Hokkaido Mathematical Journal Vol. 27 (1998) p. 321–328

Cubic P-Galois extensions over a field

Atsushi NAKAJIMA

(Received January 20, 1997; Revised July 11, 1997)

Abstract. The notion of P-Galois extensions was introduced by K. Kishimoto [K1] and [K2]. We determine all cubic P-Galois extensions over a field except that P is a cyclic group.

Key words: Galois extension, σ-derivation.

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 endmorphisms of A. Let P be a subset of $\mathrm{Hom}(A_R, A_R)$. In [K2], Kishimoto gave a fundamental properties of P-Galois extensions and in [K1], he determined the structure of cyclic P-Galois extensions under the assumption $\sigma D = D\sigma$ and $\mathrm{char}(R) = p$, where $P = \{1, D, D^2, \ldots, D^{p-1}, D^p = 0\}$, σ is an automorphism of A and D is a σ-derivation.

In this note, we determine all cubic P-Galois extensions over a field except P is a cyclic group. A *cubic P-Galois extension* means that the cardinality of P is three. The notion of P-Galois extension is not familiar to the reader, so we will begin at the definition of a P-Galois extension.

1. Preliminary results

Let A/R and P be as above. We assume that P is a partially ordered set with respect to the order $\leq$. In the following, we denote the elements of P by *Capital Greek Letters*. A *chain* of Λ means a descending chain $\Lambda = \Lambda_0 >> \Lambda_1 >> \cdots >> \Lambda_m$, where Λ_m is a minimal element and $\Lambda_t >> \Lambda_s$ means that there is no $\Lambda_t > \Lambda_u > \Lambda_s$. 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) $\Lambda \neq 0$ for all $\Lambda \in P$ and $P(\min)$, the set of all minimal elements in P, coincides with all $\Lambda \in P$ such that Λ is a ring automorphism.

1991 Mathematics Subject Classification : 16A78.

(A.2) Any two chain 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 $\Lambda\Gamma$, $\Lambda\Omega \in P$. 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 $\Omega \in P(min)$.
(iii) If $\Lambda > \Gamma$, then $g(\Lambda, \Gamma)(1) = 0$.
For a relative sequence of homomorphisms P, we set

$$\begin{aligned} R_0 &= \{a \in A \mid \Lambda(a) = a \text{ for all } \Lambda \in P(\min)\}. \\ R_1 &= \{a \in A \mid \Lambda(a) = 0 \text{ for all } \Lambda \in P - P(\min)\}. \end{aligned}$$

Then R_0 and R_1 are subrings of A. $A^P = R_0 \cap R_1$ 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 the multiplication on $D(A, P)$ by

$$(a u_\Lambda)(b u_\Gamma) = \sum_{\Lambda \geq \Omega} a g(\Lambda, \Omega)(b) u_{\Omega\Gamma},$$

where $u_{\Omega\Gamma} = 0$ if $\Omega\Gamma = 0$. Then we can check that $D(A, P)$ is an algebra, which is called the *trivial crossed product* ([K2, 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 conditins:

(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.

We denote the cardinality of P by $|P|$. We mean a n-th *P-Galois extension* is $|P| = n$. Then by (P.3), if R is a field, a n-th P-Galois extension A of R is a free R-module of rank n. So to determine all cubic P-Galois extensions, we have to classify P of $|P| = 3$.

Lemma 1.2 ([N1, Lemma 3.1]) *Let P be a relative sequence of homomorphisms with $|P| = 3$. Then P is one of the following*:

(1) *P is a cyclic group of order* 3.

(2) $P = \{1, \Lambda, \Lambda^2 \mid \Lambda^3 = 0;\ 1 < \Lambda < \Lambda^2\}$ *and Λ is a $(1, \sigma)$-derivation, that is, $\Lambda(ab) = \Lambda(a)b + \sigma(a)\Lambda(b)$ $(a, b \in \Lambda)$ and σ is an automorphism.*

(3) $P = \{1, \Lambda, \Gamma \mid \Lambda\Gamma = \Gamma\Lambda = \Lambda^2 = \Gamma^2 = 0;\ 1 < \Lambda < \Gamma\}$ *and Λ is a $(1, \sigma)$-derivation.*

(4) $P = \{1, \Lambda, \Gamma \mid \Lambda\Gamma = \Gamma\Lambda = \Lambda^2 = \Gamma^2 = 0;\ 1 < \Lambda,\ 1 < \Gamma\}$ *and Λ is a $(1, \sigma)$-derivation, Γ is a $(1, \tau)$-derivation and τ is an automorphism.*

If P is a cyclic group, then a P-Galois extension A/R is a usual cyclic Galois extension and so the essential part of P-Galois extension is the cases (2), (3) and (4). If P is of type (2), then it is discussed in [K1] under the assumptions $\sigma\Lambda = \Lambda\sigma$ and $\mathrm{char}(R) = 3$. We will discuss this case later without these conditions. First, we have the following

Theorem 1.3 *Let R be an integral domain which is contained in the center of A and let P be a relative sequence of homomorphisms in* $\mathrm{Hom}(A_R, A_R)$ *with $|P| = 3$. Assume that A has an R-free basis $\{1, x, y\}$. If P is of type* (3) *or* (4) *in the above Lemma* 1.2, *then $A^P \neq R$.*

Proof. Assume that $A^P = R$. We note that $R = \{a \in A \mid \Lambda(a) = \Gamma(a) = 0\}$ and $\Lambda(a), \Gamma(a) \in R$ for any $a \in A$. By $\Lambda(xy) = \Lambda(x)y + \sigma(x)\Lambda(y)$ and $\Lambda(x^2) = \Lambda(x)x + \sigma(x)\Lambda(x)$, we see

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

Since $\{1, x, y\}$ is an R-basis of A and R is an integral domain, we have

$\Lambda(x) = 0$ and so $\Gamma(x) \neq 0$. Similarly we also get $\Lambda(y) = 0$ and $\Gamma(y) \neq 0$. Therefore

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

which is a contradiction. □

Corollary 1.4 *Let $|P| = 3$ and A an algebra over a field k. If P is of type* (3) *or* (4) *in Lemma* 1.2, *then A/k is not a P-Galois extension.*

By corollary, the essential part of P-Galois extensions with $|P| = 3$ is the case (2) in Lemma 1.2. In [K1], Kishimoto considered the cyclic P-Galois extension A/R, that is, $P = \{1, \Lambda, \ldots, \Lambda^{p-1} \mid \Lambda^p = 0,\ 1 < \Lambda < \Lambda^2 < \cdots < \Lambda^{p-1}\}$ under the assumptions $\Lambda\sigma = \sigma\Lambda$ and $\mathrm{char}(R) = p$, where Λ is a $(1, \sigma)$-derivation. These assumptions are essential in his paper [K1].

2. Cubic P-Galois extensions

In the following we assume that A is an algebra over a field k of $\dim_k A = 3$, $A^P = k$, $P = \{1, \Lambda, \Lambda^2 \mid \Lambda^3 = 0,\ 1 < \Lambda < \Lambda^2\}$ and Λ is a $(1, \sigma)$-derivation. *We do not assume* $\Lambda\sigma = \sigma\Lambda$ *and* $\mathrm{char}(k) = 3$.

First, we have the following key lemma for cubic P-Galois extensions.

Lemma 2.1 *There exists k-basis $\{1, x, x^2\}$ of A which satisfies the following properties.*

(1) $\Lambda(x) = 1$.

(2) $\sigma(x) = r_0 + r_1 x$ $(r_0,\ r_1 \in k)$.

Proof. First, we note that $k = \{a \in A \mid \Lambda(a) = 0\}$. Since the maximal element of P is Λ^2, there exists an element $a \in A$ such that $\Lambda^2(a) = 1$ [K1, Theorem 3.4]. We set $x = \Lambda(a)$ and we can take a k-basis $\{1, x, y\}$ of A. If $\Lambda(y) \in k$, then $\Lambda(y)x - y \in k$ and so $\Lambda(y) \notin k$. We denote $\sigma(x) = r_0 + r_1 x + r_2 y$ $(r_i \in k)$. Then by $\Lambda^2(x^2) = 1 + r_1 + r_2\Lambda(y)$, $\Lambda^2(x^2) \in k$ and $\Lambda(y) \notin k$, we get $r_2 = 0$.

Now, for the above k-basis $\{1, x, y\}$, we set $x^2 = s_0 + s_1 x + s_2 y$ $(s_i \in k)$. Since $\sigma(x) = r_0 + r_1 x$, we have

$$\Lambda(x^2) = r_0 + (1 + r_1)x = s_1 + s_2\Lambda(y).$$

If $s_2 = 0$, then $\sigma(x) = r_0 - x$ and we get $\Lambda^2(xy) = x\Lambda^2(y)$. Since $\Lambda^2(xy)$ and $\Lambda^2(y)$ are contained in k, we have $\Lambda^2(y) = 0$ and so $\Lambda(y) \in k$: contradiction.

Thus $s_2 \neq 0$ and $\{1, x, x^2\}$ is a k-basis of A. □

Lemma 2.2 *Let $\{1, x, x^2\}$ be a k-basis of A in Lemma 2.1. Then the following holds.*

(1) *If $r_1 = 1$, then* $\mathrm{char}(k) = 3$. *In this case, $\sigma(x) = r_0 + x$ and*

$$x^3 = s_0 + r_0^2 x \quad \textit{for some} \quad s_0 \in k$$

(2) *If $r_1 \neq 1$, then* $\mathrm{char}(k) \neq 3$ *and k containes the primitive 3rd root ω of 1. In this case $\sigma(x) = r_0 + \omega x$ and*

$$x^3 = t_0 + r_0^2 \omega^{-1} x + r_0(\omega - 1)\omega^{-1} x^2 \quad \textit{for some} \quad t_0 \in k.$$

Proof. We set $x^3 = t_0 + t_1 x + t_2 x^2$ $(t_i \in k)$. Then by Lemma 2.1, $\sigma(x) = r_0 + r_1 x$ and

$$\begin{aligned} \Lambda(x^3) &= t_1 + r_0 t_2 + (1 + r_1) t_2 x \\ &= r_0^2 + r_0(1 + 2r_1)x + (1 + r_1 + r_1^2)x^2. \end{aligned}$$

Comparing coefficients, we have

$$(*) \qquad t_1 + r_0 t_2 = r_0^2, \quad (1 + r_1)t_2 = r_0(1 + 2r_1) \quad \text{and} \quad 0 = 1 + r_1 + r_1^2.$$

If $r_1 = 1$, then $\mathrm{char}(k) = 3$, $t_2 = 0$ and $t_1 = r_0^2$. If $r_1 \neq 1$, then r_1 is the primitive 3rd root of 1, $\mathrm{char}(k) \neq 3$, $t_2 = r_0(\omega - 1)\omega^{-1}$ and $t_1 = r_0^2 \omega^{-1}$. □

Now we get the following characterization of P-Galois extensions.

Theorem 2.3 *Let $P = \{1 < \Lambda < \Lambda^2 \mid \Lambda^3 = 0\}$ and Λ is a $(1, \sigma)$-derivation. Let A be an algebra over a field k such that $A^P = k$ and* $\dim_k A = 3$. *Then A/k is a P-Galois extension. Moreover there holds either*

(1) $\mathrm{char}(k) = 3$ *and $A \cong k[X]/(X^3 - r^2 X - s) = k[x]$ for some $s \in k$, where $\Lambda(x) = 1$ and $\sigma(x) = r + x$,*

or

(2) $\mathrm{char}(k) \neq 3$ *and $A \cong k[X]/(X^3 - t) = k[x]$ for some $t \in k$, where $\Lambda(x) = 1$ and $\sigma(x) = \omega x$, where ω is the primitive 3rd root of 1.*

Proof. First, we show A/k is a P-Galois extension. Since k is a field, it is enough to show that the map $j : D(A, P) \to \mathrm{Hom}(A_k, A_k)$ defined in (P.3) is a monomorphism. Let $\{1, x, x^2\}$ be a k-basis of A in Lemma 2.1.

For $\alpha = a_0 + a_1 u_\Lambda + a_2 u_{\Lambda^2} \in D(A, P)$, we assume $j(\alpha) = 0$. Then by $j(\alpha)(x^i) = 0$ $(i = 0, 1, 2)$, we have $a_0 = a_1 = 0$ and $a_2(1 + r_1) = 0$, where $\sigma(x) = r_0 + r_1 x$ in Lemma 2.1. Since $1 + r_1 + r_1^2 = 0$ in the last equation of $(*)$ in Lemma 2.2, we see $r_1 + 1 \neq 0$. Thus $a_2 = 0$, which means that j is a monomorphism.

Now by Lemma 2.2, we may assume

$$x^3 = t_0 + r_0^2 \omega^{-1} x + r_0(\omega - 1)\omega^{-1} x^2,$$
$$\Lambda(x) = 1 \quad \text{and} \quad \sigma(x) = r_0 + \omega x.$$

Since $\mathrm{char}(k) \neq 3$, if we set $x = z + (\omega - 1)(3\omega)^{-1} r_0$ as usual, then $\{1, z, z^2\}$ is a free basis of A, where $z^3 = v$ for some $v \in k$, $\Lambda(z) = 1$ and $\sigma(z) = \omega z$. This show the second part of the theorem. $\square$

In the sequel, we denote the extensions of type (1) and (2) in the above theorem by $A = (x, r^2, s)$ and $A = (x, t)$, respectively.

Now, we classify these P-Galois extensions. P-Galois extensions A_1 and A_2 are called *isomorphic* if there exists an isomorphism $\varphi : A_1 \to A_2$ such that $\varphi(\Omega a) = \Omega(\varphi(a))$ for any $a \in A$ and $\Omega \in P$.

Theorem 2.4 *Let $A_i = (x_i, r_i^2, s_i)$ be P-Galois extensions $(i = 1, 2)$. Then A_1 and A_2 are isomorphic as P-Galois extensions if and only if*

$$r_1 = r_2 \quad \textit{and} \quad u^3 = r_1^2 u + s_1 - s_2 \quad \textit{for some} \quad u \in k.$$

When this is the case, the isomorphism $\varphi : A_1 \to A_2$ is given by $\varphi(x_1) = u + x_2$.

Proof. Let $\varphi : A_1 = (x_1, r_1^2, s_1) \to A_2 = (x_2, r_2^2, s_2)$ be an isomorphism of P-Galois extensions. Then by $\varphi(\Lambda(x_1^i)) = \Lambda(\varphi(x_1^i))$ $(i = 1, 2)$ and $\varphi(x_1^3) = \varphi(x_1)^3$, there exists $u \in k$ such that

$$\varphi(x_1) = u + x_2, \quad u^3 = r_1^2 u + s_1 - s_2 \quad \text{and} \quad r_1 = r_2.$$

The converse is clear. $\square$

For a P-Galois extension $A = (x, t)$, the following is easily seen.

Theorem 2.5 (1) *P-Galois extensions $A_1 = (x_1, t_1)$ and $A_2 = (x_2, t_2)$ are isomorphic if and only if $t_1 = t_2$.*

(2) *$A = (x, t)$ is a cyclic $\langle g \rangle$-Galois extension with $g(x) = \omega x$, where ω is a primitive 3rd root of 1.*

A P-Galois extension (x,t) in Theorem 2.5(2) is a strongly cyclic 3-extension in the sense of [NN2], and a P-Galois extension $(x,0,s)$ is a modular extension in the sense of Kersten [Ker]. For $A=(x,r^2,s)$ with $r\neq 0$, if we take $x=ry$, then A is isomorphic to $k[Y]/(Y^3-Y-sr^{-3})=k[y]$ with group $\langle g\rangle$, where $g(y)=1+y$. This extension is called a cyclic 3-extension in [NN1]. Conversely, if $k[y]=k[Y]/(Y^3-Y-s)$ $(s\in k)$ is a cyclic 3-extension, then it is a P-Galois extension with $\Lambda(y)=1$ and $\sigma(y)=1+y$. If P-Galois extensions $A_1=(x_1,r_1^2,s_1)$ and $A_2=(x_2,r_2^2,s_2)$ are isomorphic, then the map

$$\begin{aligned}\psi : k[y_1] &= k[Y_1]/(Y_1^3-Y_1-s_1r_1^{-3}) \to k[y_2]\\ &= k[Y_2]/(Y_2^3-Y_2-s_2r_2^{-3})\end{aligned}$$

defined by $\psi(y_1)=ur_1^{-1}+y_2$ is an isomorphism for the corresponding cyclic 3-extensions. The converse is not true.

We know that the set of isomorphism classes $\mathrm{Gal}(R,G)$ of Galois extensions of R with group G has a group structure (cf. [H], [CS]), and for several cases, we see the structure of $\mathrm{Gal}(R,G)$ (cf. [CS], [N2]). On the other hand it is not known that the set of isomorphism classes $\mathrm{Gal}(R,P)$ of P-Galois extensions of R has a group structure or not. But by theorems 2.4 and 2.5, we can compute the cardinality of $\mathrm{Gal}(k,P)$ in our case.

References

[CS] Chase S.U. and Sweedler M.E., *Hopf Algebras and Galois Theory.* Lecture Note in Math. **97** (1969), Springer-Verlag, Berlin, 1969.

[H] Harrison D.K., *Abelian extension of commutative rings.* Mem. Amer. Math. Soc. **52** (1965), 1–14.

[Ker] Kersten I., *Modulare Ringerweiterrungen,* Abh. Math. Sem. Univ. Hamburg **51** (1981), 29–37

[K1] Kishimoto K., *On P-Galois extensions of rings of cyclic type.* Hokkaido Math. J. **20** (1991), 123–133.

[K2] Kishimoto K., *Finite posets P and P-Galois extensions of rings.* Math. J. Okayama Univ. **34** (1992), 21–47.

[NN1] Nagahara T. and Nakajima A., *On cyclic extensions of commutative rings.* Math. J. Okayama Univ. **15** (1971), 81–90.

[NN2] Nagahara T. and Nakajima A., *On strongly cyclic extensions of commutative rings.* Math. J. Okayama Univ. **15** (1971), 91–100.

[N1] Nakajima A., *Weak Hopf Galois extensions and P-Galois extensions of a ring.* Comm. in Alg. **23** (1995), 2851–2862.

[N2] Nakajima A., *P-polynomials and H-Galois extensions.* J. Alg. **110** (1987), 124–133.

Department of Mathematical Science
Faculty of Environmental Science and Technology
Okayama University
Tsushima, Okayama 700-8530, Japan
E-mail: nakajima@math.ems.okayama-ac.jp