Turkish Journal of Mathematics

Volume 29 | Number 3 Article 3

1-1-2005

Commutative Quartic P-Galois Extensions Over a Field of Characteristic Not 2

ATSUSHI NAKAJIMA

Turk J Math
29 (2005) , 235 – 247.

Commutative Quartic P-Galois Extensions Over a Field of Characteristic Not 2*

Atsushi Nakajima

Abstract

In [2], K. Kishimoto introduced the notion of P-Galois extensions and gave some fundamental properties of these extensions. P-Galois extensions relate Hopf Galois extensions, and the author treated these topics in [5]. Moreover, the cubic P-Galois extensions over a field were completely determined in [6]. Continuing [5] and [6], we classify commutative quartic P-Galois extensions over a field of characteristic not 2.

Key Words: Galois extension, P-Galois extension, quartic extension.

0. Introduction

Let A/R be a ring extension with common identity 1 and let P be a partially ordered subset of $\mathrm{Hom}(A_R, A_R)$. In his paper [1], Kishimoto characterized a special type of Galois extensions which he called a cyclic P-Galois extension over a ring of characteristic p. Cyclic P-Galois extensions closely relate to purely inseparable extensions and $H(u, p^m)$-Hopf Galois extensions which were given in [4]. After that he introduced a general notion of P-Galois extensions and gave some fundamental properties of them in [2].

Since the usual Galois extensions and purely inseparable extensions are P-Galois extensions, the essential part of P-Galois extensions is that P is neither a group nor a cyclic type (cf. [1]). If the cardinality $\mid P \mid$ of P is 2 or 3, then all P-Galois extensions over a field were completely classified without any assumptions in [5] and [6].

*Dedicated to Professor Arif Kaya on his 60th birthday

In this paper, continuing [5] and [6], we treat quartic P-Galois extensions, that is, $\mid P \mid = 4$. We classify commutative quartic P-Galois extensions over a field k of characteristic not 2 and determine the structure of these extensions, where P is neither a group nor a cyclic type. Using these structures, we estimate the cardinality of the isomorphism classes of these P-Galois extensions.

1. Preliminaries

The notion of a P-Galois extension might not be familiar to the reader, so according to [2], we begin with the definition of a P-Galois extension.

Let A/R be a ring extension with common identity 1. Let P be a finite partially ordered subset of $\mathrm{Hom}(A_R, A_R)$ with respect to an order $\leq$. In the following, we denote the elements of P by *Capital Greek Letters* according to [2]. The set of all mininal (resp. maximal) elements of P under $\leq$ is denoted by $P(min)$ (resp. $P(max)$). A *chain* of $\Lambda \in P$ means a descending chain

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

where Λ_m is a minimal element and $\Lambda_t >> \Lambda_s$ means that there does not exist Λ_u such that $\Lambda_t > \Lambda_u > \Lambda_s$. Then we say that Λ has *length* $m+1$. P is called a *relative sequence of homomorphisms* if the following conditions (A.1) – (A.4) and (B.1) – (B.4) are satisfied:

(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

$$\Lambda(xy) = \sum_{\Lambda \geq \Gamma} g(\Lambda, \Gamma)(x)\Gamma(y). \quad \text{(If } \Lambda \not\geq \Gamma, \text{ then we set } g(\Lambda, \Gamma) = 0.)$$

(B.3) (i) The above map $g(\Lambda, \Gamma)$ satisfies

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

(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 $\Omega \in P(min)$ such that $\Omega \leq \Lambda$.

(iii) If $\Lambda > \Gamma$, then $g(\Lambda, \Gamma)(1) = 0$.

Since $P(min)$ is a finite subsemigroup of $\mathrm{Hom}(A_R, A_R)$, then $P(min)$ is a group by (A.1)–(A.4) and if $P = \{1 < \Lambda\}$, then by (B.2) and (B.4), Λ is a $(1, \lambda)$-derivation

$$\Lambda(xy) = \Lambda(x)y + \lambda(x)\Lambda(y), \quad (g(\Lambda, \Lambda) = \lambda,\ x,\ y \in A).$$

For further details of relative sequences of homomorphisms, see [2].

Kishimoto added the following two conditions to obtain the properties of P-Galois extensions:

(A.5) $\mid P(min) \mid = \mid P(max) \mid$.

(A.6) For any $\Omega \in P(max)$, if $\Gamma \leq \Omega$, then there exist Γ_1 and $\Gamma_2 \in P$ such that $\Omega = \Gamma\Gamma_1 = \Gamma_2\Gamma$.

The types of P are restricted by the conditions of (A.1)–(A.6), but there exist various types of P even in case of $\mid P \mid = 4$. We will see them later.

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

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

Then A_1 is a subring of A and for any a, $b \in A_0$ and $\Lambda \in P - P(min)$, we see

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

by (B.2). Therefore A_0 is also a subring of A. $A^P = A_1 \cap A_0$ is called the *invariant subring* of P. Next we compose an algebra from A and P.

Let $D(A, P) = \sum_{\Lambda \in P} \oplus A u_\Lambda$ 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 $D(A, P)$ is a k-algebra, which we call a *trivial crossed product* ([2, Theorem 2.2.]). Under these circumstances, we give 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 so a P-Galois extension is a Galois extension with Galois group P. If $\mathrm{char}(R) = p$ and Λ is a derivation such that $\Lambda^p = 0$, then for

$$P = \{1 < \Lambda < \Lambda^2 < \cdots < \Lambda^{p-1}\},$$

a P-Galois extension relates a purely inseparable extension. This is a special case of cyclic P-Galois extensions. For further details of cyclic P-Galois extensions, see [1].

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

The following lemma is useful, which is easily proved by A.4(i).

Lemma 1.2. *Let P be a relative sequence of homomorphisms and $\Lambda,\ \Gamma,\ \Omega \in P$. Then we have the following.*

(1) *If $\Lambda\Omega \neq 0$, $\Gamma\Omega \neq 0$ and $\Lambda\Omega = \Gamma\Omega$, then $\Lambda = \Gamma$.*

(2) *If $\Lambda\Omega \neq 0$, $\Gamma\Omega \neq 0$ and $\Lambda < \Gamma$, then $\Lambda\Omega < \Gamma\Omega$.*

Now we treat quartic P-Galois extensions. First, we classify the type of P such that $\mid P \mid = 4$.

If $\mid P(min) \mid = 4$, then P is a group of order 4 and so we omit it. If $\mid P(min) \mid = 3$, then P contains a cyclic group of order 3 and so we can set

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

Since $P(min) = \{1,\ \Lambda,\ \Lambda^2\}$ and Γ is not minimal, we see $\Lambda^i < \Gamma$ for some $i \in \{0,\ 1,\ 2\}$. By (A.3), we get $1 = \Lambda^i\Lambda^{3-i} < \Gamma\Lambda^{3-i} \in P$. This shows that $\Lambda^{3-i}\Gamma = \Gamma$, because Λ and Λ^2 are minimal. Hence $1 < \Gamma$ and so $\Lambda < \Lambda\Gamma = \Gamma$. Then by Lemma 1.2(1), we have a contradiction: $\Lambda = 1$. Therefore the case $\mid P(min) \mid = 3$ does not happen.

Lemma 1.3. *Let* $\mid P \mid = 4$ *and* $\mid P(min) \mid = 2$. *Then we have*

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

and Γ *is a* $(1, \gamma)$*-derivation.*

Proof. Since P contains a group of order 2, we can set $P = \{1,\ \Lambda,\ \Gamma,\ \Omega \mid \Lambda^2 = 1\}$. We note that $\Lambda\Theta \neq 0$ for any $\Theta \in P$, and $\Gamma < \Omega$ implies $\Gamma\Lambda < \Omega\Lambda$, because Λ is an automorphism. The types of P are divided according to the cardinality of $P(max)$:

(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) $\{1 < \Gamma, \Omega;\ \Lambda < \Gamma\}$, (vii) $\{1 < \Gamma;\ \Lambda < \Omega\}$.

(3) $P(max) = 3$:
  (viii) $\{1 < \Gamma,\ \Omega;\ \Lambda\}$, (ix) $\{\Lambda < \Gamma,\ \Omega;\ 1\}$.

Now we examine each case.

(i) Multiplying by Λ, we have $\Lambda < \Lambda\Gamma < \Lambda\Omega$. Comparing this chain with $\Lambda < \Gamma < \Omega$, we have a contradiction by Lemma 1.2.

(ii) and (iii) Multiplying by Λ, we have

$$1 < \Lambda\Gamma < \Lambda\Omega \quad \text{and} \quad \Lambda < \Lambda\Gamma < \Lambda\Omega,$$

respectively. These contradict that 1 and Λ are maximal in (ii) and (iii), respectively. Similarly, we see that the cases (viii) and (ix) do not happen.

(iv), (v) and (vi) Since Γ has two minimal elements 1 and Λ, then by (B.2) and (B.4) 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 have $\Gamma(1) = 0$ by (B.1). Hence $\Gamma(x) = 0$ for all $x \in A$, which contradicts (A.1).

(vii) By (B.2) and (B.4), Γ is a $(1,\gamma)$-derivation and by $1 < \Gamma$, we have $\Gamma^2 = 0$. Moreover by $\Lambda\Gamma \neq 0$, we also have $\Omega = \Lambda\Gamma$. This case is in our lemma. □

Lemma 1.4. *Let* $| P | = 4$ *such that* P *satisfies the condition* (A.6). *If* $| P(min) | = 1$, *then* P *is one of the following types.*

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

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

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

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

(5) $P = \{1 < \Lambda < \Lambda^2 < \Lambda^3 \mid \Lambda^4 = 0\}$, *where* Λ *is a* $(1,\lambda)$*-derivation.*

Proof. First, we note that P contains the identity map $1 : A \to A$, because $P(min)$ is a group. So we can set

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

According to the cardinarity of $P(max)$, the types of P are divided as follows.

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

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

We examine each case.

(i) Since $\Lambda < \Lambda^2$, $\Lambda < \Lambda\Gamma$ and $\Lambda < \Lambda\Omega$, then by Lemma 1.2 and the maximality of Λ, we have $\Lambda^2 = \Lambda\Gamma = \Lambda\Omega = 0$. Similarly we have $\Gamma^2 = \Gamma\Omega = \Omega^2 = 0$. And the other properties of Λ, Γ and Ω are obtained by (B.2) and (B.4). This gives the type (1).

(ii) Multiplying by Γ and Ω, we have

$$\Gamma < \Gamma^2, \quad \Gamma < \Gamma\Lambda < \Gamma\Omega \quad \text{and} \quad \Omega < \Gamma\Omega, \quad \Omega < \Lambda\Omega < \Omega^2,$$

respectively. Then using the maximality of Γ, Lemma 1.2 and (A.6), we have

$$\Gamma^2 = \Gamma\Lambda = \Gamma\Omega = 0, \quad \Omega\Lambda = \Omega^2 = 0 \quad \text{and} \quad \Omega = \Lambda^2.$$

This gives the type (2).

(iii) By $1 < \Lambda < \Gamma$ and $1 < \Lambda < \Omega$, we have $\Omega = \Lambda^2 = \Gamma$ by (A.6), which is a contradiction. Therefore this case does not happen.

(iv) By the maximality of Ω and Lemma 1.2, we have $\Omega^2 = \Omega\Gamma = \Omega\Lambda = 0$. If $\Lambda\Gamma = 0$, then by (A.6) we get $\Omega = \Lambda^2 = \Gamma^2$. Since $\Lambda < \Omega = \Gamma^2$, we have a contradiction by (A.4)(ii). Therefore $\Omega = \Lambda\Gamma$ and $\Lambda^2 = \Gamma^2 = 0$. The other properties of Λ and Γ are obtained by (B.2) and (B.4). This gives the type (3).

(v) Since Ω is maximal, then $\Omega^2 = \Omega\Lambda = \Omega\Gamma = 0$. If $\Omega \neq \Lambda\Gamma$, then by (A.6), $\Lambda^2 = \Omega = \Gamma^2$ and so $\Gamma < \Lambda^2$. This contradicts (A.4)(ii). Hence $\Omega = \Lambda\Gamma$. On the other hand if $\Lambda^2 = 0$, then $\Lambda^2 = \Gamma^2 = 0$. And if $\Lambda^2 = \Gamma$, then $1 < \Lambda < \Lambda^2 < \Lambda^3$, $\Lambda^4 = 0$. These give the types (4) and (5). Especially, (5) is the cyclic type. □

According to Lemmas 1.3 and 1.4, we will classify commutative quartic P-Galois extensions. *So in the following, we will assume that P is a relative sequence of homomorphisms such that $\mid P \mid = 4$ and satisfies the condition* (A.6), *and A is a commutative quartic P-Galois extension over a field k of characteristic not* 2.

2. The case of Lemma 1.3

In this section, we assume

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

where Γ is a $(1,\ \gamma)$-derivation, and we have

$$A_1 = \{a \in A \mid \Lambda(a) = a\} \quad \text{and} \quad A_0 = \{a \in A \mid \Gamma(a) = 0\}.$$

Since $j : D(A, P) \to \mathrm{Hom}_k(A, A)$ is an isomorphism, then we have $\dim_k D(A, P) = 4\dim_k A = (\dim_k A)^2$. Hence $\dim_k A = 4$. First, we prove the following

Lemma 2.1. $\dim_k A_i = 2$ *or* 3. $(i = 0,\ 1)$.

Proof. Let $1,\ x,\ y,\ z$ be a k-basis of A. Suppose $A_0 = k$. Then it is easy to see that $\Gamma(a) \in A_0 = k$ $(a \in A)$ and by relations

$$\Gamma(x^2) = \Gamma(x)x + \gamma(x)\Gamma(x) \quad \text{and} \quad \Gamma(xy) = \Gamma(x)y + \gamma(x)\Gamma(y),$$

we have

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

Since $1,\ x,\ y$ are linearly independent over k, then $\Gamma(x) = 0$ and thus $x \in k$, which is a contradiction. Hence $A_0 \neq k$. By [2, Theorem 3.4], there exists $a_0 \in A$ such that $(1 + \Lambda)\Gamma(a_0) = 1$ and so $a_0 \notin A_0$. Hence $A \neq A_0$. Therefore we see $\dim_k A_0 = 2$ or 3.

On the other hand, if $A_1 = k$, then by $(1 + \Lambda)(a_0) \in A_1 = k$, we have a contradiction: $0 = \Gamma((1+\Lambda)(a_0)) = (1+\Lambda)\Gamma(a_0) = 1$. Hence $A_1 \neq k$. Since $A_1 \neq A$, we see $\dim_k A_1 = 2$ or 3. □

Lemma 2.2. (1) *A_0 has a k-basis* $1,\ x$ *such that* $x^2 = b \in k$ *and* $\Lambda(x) = -x$.

(2) *A_1 has a k-basis* $1,\ z$ *such that* $z^2 = c \in k$, $\Gamma(z) = 1$ *and* $\gamma(z) = -z$.

Proof. (1) Suppose that $\dim_k A_0 = 3$ and $1,\ w,\ y$ is a k-basis of A_0. Take $a_0 \in A$ such that $(1+\Lambda)\Gamma(a_0) = 1$ and set $z = a_0 + \Lambda(a_0)$. By $\Gamma(z) = 1$, we see that $1,\ w,\ z,\ zw$ are k-basis of A and so we set $y = s_0 + s_1 w + s_2 z + s_3 zw$ $(s_i \in k)$. Then by $0 = \Gamma(y) = s_2 + s_3 w$, we have a contradiction: $y = s_0 + s_1 w$. Therefore by Lemma 2.1, $\dim_k A_0 = 2$ and we may suppose that $1,\ w$ are k-basis of A_0. Since A_0 is a subalgebra, there exist $r,\ s \in k$ such that $w^2 = rw + s$. Take $w = x + r/2$, we have $x^2 = b$ for some $b \in k$ and $1,\ x,\ z,\ zx$ are also k-basis of A such that $\Gamma(x) = 0$ and $\Gamma(z) = 1$.

Now, we set $\Lambda(x) = t_0 + t_1 x + t_2 z + t_3 zx$ $(t_i \in k)$. By $\Gamma\Lambda(x) = \Lambda\Gamma(x)$, we have $\Lambda(x) = t_0 + t_1 x$. Since Λ induces an automorphism of A_0 and $x^2 = b$, we get $\Lambda(x) = t_1 x$ and $t_1^2 b = b$ $(t_1 \neq 0)$. Therefore by $\Lambda^2 = 1$ and $\Lambda \neq 1$, we have $\Lambda(x) = -x$.

(2) Suppose $\dim_k A_1 = 3$. Since $\Gamma(1 + \Lambda)(a) \in A_0 \cap A_1$ $(a \in A)$, we can take $a_0 \in A$ such that $\Gamma(1+\Lambda)(a_0) = 1$. Then there exists a k-basis $1,\ z,\ u$ of A_1 such that $\Gamma(z) = 1$. Let $1,\ x$ be a k-basis of A_0 as in (1). As is easily seen, $1,\ x,\ z,\ zx$ are k-basis of A and so we set $u = t_0 + t_1 x + t_2 z + t_3 zx$ $(t_i \in k)$. By $u = \Lambda(u)$ and $\Lambda(x) = -x$, we have a contradiction: $u = t_0 + t_2 z$. Therefore by Lemma 2.1, $\dim_k A_1 = 2$ and $1,\ z$ are k-basis such that $\Gamma(z) = 1$. We set $z^2 = sz + t$ for some $s,\ t \in k$. Since 2 is invertible, we can take $z_1^2 = c \in k$ such that $\Lambda(z_1) = z_1$ and $\Gamma(z_1) = 1$. □

By Lemmas 2.1 and 2.2, the following theorem is easily seen.

Theorem 2.3. *There exists a k-basis $1,\ x,\ z,\ zx$ of A such that*

(1) $x^2 = b$ *and* $z^2 = c$ *for some* $b,\ c \in k$,

(2) $\Gamma(x) = 0,\ \Lambda(x) = -x,\ \Gamma(z) = 1$ *and* $\Lambda(z) = z$.

In this case, A is isomorphic to $A_0 \otimes_k A_1$ as k-algebra.

By this theorem, we may denote a P-Galois extension A/k by a pair of elements $(b,\ c) \in k \times k$. Under these notations, we have the following theorem.

Theorem 2.4. *Let $A = (b,\ c)$ and $A' = (b',\ c')$ be P-Galois extensions denoted above. Let $1,\ x,\ z,\ zx$ and $1,\ x',\ z',\ z'x'$ be k-basis of A and A' as in* Theorem 2.3, *respectively. Then a map $\varphi : A = (b,\ c) \to A' = (b',\ c')$ is an isomorphism of P-Galois extension if and only if there exists non-zero element $r \in k$ such that $b = r^2 b'$. In this case, there hold $\varphi(x) = rx'$, $\varphi(z) = z'$ and $c = c'$.*

Proof. We set $\varphi(x) = r_0 + r_1 x' + r_2 z' + r_3 z'x'$ $(r_i \in k)$. Then by $\Gamma\varphi(x) = \varphi(\Gamma(x)) = 0$ and φ is an k-algebra isomorphism, we have $r_0 = 0$ and $b = r_1^2 b'$. Similarly we have $\varphi(z) = z'$ and $c = c'$. The converse is clear. □

By Theorem 2.4, we can estimate the cardinality of the isomorphism classes of P-Galois extensions as follows.

Corollary 2.5. *The cardinality of the isomorphism classes of P-Galois extensions is*

$$| (k^\times/(k^\times)^2) \times k | ,$$

where $k^\times$ is the multiplicative group of k.

3. The case of Lemma 1.4

In this section, we determine the structure of P-Galois extensions, where P is one of the types of Lemma 1.4.

3.1. First, let

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

where Λ, Γ and Ω are $(1,\lambda)$, $(1,\gamma)$ and $(1,\omega)$-derivations, respectively. Since 1 is the unique minimal, then $A_1 = A$ and so $A_0 = k$. Let $1,\ x,\ y,\ z$ be a k-basis of A. Since Λ is a $(1,\lambda)$-derivation, we have

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

By these relations we get

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

Using that $\Lambda(a) \in A_0 = k$ $(a \in A)$ and $1,\ x,\ y$ are linearly independent over k, we get $\Lambda(x) = 0$. Similarly we also get $\Gamma(x) = \Omega(x) = 0$. Hence $x \in k$, which is a contradiction. Therefore there does not exist a P-Galois extension.

Second, let

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

where Λ and Γ are $(1,\lambda)$ and $(1,\gamma)$- derivations, respectively. Then $A_1 = A$ and $A_0 = k$. Set

$$A_\Gamma = \{a \in A \mid \Gamma(a) = 0\}.$$

Using that Γ is a $(1,\gamma)$-derivation, we have

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

Since $\Gamma(a) \in k$ $(a \in A)$, then $\Gamma(x) = 0$ and so $x \in A_\Gamma$. Smilarly $y,\ z \in A_\Gamma$. Hence $A_\Gamma = A$. Consider the map $j : D(A,P) \to \mathrm{Hom}_k(A,A)$ defined in Definition 1.1 (P.3). Then by $j(u_\Gamma)(a) = \Gamma(a) = 0$ $(a \in A = A_\Gamma)$, j is not an isomorphism. Thus we have the following theorem.

Theorem 3.1. *If P is one of the types of* (1) *or* (2) *of* Lemma 1.4, *then there does not exist a P-Galois extension.*

3.2. In this subsection, let P be the types (3) or (4) of Lemma 1.4. Then P has the following common properties.

(1) Λ is a $(1,\lambda)$-derivation.
(2) $\Lambda\Gamma = \Gamma\Lambda$ is the unique maximal element of P.
(3) 1 is the unique minimal element of P.

(4) $\Lambda^2 = \Gamma^2 = 0$.

Using the above properties, we have the following lemma.

Lemma 3.2. *There exists a k-basis $1,\ x,\ y,\ xy$ of A such that*

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

Proof. Since $\Gamma\Lambda$ is unique maximal and 1 is unique minimal, there exists $a \in A$ such that $\Lambda\Gamma(a) = 1$ by [2,Theorem 3.4]. Set $x = \Gamma(a)$ and $y = \Lambda(a)$. Then by $\Lambda\Gamma = \Gamma\Lambda$ and $\Lambda^2 = \Gamma^2 = 0$, we have

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

Using these relations, we see that $1,\ x,\ y,\ xy$ are k-basis of A. □

Now, to determine the structure of P-Galois extension A/k, we take another k-basis as follows.

Lemma 3.3. *There exists a k-basis $1,\ z,\ w,\ zw$ of A such that*

(1) *$1,\ z$ are a linearly independent over $k[w]$ such that $z^2 = b \in k[w]$ and $w^2 = c \in k$, where $k[\omega]$ is the k-subalgebra generated by ω,*

(2) $\Lambda(z) = \Gamma(w) = 1$ and $\Lambda(w) = 0$.

Proof. As is easily seen, $A_0 = \{a \in A \mid \Lambda(a) = \Gamma(a) = 0\} = k$. Using a k-basis $1,\ x,\ y,\ xy$ as in Lemma 3.2, we may set $y^2 = r_0 + r_1x + r_2y + r_3xy$ $(r_i \in k)$. Then by $\Lambda(y^2) = \Lambda(y)y + \lambda(y)\Lambda(y) = 0 = r_1 + r_3y$, we get $r_1 = r_3 = 0$ and hence $y^2 = r_0 + r_2y$.

Now, we divide into two cases.

(i) If P is of type (3) of Lemma 1.4, then Γ is a $(1,\gamma)$-derivation and so $\Gamma(1) = 0$. Put $w = y - r_2/2$. Then $1,\ x,\ w,\ xw$ are k-basis of A such that

$$\Lambda(x) = \Gamma(w) = 1,\ \Lambda(w) = \Gamma(x) = 0 \ \text{ and } \ w^2 = c \in k. \qquad (*)$$

(ii) If P is of type (4) of Lemma 1.4, then by

$$\Gamma(1) = \Gamma(1 \cdot 1) = \Gamma(1) + g(\Gamma,\Lambda)(1)\Lambda(1) + \gamma(1)\Gamma(1)$$

and γ is an automorphism, we have $\Gamma(1) = 0$. Therefore A has k-basis $1,\ x,\ w,\ xw$ with the properties (*).

By $\Lambda(x) = 1$ and $\Lambda(w) = 0$, we see that $1,\ x$ are $k[w]$-linearly independent. Since $k[w]$ is a subalgebra, we have $x^2 = a_0 + a_1 x$ for some $a_0,\ a_1 \in k[w]$. Take $z = x - a_1/2$. Then $z^2 \in k[\omega]$, $\Lambda(z) = 1$, and $1,\ z$ are $k[w]$-linearly independent. Therefore we can easily get a k-basis $1,\ z,\ w,\ zw$ of A which is requested one. □

We denote a P-Galois extension A/k in Lemma 3.3 by $[b,\ c]$ $(b \in k[w],\ c \in k)$. Using the basis in Lemma 3.3, we prove the following theorem.

Theorem 3.4. *Let $A = [b,\ c]$ and $A' = [b',\ c']$ be P-Galois extensions. Let* $1,\ z,\ w,\ zw$ *and* $1,\ z',\ w',\ z'w'$ *be k-basis of A and A' in* Lemma 3.3, *respectively. If $\varphi : A \to A'$ is an isomorphism of P-Galois extension, then $b = b'$ and $c = c'$.*

Proof. We set

$$\varphi(w) = r_0 + r_1 z' + r_2 w' + r_3 z'w' \ \text{ and } \ \varphi(z) = s_0 + s_1 z' + s_2 w' + s_3 z'w',$$

$(r_i, s_i \in k)$. Then by $\Lambda(\varphi(w)) = \varphi(\Lambda(w))$ and $\Gamma(\varphi(w)) = \varphi(\Gamma(w))$, φ induces an isomorphism from $k[w]$ to $k[w']$ such that $\varphi(w) = r_0 + w'$ and $\varphi(w^2) = c = (r_0^2 + c') + 2r_0 w'$. Hence $r_0 = 0$, $c = c'$ and $\varphi(w) = w'$. Moreover, by $\Lambda(\varphi(z)) = \varphi(\Lambda(z))$, we have $\varphi(z) = s_0 + z' + s_2 w'$ and thus

$$\varphi(z^2) = b = (s_0 + s_2 w' + z')^2 = (s_0 + s_2 w')^2 + b' + 2(s_0 + s_2 w')z'.$$

Since $1, z'$ are linearly independent over $k[w']$ and $b,\ b',\ s_0 + s_2 w' \in k[w']$, we have $s_0 = s_2 = 0$. Hence $\varphi(z) = z'$ and $b = b'$. □

Since $\dim_k k[w] = 2$, we have

Corollary 3.5. *The cardinality of the isomorphism classes of P-Galois extensions is*

$$|\ k \times k \times k\ |\ .$$

Our results will be extended to noncommutative ring extensions under certain conditions, but it seems to me that to calculate the cardinality of the isomorphism classes is not easy. And the remaining case of $\mathrm{char}(k) = 2$ was given in [7].

Acknowledgment

The author would like to thank the referee for his or her valuable comments in this paper.

References

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

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

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

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

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

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

[7] A. Nakajima: Commutative quartic P-Galois extensions over a field of characteristic 2, Journal of The Faculty of Environmental Science and Technology Okayama University 9(2004), 27–36.

Atsushi NAKAJIMA
Received 17.11.2003
Department of Environmental and Mathematical Sciences,
Faculty of Environmental Science and Technology,
Okayama University,
Tsushima, Okayama 700-8530, JAPAN
e-mail: nakajima@ems.okayama-u.ac.jp