\Gamma^2 = \Gamma\Omega = \Omega^2 = 0$. The properties of Λ, Γ and Ω are obtained from (B.2) and (B.4). This is the case (2) in our lemma. We also see that the cases (ii) and (iv) correspond to the case (3) and (4), respectively. Moreover if P is type (v), then we have the case (5) in our Lemma and a cyclic type. And the case (iii) does not happen under our conditions. □

We determine the structure of commutative quartic P-Galois extensions A/k according to the classification of P in Lemma 1.2. In our classification, there are some types of Galois extensions, so for the convenience to the reader, we review definitions of these Galois extensions.

Let R be a commutative algebra over the prime field $GF(p)$, m a positive integer and A a commutative R-algebra with common identity. A ring extension A/R is called a *cyclic p^m-extension* if A/R is a Galois extension with cyclic Galois group (σ) of order p^m. The basic properties of commutative Galois extensions can be seen in [1] or in [3], and some elementray properties of commutative cyclic p^m-extensions were given in [6].

The above cyclic p^m-extensions and purely inseparable extensions were unified in [8] as follows. For any $u \in R$, let $H(u,p^m)$ be the free Hopf algebra over R with basis $\{1, \delta,\ \delta^2,\ \cdots,\ \delta^{p^m-1}\}$ whose Hopf algebra structure is defined by

$$\delta^{p^m} = 0, \quad \Delta(\delta) = \delta \otimes 1 + (1 + u\delta) \otimes \delta, \quad \varepsilon(\delta) = 0 \quad \text{and} \quad S(\delta) = \sum_{i=1}^{p^m-1} (-1)^i u^{i-1}\delta^i,$$

where $S : H \to H$ is an antipode. Then we see that the action of H on A is given by

$$\delta(xy) = \delta(x)y + (1 + u\delta)(x)\delta(y)$$

for any $x,\ y \in A$. In [8], the author characterized commutative $H(u,p^m)$-Hopf Galois extensions and computed the isomorphism class group of these extesions.

In [9], we defined the notion of an (H,J)-Galois extension as follows. Let H be a Hopf algebra and let J be an augmented algebra with augmentation $\varepsilon_J : J \to R$ and a left H-comodule structure map $\rho : J \to H \otimes J$. A is called an (H,J)- *module algebra* if the following conditions are satisfied.

(MA.1) A is a left H-module algebra.

(MA.2) A is a left J-module such that for any $\Lambda \in J$

$$\Lambda(xy) = \sum_{(\Lambda)} \Lambda_{(-1)}(x)\Lambda_{(0)}(y) \quad \text{and} \quad \Lambda(1) = \varepsilon_J(\Lambda)1,$$

where $\rho(\Lambda) = \sum_{(\Lambda)} \Lambda_{(-1)} \otimes \Lambda_{(0)} \in H \otimes_R J$.

For an (H, J)-module algebra A, we can construct the smash product algebra $A\sharp H$ as usual. A/R is called an (H, J)-*Galois extension* if the following conditions are satisfied.

(G.1) A is an (H, J)-module algebra.
(G.2) $R = A^J = \{a \in A \mid \Lambda(a) = \varepsilon_J(\Lambda)a \text{ for any } \Lambda \in J\}$.
(G.3) A is a finitely generated projective R-module.
(G.4) The map $\varphi : A\sharp J \to \mathrm{Hom}_R(A, A)$ defined by $\varphi(a\sharp\Lambda)(x) = a\Lambda(x)$ is an isomorphism.

If $H = J$ is a Hopf algebra, then an (H, H)-Galois extension is an H-Hopf Galois extension in the sense of [2]. The above (H, J)-Galois extension was called a *weak* (H, J)-*Galois extension* in [9]. The relations with P-Galois extensions and weak (H, J)-Galois extensions were also given in [9]. For further detail of Hopf Galois extensions, see [2] and [12].

Throughout the following, k is a field of characteristic 2 and A is a k-algebra. We denote it by A/k.

2. The cases (1) in Lemma 1.2

In this section, let

$$P = \{1 < \Gamma\ ;\ \Lambda < \Lambda\Gamma = \Gamma\Lambda \mid \Lambda^2 = 1,\ \Gamma^2 = 0\},$$

where Γ is a $(1, \gamma)$-derivation. For a P-Galois extension A/k, since k is a direct summand of A, then by [5, Theorem 3.4] there exists $a \in A$ such that $(1 + \Lambda)\Gamma(a) = 1$. We set

$$(1 + \Lambda)(a) = x \quad \text{and} \quad \Gamma(a) = y.$$

First, we note that $\dim_k A = 4$ by definition 1.1 (P.3). Then we have the following

Lemma 2.1. *Under the above notations,* $\{1,\ x,\ y,\ xy\}$ *is a* k*-basis of* A *such that*

$$\Lambda(x) = x, \quad \Gamma(x) = 1, \quad \Lambda(y) = y + 1 \quad \text{and} \quad \Gamma(y) = 0.$$

Moreover,

$$A_0 = \{b \in A \mid \Gamma(b) = 0\} = k[y]$$

and $\{1,\ x\}$ *are linearly independent over* A_0.

Proof. Since $\Lambda^2 = 1$ and $\mathrm{char}k = 2$, we see $(1 + \Lambda)(x) = 2(1 + \Lambda)(a) = 0$ and so $\Lambda(x) = x$. By $\Lambda\Gamma = \Gamma\Lambda$, we also see $\Gamma(x) = 1$ and $\Lambda(y) = y + 1$. And by $\Gamma^2 = 0$, $\Gamma(y) = 0$ is easily seen. Assume that $r_0 + r_1x + r_2y + r_3xy = 0$ for $r_i \in k$. Then by using $\Gamma(k) = 0$ and Γ is a $(1, \gamma)$-derivation, we get $0 = \Gamma(r_0 + r_1x + r_2y + r_3xy) = r_1 + r_3y$. Applying $1 + \Lambda$, we have $2r_1 + 2r_2y + r_3 = 0$ and so $r_3 = r_1 = 0$. Therefore $r_0 + r_2y = 0$. Applying $1 + \Lambda$ again, we have $r_2 = r_0 = 0$. Hence $\{1,\ x,\ y,\ xy\}$ is a k-basis of A.

Now by defnition of A_0, we have $A_0 = \{b \in A \mid \Gamma(b) = 0\}$ and by $\Gamma(y) = 0$, y is contained in A_0. Since $\Lambda(y) \neq 0$, we have $A_0 \supsetneq k[y]$ and $\dim_k A_0 \geq \dim_k k[y] \geq 2$. Furthermore, if $b + cx = 0$ $(b,\ c \in A_0)$, then by

$$0 = \Gamma(b + cx) = \Gamma(b) + \Gamma(c)x + \gamma(c)\Gamma(x) = \gamma(c)$$

and γ is an automorphism, we have $c = 0$ and so $b = 0$. Therefore $\{1,\ x\}$ are a linearly independent over A_0 and thus $\dim_k A_0 = 2$. Hense $A_0 = k[y]$. □

Theorem 2.2. *Let* A/k *be a* P*-Galois extension with* k*-basis* $\{1,\ x,\ y,\ xy\}$ *given by* Lemma 2.1. *Then the following hold.*

(1) $A = k[y][x]$ *and* $y^2 = y + t$ *for some* $t \in k$. *When this is the case* $k[y]/k$ *is a cyclic* 2*-extension with group* (Λ).

(2) $k[x]/k$ *is an* $H(u, 2)$*-Hopf Galois extension for some* $u \in k$.

Proof. (1) By $\Gamma(xy) = \Gamma(yx)$, we have $\gamma(y) = y$. We set $y^2 = r_0 + r_1x + r_2y + r_3xy$ $(r_i \in k)$. Since Γ is a $(1, \gamma)$-derivation and by $\Gamma(y) = 0$ and $\Gamma(x) = 1$, we have $0 = \Gamma(y^2) = r_1 + r_3y$, which shows $r_1 = r_3 = 0$. Moreover by $\Lambda(y) = y + 1$ and $\mathrm{char}k = 2$, we see

$$\Lambda(y^2) = (y + 1)^2 = r_0 + r_2y + 1 = \Lambda(r_0 + r_2y) = r_0 + r_2(y + 1).$$

Thus $r_2 = 1$ and so $y^2 = y + r_0$. Since Λ induces an automorphism of $k[y]$, $k[y]/k$ is a cyclic 2-extension with group (Λ).

(2) We set $x^2 = s_0 + s_1x + s_2y + s_3xy$ $(s_i \in k)$. Applying Λ on both sides, we have $\Lambda(x^2) = x^2 = s_0 + s_1x + s_2(y+1) + s_3x(y+1)$ and thus $s_2 = s_3 = 0$. Therefore $x^2 = s_0 + s_1x$. Moreover by $\Gamma(x^2) = x + \gamma(x) = \Gamma(s_0 + s_1x) = s_1$, we obtain $\gamma(x) = s_1 + x$.

Now let H be a k-algebra with basis $\{1,\ \Gamma\}$. Define

$$\begin{aligned}&\text{algebra structure: } \Gamma^2 = 0,\\ &\text{coalgebra structure: } \Delta(\Gamma) = \Gamma \otimes 1 + (1 + s_1\Gamma) \otimes \Gamma,\ \varepsilon(\Gamma) = 0,\\ &\text{antipode: } S(\Gamma) = \Gamma.\end{aligned}$$

Then it is easy to see that H is a Hopf algebra which is denoted by $H(s_1, 2)$. Since the action of Γ on $k[x]$ is given by

$$\Gamma(x^2) = \Gamma(x)x + \gamma(x)\Gamma(x) = \Gamma(x)x + (1 + s_1\Gamma)(x)\Gamma(x).$$

This shows that the P-action on $k[x]$ coincides to the $H = \{1, \Gamma\}$-Hopf algebra action on $k[x]$. Consider the map

$$\varphi : k[x]\sharp H(s_1, 2) \to \mathrm{Hom}_k(k[x], k[x]) \quad \text{defined by} \quad \varphi(b\sharp\Omega)(u) = b\Omega(u) \quad (b, u \in k[x],\ \Omega \in J)$$

and assume $\varphi = 0$. Then by $\varphi(b\sharp\Gamma)(x) = b = 0$, φ is a monomorphism. Counting dimensions, we see that φ is an isomorphism. Therefore $k[x]/k$ is an $H(s_1, 2)$-Hopf Galois extension. □

Now, we classsify these P-Galois extensions. Let A/k and A'/k be P-Galois extensions with bases

$$\begin{aligned}&\{1,\ x,\ y,\ xy\} \text{ such that } y^2 = y + r,\ x^2 = ax + b, \quad (r, a, b \in k)\\ &\{1,\ x',\ y',\ x'y'\} \text{ such that } (y')^2 = y' + r',\ (x')^2 = a'x' + b', \quad (r', a', b' \in k)\end{aligned}$$

respectively. Let $\psi : A \to A'$ be an isomorphism of P-Galois extensions. We set

$$\psi(x) = r_0 + r_1x' + r_2y' + r_3x'y' \quad \text{and} \quad \psi(y) = s_0 + s_1x' + s_2y' + s_3x'y'$$

for some $r_i, s_i \in k$. Then by $\Omega\psi(z) = \psi(\Omega(z))$ for any $z \in \{x, y\}$ and $\Omega \in \{\Lambda, \Gamma\}$, we see

$$\psi(x) = x' + v \quad \text{and} \quad \psi(y) = y' + u \quad \text{for some } v,\ u \in k.$$

Since $\Lambda(x) = x$, $\Gamma(x) = 1$, $\Lambda(y) = y + 1$ and $\Gamma(y) = 0$, the invariant subrings of Γ and $\{1,\ \Lambda\} = P(min)$ are $A_0 = k[y]$ and $A_1 = k[x]$, respectively. When this is the case, ψ induces an isomorphism $\psi_1 = \psi|k[y] : k[y] \to k[y']$ as $P(min)$-Galois extensions if and only if there exists $u \in k$ such that $u^2 + u = r + r'$. And $\psi_2 = \psi|k[x] : k[x] \to k[x']$ is an isomorphism if and only if $a = a'$ and there exists $v \in k$ such that $v^2 + av = b + b'$.

Conversely, let $\psi_1 : k[y] \to k[y']$ is an isomorphism of $P(min) = (\Lambda)$-Galois extesions and $\psi_2 : k[x] \to k[x']$ is an isomorphism of $P_1 = \{1,\ \Gamma\}$-Galois extensions with relations

$$y^2 = y + s, \quad x^2 = ax + b \quad \text{and} \quad (y')^2 = y' + s', \quad (x')^2 = a'x' + b'.$$

For P-Galois extensions A/k and A'/k, we denote the set of isomorphisms from A/k to A'/k by $\mathrm{Iso}(A, A')$. Then it is easy to see that the map $\psi : A \to A'$ defined by $\psi(y) = \psi_1(y)$ and $\psi(x) = \psi_2(x)$ is an isomorphism of P-Gālois extensions. Moreover the correspondence

$$\mathrm{Iso}(A, A') \ni \psi \mapsto (\psi_1, \psi_2) \in \mathrm{Iso}(k[y], k[y']) \times \mathrm{Iso}(k[x], k[x'])$$

is one to one and onto. Thus it is enough to consider the isomorphisms $\psi_1 : k[y] \to k[y']$ as (Λ)-Galois extensions and $\psi_2 : k[x] \to k[x']$ as $P_1 = \{1,\ \Gamma\}$-Galois extensions. Since $k[y]$ and $k[y']$ are cyclic 2-extensions over k, $k[y]$ and $k[y']$ are isomorphic if and only if there exists $u \in K$ such that $u^2 + u = s + s'$ and ψ_1 is given by $\psi_1(y) = y' + u$. On the other hand, since $\Gamma(\psi_2(x)) = \psi_2(\Gamma(x))$, we see that $k[x]$ and $k[x']$ are isomorphic if and only if $a = a'$ and there exists $v \in k$ such that $v^2 + av = b + b'$. And ψ_2 is given by $\psi_2(x) = x' + v$. Therefore we have the following

Theorem 2.3. *Let P be the type* (2) *in* Lemma 1.3. *Let $A = k[y][x]$ and $A' = k[y'][x']$ be P-Galois extensions with relations*

$$y^2 = y + s,\ x^2 = ax + b \quad \text{and} \quad (y')^2 = y' + s',\ (x')^2 = a'x' + b'. \quad (s, s', a, a', b, b' \in k)$$

Then A and A' are isomorphic if and only if $a = a'$ and there exist $u,\ v \in k$ such that $u^2 + u = s + s'$ and $v^2 + av = b + b'$. When this is the case, the isomorphism $\varphi : A \to A'$ is given by $\varphi(y) = y' + u$ and $\varphi(x) = x' + v$.

Although the isomorphism classes of commutative Hopf Galois extensions has a group structure, we do not know that the isomorphism classes of commutative P-Galois extensions has also a group structure or not. But in this case, we can compute the cardinality of the isomorphism classes of these types of P-Galois extensions. For example, by the above theorem, [7, Corollary 2.8] and [8, section 3.1], we have the following

Corollary 2.4. *The cardinality of the isomorphism classes of commutative P-Galois extensions over k is equal to the cardinality of the additive group*

$$k^+/\{u^2 + u \mid u \in k\} \times k^+/\{v^2 + av \mid v \in k\},$$

where k^+ is the additive group of k.

3. The cases (2) and (3) in Lemma 1.2

Let P be one of the types of (2) and (3) in Lemma 1.2. Then as similar as the case of characteristic not 2, we have the following

Theorem 3.1. *There does not exist P-Galois extensions of the types* (2) *and* (3) *of* Lemma 1.2.

The proof of this theorem is similar to the proof of [11, Theorem 3.1]. So we give here an outline of the proof.

First, let P be type (2) in Lemma 1.2, that is,

$$P = \{1 < \Lambda\ ;\ 1 < \Gamma\ ;\ 1 < \Omega \mid \Lambda^2 = \Gamma^2 = \Omega^2 = \Lambda\Gamma = \Lambda\Omega = \Gamma\Omega = 0\},$$

where Λ, Γ and Ω are $(1, \lambda)$, $(1, \gamma)$ and $(1, \omega)$-derivations, respectively. Then for a P-Galois extension A/k, it is easy to see that $A_1 = \{a \in A \mid 1(a) = a\} = A$ and $A_0 = \{a \in A \mid \Lambda(a) = \Gamma(a) = \Omega(a) = 0\}$. Therefore $A_1 \cap A_0 = A_0 = k$.

Let $\{1,\ x,\ y,\ z\}$ be a k-basis of A. Since Λ is a $(1, \lambda)$-derivation, we see

$$\Lambda(x^2) = \Lambda(x)x + \lambda(x)\Lambda(x) \quad \text{and} \quad \Lambda(xy) = \Lambda(x)y + \lambda(x)\Lambda(y).$$

By these relations we have

$$\Lambda(x^2)\Lambda(y) - \Lambda(xy)\Lambda(x) = \Lambda(x)\Lambda(y)x - \Lambda(x)^2 y.$$

Since $A_0 = k$, then by the structure of P we see $\Lambda(a) \in k$ for any $a \in A$. Moreover $\{1,\ x,\ y\}$ are linearly independent over k, we obtain $\Lambda(x) = 0$. Similarly, we also get $\Gamma(x) = \Omega(x) = 0$, because the conditions of Λ, Γ and Ω are quite similar. Therefore we have a contradiction $x \in k$. This shows that there does not exist P-Galois extensions in case of type (2) in Lemma 1.2.

Next, let P be type (3) in Lemma 1.2, that is,

$$P = \{1 < \Gamma\ ;\ 1 < \Lambda < \Lambda^2 \mid \Lambda^3 = \Gamma^2 = \Lambda\Gamma = 0\},$$

where Λ and Γ are $(1, \lambda)$ and $(1, \gamma)$- derivations, respectively. Then we see that

$$A_0 = \{a \in A \mid \Lambda(a) = \Gamma(a) = 0\} = k.$$

We set $A_\Gamma = \{a \in A \mid \Gamma(a) = 0\}$. Since Γ is a $(1, \gamma)$-derivation, then by the similar calculation for Λ in the discussion above, we have

$$\Gamma(x^2)\Gamma(y) - \Gamma(xy)\Gamma(x) = \Gamma(x)\Gamma(y)x - \Gamma(x)^2 y = 0.$$

In this case, $\Gamma(a) \in k$ for any $a \in A$ by $\Gamma^2 = \Lambda\Gamma = 0$. Therefore we get $\Gamma(x) = 0$, because $\{x,\ y\}$ are linearly independent over k. Hence x is contained in A_Γ. Similarly, y and z are also contained in A_Γ, which means $A_\Gamma = A$. Consider the map

$$j : D(A, P) = \sum_{\Omega \in P} \oplus A u_\Omega \to \mathrm{Hom}_k(A, A)$$

defined in Definition 1.1(P.3). Then for any $a \in A_\Gamma = A$, we see $j(u_\Gamma)(a) = \Gamma(a) = 0$ by definition of A_Γ. Therefore j is not an isomorphism and thus there does not exist P-Galois extension in this case.

4. The case (4) in Lemma 1.2

In this section, we set

$$P = \{1 < \Lambda,\ \Gamma < \Lambda\Gamma \mid \Gamma\Lambda = \Lambda\Gamma,\ \Lambda^2 = \Gamma^2 = 0\},$$

where Λ is a $(1,\ \lambda)$-derivation and Γ is a $(1,\ \gamma)$-derivation. Then for a P-Galois extension A/k, we have

Lemma 4.1. *There exists a k-basis $\{1,\ x,\ y,\ xy\}$ of A which satisfies the following conditions.*

(1) $\Lambda(x) = \Gamma(y) = 1$ *and* $\Lambda(y) = \Gamma(x) = 0$.

(2) $y^2 = sy + t$ *and* $x^2 = ax + b$ *for some* $s,\ t,\ a,\ b \in k$.

Proof. Since $\Lambda\Gamma$ is the unique maximal element of P with minimal element 1, we have by [5, Theorem 3.4] $\Lambda\Gamma(a) = 1$ for some $a \in A$. Then the existence of a k-basis of A which satisfies the condition (1) is similarly proved as in Lemma 2.1. By $\Lambda(xy) = \Lambda(yx)$ and $\Gamma(xy) = \Gamma(yx)$, we have $\lambda(y) = y$ and $\gamma(x) = x$. Let $x^2 = r_0 + r_1x + r_2y + r_3xy$ $(r_i \in k)$. Applying Γ on both sides, we have

$$\Gamma(x^2) = \Gamma(x)x + \gamma(x)\Gamma(x) = 0 = r_2 + r_3\gamma(x) = r_2 + r_3x.$$

Thus $r_2 = r_3 = 0$ and $x^2 = r_1x + r_0$. And by $\Lambda(x^2) = r_1$, we get $\lambda(x) = x + r_1$. Since the conditions of Λ, x and Γ, y are symmetric, we also have $y^2 = sy + t$ and $\gamma(y) = y + s$ $(s,\ t \in k)$.

Theorem 4.2. *Let A/k be a P-Galois extension with k-basis $\{1,\ x,\ y,\ xy\}$ given in* Lemma 4.1. *Then A is isomorphic to $k[y] \otimes_k k[x]$ as k-algebras and $k[y] \otimes_k k[x]$ is an $H(s,2) \otimes H(a,2)$-Hopf Galois extesnion.*

Proof. Define a map $f : A \to k[y] \otimes k[x]$ by

$$f(r_0 + r_1x + r_2y + r_3xy) = r_0(1 \otimes 1) + r_1(1 \otimes x) + r_2(y \otimes 1) + r_3(y \otimes x).$$

Then it is easily seen that f is an isomorphism of k-algebras. Since $H(s,2)$ is an Hopf algebra with basis $\{1,\ \Gamma\}$ such that

$$\Gamma^2 = 0, \quad \Delta(\Gamma) = \Gamma \otimes 1 + \gamma \otimes \Gamma \quad \text{and} \quad \varepsilon(\Gamma) = 0,$$

then by $\gamma(x) = x$, $\gamma(y) = y + s$, $\Gamma(x) = 0$ and $\Gamma(y) = 1$, we see $\gamma = 1 + s\Gamma$. Therefore, the action of $H(s,2)$ on $k[y]$ is the same as the action of P on $k[y]$, and we can easily check that the map $\varphi : A\sharp H(s,2) \to \mathrm{Hom}_k(k[y], k[y])$ defined by $\varphi(b\sharp h)(z) = bh(z)$ is an isomorphism $(a, z \in A, h \in H)$. Thus $k[y]/k$ is an $H(s,2)$-Hopf Galois extension. Since the conditions of Γ and Λ are symmetirc, we also have $k[x]/k$ is an $H(a,2)$-Hopf Galois extension, where $H(a,2)$ is a Hopf algebra defined as similar as $H(s,2)$ with basis $\{1, \Lambda\}$. Thus the result is clear. □

Theorem 4.3. *Let A/k and A'/k be commutative P-Galois extensions with basis $\{1,\ x,\ y,\ xy\}$ and $\{1,\ x',\ y',\ x'y'\}$, respectively. We set*

$$y^2 = sy + t, \quad x^2 = ax + b \quad \text{and} \quad (y')^2 = s'y' + t', \quad (x')^2 = a'x' + b',$$

where $s,\ s',\ t,\ t' \in k$, $a,\ a',\ b,\ b' \in k[y]$. Then A and A' are isomorphic if and only if $s = s'$, $a = a'$ and there exist $u,\ v \in k$ such that $u^2 + su = t + t'$ and $v^2 + av = b + b'$. When this is the case, the isomorphism $\varphi : A \to A'$ is given by $\varphi(y) = y' + u$ and $\varphi(x) = x' + v$.

Proof. Let $\varphi : A \to A'$ be an isomorphism of P- Galois extension. Then as in the proof of Theorem 2.2, φ induces isomorphisms

$$\varphi_1 : k[y] \ni y \mapsto y' + u \in k[y'] \quad \text{and} \quad \varphi_2 : k[x] \ni x \mapsto x' + v \in k[x'].$$

Moreover, for $y^2 = sy + t$ and $(y')^2 = s'y' + t'$, $\varphi_1 : k[y] \ni y \mapsto y' + u \in k[y']$ is an isomorphism if and only if $s = s'$ and $u^2 + su = t + t'$. Since the conditions of y and x are same, we also have $\varphi_2 : k[x] \ni x \mapsto x' + v \in k[y']$ is an isomorphism if and only if $a = a'$ and $v^2 + av = b + b'$. Hence our theorem is proved. □

Corollary 4.4. *The cardinality of the isomorphism classes of commutative P-Galois extensions over k is equal to the cardinality of the additive group*

$$k^+/\{u^2 + su \mid u \in k\} \times k^+/\{v^2 + av \mid v \in k\}.$$

5. The case (5) in Lemma 1.2

In the final section, we assume

$$P = \{1 < \Lambda < \Gamma < \Lambda\Gamma \mid \Lambda\Gamma = \Gamma\Lambda,\ \Lambda^2 = \Gamma^2 = 0\},$$

where Λ is a $(1, \lambda)$-derivation. First, we have the following

Lemma 5.1. *Let A/k be a P-Galois extension. Then there exists a k-basis $\{1, x, y, xy\}$ of A such that the following conditions satisfy.*

(1) $\Lambda(x) = \Gamma(y) = 1$ *and* $\Lambda(y) = \Gamma(x) = 0$.

(2) $y^2 = sy + t$ *for some* $s, t \in k$, $\lambda(y) = y$ *and* $\gamma(y) = y + s$.

Proof. (1) is easily obtained by Lemma 4.1. Assume that $r_0 + r_1x + r_2y + r_3xy = 0$ $(r_i \in k)$. Applying Λ, we have $0 = r_1 + r_3y$, because Λ is a $(1, \lambda)$-derivation. Thus $0 = \Gamma(r_1 + r_3y) = r_3$ and so $r_1 = 0$. Therefore, we have $0 = r_0 + r_2y$. Similarly, we get $r_0 = r_2 = 0$. Hence $\{1, x, y, xy\}$ is a k-basis of A.

Now we set $y^2 = s_0 + s_1x + s_2y + s_3xy$ $(s_i \in k)$. Then by $\Lambda(y^2) = 0 = s_1 + s_3y$, we have $s_1 = s_3 = 0$ and thus $y^2 = s_0 + s_2y$. Since A is commutative, we see $y = \lambda(y)$ by $\Lambda(xy) = \Lambda(yx)$. Finally, by

$$\Gamma(y^2) = \Gamma(y)y + g(\Gamma, \Lambda)(y)\Lambda(y) + \gamma(y)\Gamma(y) = y + \gamma(y) = s_2,$$

we get $\gamma(y) = y + s_2$. □

Finally, we have the following

Theorem 5.2. *Let A and A' be commutative P-Galois extensions of k with basis $\{1, x, y, xy\}$ and $\{1, x', y', x'y'\}$ as in* Lemma 2.1, *respectively. We set*

$$y^2 = sy + t, \quad x^2 = ax + b \quad \text{and} \quad (y')^2 = s'y' + t', \quad (x')^2 = a'x' + b',$$

where $s, s', t, t' \in k$, $a, a', b, b' \in k[y]$. If $\varphi : A \to A'$ is an isomorphism of P-Galois extensions, then φ induces an isomorphism $\varphi_1 : k[y] \to k[y']$. When this is the case, $s = s'$, $\varphi(a) = a'$ and there exist α, $\beta \in k$ such that the following conditions satisfy:

$$\alpha^2 + s\alpha + t + t' = 0 \quad \text{and} \quad \beta^2 + \varphi(a)\beta + \varphi(b) + b' = 0.$$

Conversely, let $\psi_1 : k[y] \to k[y']$ be an isomorphism of P-Galois extensions. If $a' = \psi_1(a)$ and there exists $\beta \in k$ such that $\beta^2 + \psi_1(a)\beta + \psi_1(b) + b' = 0$, then ψ_1 is extended to the isomorphism $\psi : A$ to A' of P-Galois extensions.

Proof. Let $\varphi : A \to A'$ be an isomorphism of P-Galois extensions. Then by $\Lambda\varphi(x) = \varphi(\Lambda(x))$ and $\Gamma\varphi(x) = \varphi(\Gamma(x))$, we have $\varphi(x) = x' + \beta$ for some $\beta \in k$. Similarly we have $\varphi(y) = y' + \alpha$ for some $\alpha \in k$. Since φ is a k-algebra isomorphism, we obtain $s = s'$ and $\alpha^2 + s\alpha + t + t' = 0$. Moreover by

$$\varphi(x^2) = (\varphi(x' + \beta))^2 = \varphi(ax + b) = \varphi(a)(x' + \beta) + \varphi(b),$$

we get $\varphi(a) = a'$ and $\beta^2 + \varphi(a)\beta + \varphi(b) + b' = 0$, because $\varphi(k[y])$ is contained in $k[y]$.

Conversely, if we define $\psi : A \to A'$ by $\psi(y) = \psi_1(y)$ and $\psi(x) = x' + \beta$, then ψ is an isomorphism of P-Galois extensions which is an extensions of ψ_1. □

Unfortunately, we do not know that the cardinality of the isomorphism classes of these P-Galois extensions. All P-Galois extensions which is known till now (cf. [4], [5], [9], [10] and [11]) are Hopf Galois extensions and so we ask that does there exists a P-Galois extension over a field which is not a Hopf Galois extension?

REFERENCES

[1] S.U.Chase, D.K.Harrison and A.Rosenberg: *Galois theory and Galois cohomology of commutative rings,* Mem. A.M.S. No.**52**(1965).

[2] S.U.Chase and M.E.Sweedler: *Hopf Algebras and Galois theory,* Lecture Notes in Math. No.**97**, Springer-Verlag, Berlin (1969).

[3] F.DeMeyer and E.Ingraham: *Separable Algebras Over Commutative Rings,* Lecture Notes in Math. No.**181**, Springer-Verlag, Berlin (1971).

[4] K.Kishimoto: *On P-Galois extensions of rings of cyclic type,* Hokkaido Math. J. **20**(1991), 123–133.

[5] K.Kishimoto: *Finite posets P and P-Galois extensions of rings,* Math. J. Okayama Univ. **34**(1992), 21–47.

[6] T.Nagahara and A.Nakajima: *On cyclic extensions of commutative rings,* Math. J. Okayama Univ. **15**(1971), 81–90.

[7] A.Nakajima: *On a group of cyclic extensions over commutative rings,* Math. J. Okayama Univ. **15**(1972), 163–172.

[8] A.Nakajima: *A certain type of commutative Hopf Galois extensions and their groups,* Math. J. Okayama Univ. **24**(1982), 137-152.

[9] A.Nakajima: *Weak Hopf Galois extensions and P-Galois extensions of a ring,* Comm. in Alg. **23**(1995), 2851–2862.

[10] A.Nakajima: *Cubic P-Galois extensions over a field,* Hokkaido Math. J. **27**(1998), 321–328.

[11] A.Nakajima: *Commutative quartic P-Galois extensions over a field of characteristic not* 2, submitted.

[12] M.E.Sweedler: *Hopf Algebras,* Benjamin New York, 1971.