On isomorphism class groups of non-commutative quadratic Galois extensions

Atsushi Nakajima*

*Okayama University

ON ISOMORPHISM CLASS GROUPS
OF NON-COMMUTATIVE QUADRATIC
GALOIS EXTENSIONS

Dedicated to Professor Manabu Harada on his 60th birthday

ATSUSHI NAKAJIMA

0. Introduction. Let R be a commutative ring with identity 1 and let J be a bialgebra over R. An R-algebra A is called a *left J-comodule algebra* if there exists an R-algebra morphism $\rho: A \to J \otimes_R A$ such that $(I \otimes \rho)\rho = (\Delta \otimes I)\rho$ and $(\varepsilon \otimes 1)\rho = I$, where Δ is the comultiplication of J, ε is the counit of J and I is the identity morphism. Let B be an R-subalgebra of A. An R-algebra extension A/B is called a *J-extension* if A is a left J-comodule algebra and B is the *invariant subalgebra* $A_0 = \{a \in A \mid \rho(a) = 1 \otimes a\}$ by ρ. Moreover A/B is called a *J-Galois extension* if A is a J-extension such that the morphism $\gamma: A \otimes_B A \to J \otimes_R A$ defined by $\gamma(x \otimes_B y) = \rho(x)(1 \otimes_R y) \cdot$ is an isomorphism.

Now let J be a free R-module with basis $\{1, \theta\}$. Then in [3], Kreimer showed that J has the following structure :

$$\theta^2 = q\theta, \quad \Delta(\theta) = \theta \otimes 1 + 1 \otimes \theta + p\theta \otimes \theta \quad \text{and} \quad \varepsilon(\theta) = 0,$$

where $p, q \in R$ and $\otimes = \otimes_R$. Moreover

(H) $\qquad\qquad$ J is a Hopf algebra if and only if $pq + 2 = 0$.

In this paper we will treat free quadratic J-Galois extensions for the bialgebra J defined above. For a free quadratic J-extension A/B with right B-basis $\{1, x\}$, a left J-comodule structure morphism $\rho: A \to J \otimes_R A$ is given by

$$\rho(x) = 1 \otimes x + \theta \otimes c + \theta \otimes xd \quad (c, d \in B).$$

So in sections 1 and 2, we will discuss the case of $d = 0$ and of d is invertible, respectively. In both cases, we can define two kind of products on a certain set of isomorphism classes of free quadratic J-Galois extensions and, under these products they have non-commutative semi-group structure which are anti-isomorphic to each other. These structure does not coincide with Kishimoto's product [4] and Nagahara's product [5] which is a generalization of Kishimoto's one. But if $B = R$, then they are isomorphic to the group of

47

commutative Galois J-objects in the sense of Chase-Sweedler [1].

Throughout the following, R is a commutative ring with identity 1, A is an R-algebra with R-subalgebra B which has the same identity 1 and J is a free quadratic bialgebra defined above. All things are treated in the category of unitary R-modules unless otherwise stated. This means that all morphisms are R-linear, $\otimes = \otimes_R$ and etc.

1. Preliminaries. Let A be an R-algebra which is a free right B-module with basis $\{1, x\}$. We set

$$bx = x\sigma(b) + D(b) \quad (b \in B),$$
$$x^2 = xm + n \quad (m, n \in B).$$

Then it is easy to see that σ is a ring homomorphism of B with $\sigma(1) = 1$, and D is a $(\sigma, 1)$-derivation of B, that is,

$$D(rs) = D(r)\sigma(s) + rD(s).$$

Moreover by $b(xm + n) = bx^2$ and $x^3 = x(xm + n) = (xm + n)x$, we have the following relations which were discussed by Cohn in [2, pp. 532−533].

(1) $\qquad\qquad (D\sigma + \sigma D)(b) = (m_r\sigma - m\sigma^2)(b)$

(2) $\qquad\qquad (D^2 - m_rD)(b) = (n_r - n\sigma^2)(b)$

(3) $\qquad\qquad D(m) = m(m - \sigma(m)) + n - \sigma(n)$

(4) $\qquad\qquad\quad D(n) = n(m - \sigma(m)),$

where m_r is the right multiplication of m.

In the following we denote the ring extension A of B stated above by $B[x; m, n, \sigma, D]$ and we call it a *free quadratic extension* of B. Now we assume that $A = B[x; m, n, \sigma, D]$ is a J-extension with left J-comodule structure morphism ρ. Noting that $J \otimes A$ has a right B-module basis $\{1 \otimes 1, 1 \otimes x, \theta \otimes 1, \theta \otimes x\}$, B is the invariant subalgebra of A by ρ and $(\varepsilon \otimes 1)\rho(x) = x$, ρ is given by

(5) $\qquad\qquad \rho(x) = 1 \otimes x + \theta \otimes c + \theta \otimes xd \quad (c, d \in B).$

Since ρ is a ring homomorphism and $\rho(b) = 1 \otimes b$ $(b \in B)$, we have the following relations :

(6) $\qquad\qquad\qquad\qquad cd = cp,$

(7) $\qquad\qquad\qquad\qquad d^2 = dp,$

$$(8) \qquad cm = D(c)(1+dq)+n\{d+\sigma(d)+\sigma(d)dq\}+c^2q,$$

$$(9) \qquad dm = (1+dq)c+\{\sigma(c)+D(d)+m\sigma(d)\}(1+dq)+md,$$

$$(10) \qquad D(b)d = c\sigma(b)-bc \quad (b \in B),$$

$$(11) \qquad d\sigma(b) = \sigma(b)d \quad (b \in B).$$

Now, since ρ is right B-linear, we can define the right A-linear morphism $\gamma\colon A \otimes_B A \to J \otimes A$ by $\gamma(s \otimes_B t) = \rho(s)(1 \otimes t)$. Then the following are easily obtained.

γ is an epimorphism if and only if there exist elements b_1, b_2 in B such that the following equations satisfy.

$$(12) \qquad cb_1+\{D(c)+n\sigma(d)\}b_2 = 1$$

$$(13) \qquad db_1+\{\sigma(c)+m\sigma(d)+D(d)\}b_2 = 0.$$

γ is a monomorphism if and only if the following equations with indeterminates s_1 and s_2 have only the trivial solutions.

$$(14) \qquad cs_1+\{D(c)+n\sigma(d)\}s_2 = 0$$

$$(15) \qquad ds_1+\{\sigma(c)+m\sigma(d)+D(d)\}s_2 = 0.$$

It is known that a left J-comodule structure of A induces a left J^*-module structure (cf. [1, p. 56]), where $J^* = \mathrm{Hom}_R(J, R)$, the dual bialgebra of J. So in our case, using the dual basis $\{1, \theta^*\}$ of J^* with respect to $\{1, \theta\}$, the left J^*-module structure of A induced by (5) is given by

$$\theta^*(x) = xd+c,$$

and when this is the case, the bialgebra structure of J^* is given by

$$\Delta(\theta^*) = 1 \otimes \theta^*+\theta^* \otimes 1+q\theta^* \otimes \theta^*, \ (\theta^*)^2 = p\theta^* \text{ and } \varepsilon(\theta^*) = 0$$

(only replace p with q in the structure of J). Thus the cases of $d = 0$ and of d is invertible are interesting. So in the following two sections, we will treat the cases that $d = 0$ and d is invertible.

2. In case of d = 0. Let $A = B[x; m, n, \sigma, D]$ be a J-Galois extension of B with structure morphism ρ given by

$$\rho(x) = 1 \otimes x+\theta \otimes c.$$

Then by the theorem below, we will prove that $p = 0$, c is invertible and the characteristic of R is 2. So if we set $y = xc^{-1}$, then $\{1, y\}$ is a free right B-module basis of A and our result contains the following two cases.

(i)   If $q = 0$, then θ^* is a nilpotent derivation with nilpotency index two which acts on A as $\theta^*(y) = 1$.

(ii)   If q is invertible, then $\xi = 1 + q\theta^*$ generates a cyclic group of order two which acts on A as $\xi(y) = y + q$.

The case (i) is a purely inseparable extension and the case (ii) is a cyclic extension in the sense of [6].

First, we will prove the structure theorem of this free quadratic J-Galois extension.

Theorem 2.1.   *Let* $A = B[x; m, n, \sigma, D]$ *be a free quadratic J-Galois extension of B with structure morphism ρ which is given by $\rho(x) = 1 \otimes x + \theta \otimes c$. Then*

(a)   *R has characteristic 2 and c is invertible.*

(b)   *J is a Hopf algebra.*

(c)   *There exists a derivation D_1 of B and a free basis $\{1, y\}$ such that* $A = B[y; q, nc^{-2}, 1, D_1]$.

(d)   *$D_1(nc^{-2}) = 0$, $D_1^2 + qD_1 = I_{nc^{-2}}$ and $\rho(y) = 1 \otimes y + \theta \otimes 1$, where $I_{nc^{-2}}$ is the inner derivation defined by nc^{-2}.*

Conversely, assume that R has characteristic 2, J is a Hopf algebra with $p = 0$ in (H) and $A = B[x; q, s, I, D]$ is a free quadratic extension of B. If we define a right B-linear morphism $\rho : A \to J \otimes A$ by $\rho(x) = 1 \otimes \theta + x \otimes 1$, then ρ gives a left J-comodule algebra structure and A is a J-Galois extension of B.

Proof.   Since $d = 0$ in (5), then we have by (8) and (9),

$$(16) \qquad D(c) = cm - c^2 q \quad \text{and} \quad \sigma(c) = -c.$$

By (12) and (16), $c(b_1 + mb_2 - cqb_2) = 1$ and so c is invertible. Then by (6), $p = 0$ and by (10), we obtain

$$(17) \qquad \sigma(b) = c^{-1}bc \quad \text{for any} \quad b \in B.$$

Thus by $\sigma(c) = -c$, the characteristic of R is 2 and so by (H), J is a Hopf algebra. These show (a) and (b). Now we set $y = xc^{-1}$. Then $c_r^{-1}D$ is a derivation and

$$by = yb + c_r^{-1}D(b) \quad \text{and} \quad \rho(y) = 1 \otimes y + \theta \otimes 1.$$

Moreover using (16), $D(c^{-1}) = -c^{-1}D(c)c^{-1}$ and the characteristic of R is 2, we get

$$y^2 = (xm+n)c^{-2}+xc^{-1}D(c)c^{-2}$$
$$= x(m+c^{-1}D(c))c^{-2}+nc^{-2}$$
$$= xcqc^{-2}+nc^{-2}$$
$$= yq+nc^{-2},$$

and by $D(c^{-2}) = c^{-1}D(c)c^{-2}+c^{-2}D(c)c^{-1} = mc^{-2}+c^{-1}mc^{-1}$, (4) and (17), we also have

$$c_r^{-1}D(nc^{-2}) = \{D(n)\sigma(c^{-2})+nD(c^{-2})\}c^{-1}$$
$$= n\{m-\sigma(m)\}c^{-3}+n(mc^{-2}+c^{-1}mc^{-1})c^{-1}$$
$$= 0.$$

Finally by (16), (2) and (17), we have

$$\{(c_r^{-1}D)^2+qc_r^{-1}D\}(b) = \{D^2(b)\sigma(c^{-1}+D(b)D(c^{-1})+qD(b)\}c^{-1}$$
$$= \{D^2(b)+D(b)c^{-1}(cm-c^2q)+qD(b)c\}c^{-2}$$
$$= (D^2+m_rD)(b)c^{-2}$$
$$= bnc^{-2}-nc^{-2}b$$
$$= I_{nc^{-2}}(b).$$

Thus (c) and (d) are proved.

Conversely, assume that R has characteristic 2 and J is a Hopf algebra with $p = 0$ in (H). In the quadratic extension $A = B[x ; q, s, I, D]$, if we define a B-linear morphism $\rho : A \to J \otimes A$ by $\rho(x) = 1 \otimes x + \theta \otimes 1$, then it is easy to see that A is a J-extension of B. Moreover the equations (12) and (13) have the solution, and (14) and (15) are only the trivial solution. Thus A is a J-Galois extension of B, completing the proof.

Note that $D(s) = 0$ and $D^2+qD = I_s$ are obtained by (2) and (4). Now we denote the J-Galois extension A discussed above by $B[x; s, D]$ and we call it a *derivation type*. This means that there exists a derivation D of B and the strucutre of free quadratic extension $B[x; s, D]$ is defined by

(d-1) $x^2 = xq+s, \quad \rho(x) = 1 \otimes x + \theta \otimes 1,$
(d-2) $D^2+qD = I_s, \quad D(s) = 0.$

Two J-Galois extensions S and T are *isomorphic* if there exists a B-B-bilinear and an algebra isomorphism $\varphi : S \to T$ such that $\rho_T\varphi = (I \otimes \varphi)\rho_S$.

Theorem 2.2. *Let $S = B[x; s, D]$ and $T = B[y; t, E]$ be J-Galois extensions defined above. Then S is isomorphic to T as J-Galois extensions*

if and only if there exists an element b_0 in B such that

$$(18) \qquad b_0^2 + q b_0 + E(b_0) = s + t \quad and \quad D - E = I_{b_0}.$$

When this is the case, the isomorphism $\varphi : S \to T$ is given by $\varphi(x) = y + b_0$.

Proof. We set $\varphi(x) = yb_1 + b_0$ $(b_0, b_1 \in B)$. Then by $\rho_T \varphi = (I \otimes \varphi)\rho_S$, $b_1 = 1$. Since φ is a B-B-bilinear and an algebra morphism, $(D - E)(b) = bb_0 - b_0 b = I_{b_0}$ $(b \in B)$ and $b_0^2 + q b_0 + E(b_0) = s + t$ are easily seen.

Conversely if there exists an element $b_0 \in B$ which satisfies the condition (18), then the B-B-linear morphism φ defined by $\varphi(x) = y + b_0$ is an algebra isomorphism.

Two J-Galois extensions $S = B[x\,;\,s, D]$ and $T = B[y\,;\,t, E]$ are called *strongly isomorphic* if there exists an element $r \in R$ such that the algebra isomorphism $\varphi : S \to T$ is given by $\varphi(x) = y + r$ and φ is called a *strong isomorphism*. Then by Th. 2.2, if $B[x\,;\,s, D]$ and $B[y\,;\,t, E]$ are strongly isomorphic then there exists an element $r \in R$ such that

$$(\text{SI-d}) \qquad r^2 + q r = s + t \quad and \quad D = E.$$

A J-Galois extension $A = B[x\,;\,s, D]$ of B is called a *strongly J-Galois* if s is contained in R. Thus by (d-2),

$$(\text{SG-d}) \qquad \text{If } B[x\,;\,s, D] \text{ is strongly } J\text{-Galois, then} \quad D^2 + qD = 0.$$

Note that in the conditions (SI-d) and (SG-d), if R is the center of B, then the converse parts are also true.

In the rest of this section, we assume that B is a flat R-module. Now, the next two theorems need to define a product in a certain set of isomorphism classes of $B[x\,;\,s, D]$.

Theorem 2.3r. *Let $S = B[x\,;\,s, D]$ be a strongly J-Galois extension of B and let $T = B[y\,;\,t, E]$ be a J-Galois (resp. strongly J-Galois) extension of B. Then there exists a J-Galois (resp. strongly J-Galois) extension $S \times_r T$ of $R \otimes B = B_r \cong B$ in $S \otimes T$ which is contained in the $\ker(\xi)$, where $\xi = \rho_S \otimes I - (tw \otimes I)(I \otimes \rho_T) : S \otimes T \to J \otimes S \otimes T$ and $tw : s \otimes t \to t \otimes s$ (the twist morphism). When this is the case,*

$$S \times_r T = B_r[x \otimes 1 + 1 \otimes y\,;\, s \otimes 1 + 1 \otimes t, \, D \otimes 1 + 1 \otimes E]$$
$$= B_r[x \otimes 1 + 1 \otimes y\,;\, 1 \otimes (s+t), \, 1 \otimes E].$$

Proof. We set $z = x \otimes 1 + 1 \otimes y$ and $F = D \otimes 1 + 1 \otimes E$. As is easily

seen, z is contained in the $\ker(\xi)$ and F is a derivation on $R \otimes B = B_r \cong B$ such that $F^2 + qF = I_{s \otimes 1 + 1 \otimes t}$ and $F(s \otimes 1 + 1 \otimes t) = 0$. Moreover we have

$$z^2 = zq + (s \otimes 1 + 1 \otimes t) = zq + 1 \otimes (s + t) \text{ and}$$
$$bz = (1 \otimes b)(x \otimes 1 + 1 \otimes y) = zb + F(1 \otimes b) = zb + 1 \otimes E(b).$$

Since $\ker(\xi)$ is a left J-comodule with structure morphism $\rho_s \otimes I = (tw \otimes I)$ $(I \otimes \rho_T)$ such that $(\rho_s \otimes I)(z) = 1 \otimes z + \theta \otimes 1 \otimes 1$, then by Th. 2. 1, the subring $S \times_r T$ generated by B_r and z in $S \otimes T$ is a J-Galois extension of $B_r = B$, and the structure of $S \times_r T$ as a J-Galois extension is clear, completing the proof.

Theorem 2.4r. *Let* $S = B[x ; s, D]$ *be a strongly J-Galois extension of B and let* $T_i = B[y_i ; t_i, E_i]$ *be J-Galois extensions of* B $(i = 1, 2)$. *If T_1 and T_2 are isomorphic (resp. strongly isomorphic) as J-Galois extensions, then $S \times_r T_1$ and $S \times_r T_2$ are isomorphic (resp. strongly isomorphic) as J-Galois extensions of $B_r \cong B$.*

Proof. Since T_1 and T_2 are isomorphic (resp. strongly isomorphic) as J-Galois extensions, then by Th. 2. 2 there exists an element $b \in B$ (resp. $b \in R$) such that $b^2 + qb + E_2(b) = t_1 + t_2$ and $E_1 - E_2 = I_b$ (resp. $b^2 + qb = t_1 + t_2$ and $E_1 - E_2 = 0$). By Th. 2. 3r,

$$S \times_r T_1 = B_r[z_1 ; s \otimes 1 + 1 \otimes t_1, D \otimes 1 + 1 \otimes E_1]$$

and

$$S \times_r T_2 = B_r[z_2 ; s \otimes 1 + 1 \otimes t_2, D \otimes 1 + 1 \otimes E_2],$$

where $z_i = x \otimes 1 + 1 \otimes y_i$ $(i = 1, 2)$. Define a morphism $\varphi: S \times_r T_1 \to S \times_r T_2$ by $\varphi(z_1) = z_2 + 1 \otimes b$. Then by Th. 2. 2, φ is an isomorphism of J-Galois (resp. strongly J-Galois) extension, completing the proof.

The above two theorems are right and left symmetric, so we have the following

Theorem 2.3l. *Let* $S = B[x ; s, D]$ *be a J-Galois (resp. strongly J-Galois) extension of B and let $T = B[y ; t, E]$ be a strongly left J-Galois extension. Then there exists a J-Galois (resp. strongly J-Galois) extension $S \times_l T$ of $B \otimes R = B_l \cong B$ in $S \otimes T$ which is contained in the $\ker(\xi)$,*

where ξ is defined in Th. 2.3r. *When this is the case,*

$$S \times_l T = B_l[x \otimes 1 + 1 \otimes y ; s \otimes 1 + 1 \otimes t, D \otimes 1 + 1 \otimes E]$$
$$= B_l[x \otimes 1 + 1 \otimes y ; (s+t) \otimes 1, D \otimes 1].$$

Theorem 2.4l. *Let $S_i = B[x_i ; s_i, D_i]$ be J-Galois extensions of B $(i = 1, 2)$ and let $T = B[y ; t, E]$ be a strongly J-Galois extension of B. If S_1 and S_2 are isomorphic (resp. strongly isomorphic) as J-Galois extensions, then $S_1 \times_l T$ and $S_2 \times_l T$ are isomorphic (resp. strongly isomorphic) as J-Galois extensions of $B_l \cong B$.*

Remark 2.5. For J-Galois extensions $S = B[x ; s, D]$ and $T = B[y ; t, E]$, our product $S \times_r T$ (resp. $S \times_l T$) is considered as a subset of $S \otimes T$. It is reasonable because if $B = R$, then $S \times_r T$ (resp. $S \times_l T$) is the usual product of Galois J-objects in the sense of Chase-Sweedler [1].

Let $S_i = B[x_i ; s_i, D_i]$ and $T_j = B[y_j ; t_j, E_j]$ be strongly J-Galois extensions of $B (i, j = 1, 2)$. Then by Th. 2.3r, we have strongly J-Galois extensions $S_i \times_r T_j$ of $B \cong B_r = R \otimes B$. Assume that $\varphi : S_1 \to S_2$ (resp. $\psi : T_1 \to T_2$) is a strong isomorphism such that $\varphi(x_1) = x_2 + b$ for some $b \in R$ (resp. $\psi(y_1) = y_2 + c$ for some $c \in R$). Then we have the following diagram of strongly J-Galois extensions of B:

$$
\begin{array}{ccc}
S_1 \times_r T_1 & \xrightarrow{\ \Phi_1\ } & S_1 \times_r T_2 \\
\downarrow{\scriptstyle \Psi_1} & & \downarrow{\scriptstyle \Psi_2} \\
S_2 \times_r T_1 & \xrightarrow{\ \Phi_2\ } & S_2 \times_r T_2,
\end{array}
$$

where Φ_i and Ψ_i are defined as follows. For $z_{ij} = x_i \otimes 1 + 1 \otimes y_j$ in $S_i \times_r T_j$, $\Phi_i(z_{i1}) = z_{i2} + 1 \otimes b$ and $\Psi_j(z_{1j}) = z_{2j} + 1 \otimes c$. By $b^2 + qb = s_1 + s_2$, $c^2 + qc = t_1 + t_2$ and $b, c \in R$, Φ_i and Ψ_j are strong isomorphisms by Th. 2.4r. And the commutativity of the above diagram is easily seen. Therefore we can define a *right product* on the set of strongly isomorphic classes of strongly J-Galois extensions $\mathrm{Gal}_s(B, J)$ of B of derivation type as follows : For $(S), (T)$ in $\mathrm{Gal}_s(B, J)$,

$$(S) \times_r (T) = (S \times_r T).$$

Now we will prove the following

Theorem 2.6. *Let $\mathrm{Gal}_s(B, J)$ be defined above. For a fixed derivation*

D, we set $\operatorname{Gal}_s(B, J)_D$ the strongly isomorphic classes of strongly J-Galois extensions of type $B[x; s, D]$.

(a)   If there exist two distinct derivations D_i of B such that $D_i^2 + qD_i = I_{s_i}$ ($i = 1, 2$), then $\operatorname{Gal}_s(B, J)$ is a non-commutative semi-group with respect to $\times_r$ and has no right identity.

(b) $\operatorname{Gal}_s(B, J) = \bigcup_D \operatorname{Gal}_s(B, J)_D$ and $\operatorname{Gal}_s(B, J)_D \cap \operatorname{Gal}_s(B, J)_E = \phi$ if $D \neq E$.

(c)   If there exists an element b in B such that $b^2 + qb$ in R and if B has a derivation D such that $D^2 + qD = 0$, then $(B[x; b^2 + qb, D])$ is a left identity of $\operatorname{Gal}_s(B, J)$.

(d)   If $\operatorname{Gal}_s(B, J)_D$ is non-empty, then it is an abelian subgroup of $\operatorname{Gal}_s(B, J)$ with exponent 2.

(e)   If R is the center of B and if there exists derivation D of B such that $D^2 + qD = 0$, then $\operatorname{Gal}_s(B, J)_D$ is isomorphic to the additive group $R^+/\{r^2 + qr \mid r \in R\}$, where R^+ is the additive group of R.

Proof.   Let $S = B[x; s, D]$ and $T = B[y; t, E]$ be strongly J-Galois extensions of B. Then by Th. 2.3r,

$$S \times_r T = B_r[x \otimes 1 + 1 \otimes y; 1 \otimes (s+t), 1 \otimes E]$$

and

$$T \times_r S = B_r[y \otimes 1 + 1 \otimes x; 1 \otimes (t+s), 1 \otimes D]$$

(a)   By (SI-d), if $S \times_r T$ is strongly isomorphic to $T \times_r S$ as strongly J-Galois extensions, then there exists an element $b \in R$ such that

$$b^2 + qb = 0 \quad \text{and} \quad D = E.$$

So if $D \neq E$, then $S \times_r T$ and $T \times_r S$ are not strongly isomorphic, and hence the product $\times_r$ is non-commutative. The associativity of $\times_r$ is easily proved by Th. 2.3r. Moreover for a strongly J-Galois extension $S_1 = B[x_1; s_1, D_1]$, if $S \times_r S_1$ is strongly isomorphic to S, then $S = B[x, t^2 + qt, D_1]$, which means $D = D_1$ by (SI-d). Thus $\operatorname{Gal}_s(B, J)$ has no right identity.

(b)   If S and T are strongly isomorphic, then by (SI-d), $D = E$. Therefore $\operatorname{Gal}_s(B, J) = \bigcup_D \operatorname{Gal}_s(B, J)_D$ and $\operatorname{Gal}_s(B, J)_D \cap \operatorname{Gal}_s(B, J)_E = \phi$ if $D \neq E$ are easily seen.

(c)   By the definition of $\times_r$ and (SI-d), if $S \times_r T$ is strongly isomorphic to T, then there exists an element c in R such that $c^2 + qc = s$. Thus by $D^2 + qD = 0 = I_s$, $(S) = (B[x; c^2 + qc, D])$ is a left identity.

                              A. NAKAJIMA

(d)　If $S \times_r T$ is strongly isomorphic to S, then as a similar compu-
tation as above shows that $T \cong B[y ; c^2 + qc, D]$ for some element $c \in R$,
and $(T) = (B[y ; c^2 + qc, D]$ is unique in $\mathrm{Gal}_s(B, J)_D$, because for any $c, e \in$
$R, B[y ; c^2 + qc, D]$ is strongly isomorphic to $B[z ; e^2 + qe, D]$ by (SI-d).
So by the definition of $\times_r$, $\mathrm{Gal}_s(B, J)_D$ is an abelian group with identity
$(B[y ; c^2 + qc, D])$ $(c \in R)$. Moreover by Th. 2. 3r, $S \times_r S \cong B[y ; 0, D]$
and so $\mathrm{Gal}_s(B, J)_D$ has exponent 2.

(e)　For any $s \in R$, since $B[x ; s, D]$ is a strongly J-Galois extension,
we can define a morphism $\varphi : R^+ \to \mathrm{Gal}_s(B, J)_D$ by $\varphi(s) = (B[x ; s, D])$.
As is easily seen, φ is a group homomorphism with kernel $\{r^2 + qr \mid r \in R\}$.
Conversely for a strongly J-Galois extension $S = B[x ; s, D]$, the structure
of S is given by Th. 2. 1 and in our case, $D^2 + qD = 0 = I_s$. Thus s is
contained in R, which shows that φ is an epimorphism, completing the proof.

These results are also true for the *left product*

$$(S) \times_l (T) = (S \times_l T)$$

in $\mathrm{Gal}_s(B, J)$.

Theorem 2.7.　*The identity morphism*

$$I : \mathrm{Gal}_s(B, J) \to \mathrm{Gal}_s(B, J)$$

gives the anti-isomorphism from the right product $\times_r$ *to the left product* $\times_l$.

3. In case of d is invertible.　Let $A = B[x ; m, n, \sigma, D]$ be a J-Galois
extension of B with struture morphism ρ given by (5). Assume that d is
invertible in (5). Then by (7), $d = p$ is invertible. Using (12) and (13),
we have

$$-c\sigma(c) - cmp + D(c)p + np^2 \in U(B),$$

where $U(B)$ is the set of all invertible elements in B. And by (8) and (10),
we also have

$$
\begin{aligned}
& -c\sigma(c) - cmp + D(c)p + np^2 \\
&= -c\sigma(c) - \{D(c)p + c^2\}pq - np^2(1 + pq) \\
&= -\{c\sigma(c) + np^2\}(pq + 1).
\end{aligned}
$$

Thus

(19)　　　　　　　　$c\sigma(c) + np^2, \ pq + 1 \in U(B)$.

On the other hand, $(pq+1)\{c+\sigma(c)+mp\} = 0$ by (9) and so

(20) $$mp = -\{c+\sigma(c)\}.$$

Multiplying (8) by p and using (10) and (20), we can show that

$$\{c\sigma(c)+np^2\}(pq+2) = 0.$$

Therefore $pq+2 = 0$, which means that J is a Hopf algebra by (H). Now we set

$$y = xp+c \quad \text{and} \quad \xi = 1+\theta p.$$

Then by the invertibility of p and $pq+2 = 0$, $\{1, \xi\}$ is a free basis of J and ξ is a group-like element with $\xi^2 = 1$. Thus $J = R[\xi]$ is a group algebra. Moreover, $\{1, y\}$ is a free basis of A as a right B-module and by using (10), (20) and (19),

$$y^2 = c\sigma(c)+np^2, \; by = y\sigma(b) \quad \text{and} \quad \rho(y) = \xi \otimes y.$$

Therefore we have the following structure theorem which corresponds to Th. 2. 1.

Theorem 3.1. *Let* $A = B[x; m, n, \sigma, D]$ *be a free quadratic J-Galois extension of B with structure morphism ρ given by*

$$\rho(x) = 1 \otimes x + \theta \otimes c + \theta \otimes xd$$

with invertible element d in B. Then

(a)   *J is a Hopf algebra such that $J = R[\xi]$, where ξ is a group-like element of order 2.*

(b)   *There exists a free basis $\{1, y\}$ such that $A = B[y; 0, c\sigma(c)+np^2, \sigma, 0]$ and $c\sigma(c)+np^2$ is in $U(B)$.*

(c)   *σ^2 is the inner automorphism defined by $c\sigma(c)+np^2$ and $\rho(y) = \xi \otimes y$.*

Conversely, assume that J is a Hopf algebra such that p is invertible in (H) *and $A = B[x; 0, s, \sigma, 0]$ is a free quadratic extension of B with invertible element s in B. If we define a right B-linear morphism $\rho: A \to J \otimes A$ by $\rho(x) = \xi \otimes x$, then ρ gives a left J-comodule algebra structure and A is a J-Galois extension of B.*

In the above theorem, we set $y = xp+c$. Then $\{1, y\}$ is a free right B-module basis of A, and so our results contains the following two cases.

(i) If $q = 0$, then the characteristic of R is 2. So if we set $\xi^* = p^{-1}\theta^*$, then $\Delta(\xi^*) = \xi^* \otimes 1 + 1 \otimes \xi^*$ and $(\xi^*)^2 = \xi^*$. Thus ξ^* is a non-nilpotent derivation which acts on A by $\xi^*(y) = y$.

(ii) If q is invertible, then 2 is invertible. If we set $\xi^* = 1 + q\theta^*$, then $\Delta(\xi^*) = \xi^* \otimes \xi^*$ and $(\xi^*)^2 = 1$. So ξ^* is a group-like element of order 2 which acts on A by $\xi^*(y) = -y$.

We denote the J-Galois extension A defined above by $B[x; s, \sigma]$ and we call it an *automorphism type*. This means that there exists an automorphism σ of B and the free quadratic extension $B[x; s, \sigma]$ is defined by

(a-1) $x^2 = s \in U(B),\ \rho(x) = \xi \otimes x,$
(a-2) $\sigma^2(b) = \tilde{s}(b) = s^{-1}bs,$

where $J = R[\xi]$.

Theorem 3.2. *Let $S = B[x; s, \sigma]$ and $T = B[y; t, \tau]$ be J-Galois extensions defined above. Then S is isomorphic to T as J-Galois extension if and only if there exists an invertible element b_0 in B such that*

$$s = t\tau(b_0)b_0 \quad and \quad \tau(b) = b_0\sigma(b)b_0^{-1} \quad for\ any \quad b \in B.$$

When this is the case, the isomorphism $\varphi: S \to T$ is given by $\varphi(x) = yb_0$.

Proof. We set $\varphi(x) = yb_0 + b_1$ $(b_0, b_1 \in B)$. Then by $\rho_T\varphi = (I \otimes \varphi)\rho_S$ and φ is an isomorphism, we have $b_1 = 0$ and $b_0 \in U(B)$. Since φ is a B-B-linear and an algebra morphism, we have $\tau(b) = b_0\sigma(b)b_0^{-1}$ and $s = t\tau(b_0)b_0$. The converse part is clear.

Now as in section 2, we define that two J-Galois extensions $S = B[x; s, \sigma]$ and $T = B[y; t, \tau]$ are called *strongly isomorphic* if there exists an element $r \in U(R)$ such that the isomorphism $\varphi: S \to T$ is given by $\varphi(x) = yr$ and φ is called a *strong isomorphism*. Then by Th. 3. 2, if $B[x; s, \sigma]$ and $B[y; t, \tau]$ are strongly isomorphic, then there exists an element $r \in U(R)$ such that

(SI-a) $s = tr^2 \quad and \quad \sigma = \tau.$

A J-Galois extension $A = B[x; s, \sigma]$ of B is called a *strongly J-Galois* if s is contained in R. Thus by (a-2),

(SG-a)   If $B[x; s, \sigma]$ is strongly J-Galois, then $\sigma^2 = I$.

Note that in the conditions (SI-a) and (SG-a), if R is the center of B, then the converse parts are also true.

Now, in the rest of this section, we assume that B is a flat R-module. Then we have the similar results as in section 2, Ths. 2.3r and 2.4r, so we omit the proofs.

Theorem 3.3r. Let $S = B[x; s, \sigma]$ be strongly J-Galois extension of B and let $T = B[y; t, \tau]$ be a J-Galois (resp. strongly J-Galois) extension of B. Then there exists a J-Galois (resp. strongly J-Galois) extension $S \times_r T$ of $R \otimes B = B_r \cong B$ in $S \otimes T$ which is contained in the $\ker(\xi)$, where ξ is defined in Th. 2.3r. When this is the case,

$$S \times_r T = B[x \otimes y; s \otimes t, \sigma \otimes \tau]$$
$$= B[x \otimes y; 1 \otimes st, 1 \otimes \tau].$$

Theorem 3.4r. Let $S = B[x; s, \sigma]$ be a strongly J-Galois extension of B and let $T_i = B[y_i; t_i, \tau_i]$ be J-Galois extensions of $B (i = 1, 2)$. If T_1 and T_2 are isomorphic (resp. strongly isomorphic) as J-Galois extensions, then $S \times_r T_1$ and $S \times_r T_2$ are isomorphic (resp. strongly isomorphic) as J-Galois extensions of B.

Similarly we have the following

Theorem 3.3l. Let $S = B[x; s, \sigma]$ be a J-Galois (resp. strongly J-Galois) extension of B and let $T = B[y; t, \tau]$ be a strongly J-Galois extension of B. Then there exists a J-Galois (resp. strongly J-Galois) extension $S \times_l T$ of $B \otimes R = B_l \cong B$ in $S \otimes T$ which contained in the $\ker(\xi)$, where ξ is defined in Th. 2.3r. When this is the case,

$$S \times_l T = B_l[x \otimes y; s \otimes t, \sigma \otimes \tau]$$
$$= B_l[x \otimes y; st \otimes 1, \sigma \otimes 1].$$

Theorem 3.4l. Let $S_i = B[x_i; s_i, \sigma_i]$ be J-Galois extensions of B and let $T = B[y; t, \tau]$ be a strongly J-Galois extension of B. If S_1 and S_2 are isomorphic (resp. strongly isomorphic) as J-Galois extensions, then $S_1 \times_l T$ and $S_2 \times_l T$ are isomorphic (resp. strongly isomorphic) as J-Galois extensions of $B_l \cong B$.

Let $\mathrm{Gal}_s(B, J)$ be the set of strongly isomorphic classes of strongly J-Galois extensions of B of automorphism type. Using Ths. 3.3r and 3.4r,

60   A. NAKAJIMA

for (S) and (T) in $\mathrm{Gal}_s(B, J)$, the right product

$$(S) \times_r (T) = (S \times_r T)$$

is well defined. So we have the following

Theorem 3.5. *Let* $\mathrm{Gal}_s(B, J)$ *be defined above. Let* $\mathrm{Gal}_s(B, J)_\sigma$ *be the set of strongly isomorphic classes of strongly J-Galois extensions of type* $B[x; s, \sigma]$. *Then*

(a) *If there exist two distinct automorphisms* σ_i *such that* $\sigma_i^2 = I$, *then* $\mathrm{Gal}_s(B, J)$ *is a non-commutative semi-group with respect to* $\times_r$ *and has no right identity.*

(b) $\mathrm{Gal}_s(B, J) = \bigcup_\sigma \mathrm{Gal}_s(B, J)_\sigma$ *and* $\mathrm{Gal}_s(B, J)_\sigma \cap \mathrm{Gal}_s(B, J)_\tau = \phi$ *if* $\sigma \neq \tau$.

(c) *If there exists an element* s *in* $U(B)$ *such that* s^2 *in* R *and if* B *has an automorphism* σ *such that* $\sigma^2 = I$, *then* $(B[x; s^2, \sigma])$ *is a left identity in* $\mathrm{Gal}_s(B, J)$.

(d) *If* $\mathrm{Gal}_s(B, J)_\sigma$ *is non-empty, then it is an abelian subgroup of* $\mathrm{Gal}_s(B, J)$ *with exponent 2.*

(e) *If* R *is the center of* B *and there exists an automorphism* σ *of* B *such that* $\sigma^2 = I$, *then* $\mathrm{Gal}_s(B, J)_\sigma$ *is isomorphic to the multiplicative group* $U(R)/U(R)^2$.

Proof. Let $S = [x; s, \sigma]$ and $T = [y; t, \tau]$ be strongly J-Galois extensions of B. Then by Th. 3. 3r,

$$S \times_r T = [x \otimes y; 1 \otimes st, 1 \otimes \tau] \text{ and}$$
$$T \times_r S = [x \otimes y; 1 \otimes ts, 1 \otimes \sigma].$$

(a) If $\sigma \neq \tau$, then by (SI-a), $S \times_r T$ is not strongly isomorphic to $T \times_r S$. Thus the right product is non-commutative. The associativity of $\times_r$ is easily seen by Th. 3. 3r.

(b) is proved as similar as in the proof of Th. 2. 6 (b).

(c) Let $S = [x; s^2, \sigma]$ and $T = [y; t, \tau]$ be strongly J-Galois extensions such that $\sigma \neq \tau$. Then by (SI-a), $S \times_r T$ is strongly isomorphic to T and so $(S) \times_r (T) = (T)$.

(d) By the definition of $\times_r$, $\mathrm{Gal}_s(B, J)_\sigma$ is closed and commutative under $\times_r$. Since for any $t \in U(B)$, $B[x; 1, \sigma]$ is strongly isomorphic to $B[y; t^2, \sigma]$, $\mathrm{Gal}_s(B, J)_\sigma$ has the identity $(B[x; 1, \sigma])$ and $S \times_r S \cong B[y; s^2, \sigma]$ is easily seen.

(e) If we define a morphism $\varphi: U(R) \to \mathrm{Gal}_s(B, J)_\sigma$ by $\varphi(r) = (B[x; r, \sigma])$, then it is easy to see that φ is a group homomorphism with kernel $U(R)^2 = \{\, r^2 \mid r \in U(R)\}$. Moreover if $(B[x; r, \sigma])$ is contained in $\mathrm{Gal}_s(B, J)_\sigma$, then $\sigma^2 = I = \tilde{r}$ and so r is contained in the center of $B = R$, which shows that φ is an epimorphism, completing the proof.

Theorem 3.6. *The identity morphism*

$$I: \mathrm{Gal}_s(B, J) \to \mathrm{Gal}_s(B, J)$$

gives the anti-isomorphism from the right product $\times_r$ to the left product $\times_l$.

4. Relation with another product and remarks. In his paper [4], Kishimoto defined a product on a certain set of isomorphism classes of free quadratic extensions of B for a fixed derivation D or a fixed automorphism σ and proved some results. Kishimoto's set of isomorphism classes and our $\mathrm{Gal}_s(J, B)_D$ does not coincide, but if q is invertible, his product is defined in our set $\mathrm{Gal}_s(J, B)_D$. In [5], Nagahara defined the product in a certain set of quadratic polynomials, and generalized and sharpend of Kishimoto's results. The conditions of Kishimoto's product is complicated and Nagahara's one is more complicated, delicate and classificatory than Kishimoto's one, so in this section we roughly explain the relation of Kishimoto's product and our qroduct, and we also give some examples of strongly J-Galois extensions and etc.

4.1. In case of $2 = 0$. In this subsection we assume that the characteristic of R is 2.

(a) **Kishimoto's product** [4]. Let D be a derivation of B and let b be an element of B such that

(D) $$D(b) = 0 \quad \text{and} \quad D^2 + qD = I_b.$$

We fix these D, b and assume that q is invertible. Consider the free quadratic extension $B[x; s, D] (= B[x_s])$ as in section 2. Kishimoto's product is defined as follows :

$$(B[x_s])(B[x_t]) = (B[x_{s+t+b}]),$$

where $(B[x_s])$ is the B-ring isomorphism class of type $B[x_s]$. Then, under the suitable conditions, the set of B-ring isomorphism classes $P_b^q(B)$ of $B[x_s]$ forms an abelian group with identity element $(B[x_b])$ of exponent 2. In his

62   A. NAKAJIMA

case, $(B[x_b])$ is able to be an identity element in $P_D^q(B)$ for any fixed element b with properties (D) and thus the definition of product relates to b. Under his reasonable complicated conditions [4, section 3], his product is unique in our set $\mathrm{Gal}_s(J, B)_D$ and if R is the center of B and B is flat R-module, then by Th. 2. 6 and [4, Cor. 1],

$$\mathrm{Gal}_s(J, B)_D \cong P_D^q(B) \cong R^+/\{r^2+qr \mid r \in R\}.$$

(b) **Examples.** For $\alpha, \beta \in B$, we set

$$S = B[x; \alpha^2+q\alpha, I_\alpha] \quad \text{and} \quad T = B[y; \beta^2+q\beta, I_\beta].$$

Then by Ths. 2. 1 and 2. 2, S and T are J-Galois extensions of B and they are isomorphic as J-Galois extensions. Moreover S and T are strongly isomorphic if and only if $\alpha+\beta \in R$.

(1) If $\alpha^2+q\alpha$, $\beta^2+q\beta \notin R$ and $\alpha+\beta \in R$, then S and T are not strongly J-Galois extensions but they are strongly isomorphic.

(2) If $\alpha+\beta \notin R$, then S and T is not strongly isomorphic.

(3) If $\alpha^2+q\alpha \notin R$, $\beta^2+q\beta \in R$ and $\alpha+\beta \notin R$, then S is not a strongly J-Galois extension and T is a strongly J-Galois extension, but S and T are isomorphic as J-Galois extensions and they are not strongly isomorphic.

(4) If $\alpha^2+q\alpha$, $\beta^2+q\beta \in R$ and $\alpha+\beta \notin R$, then S and T are strongly J-Galois extensions of B, and they are isomorphic as J-Galois exensions but are not strongly isomorphic.

Now if we take that B is the 2×2-matrix algebra over R, then we can easily find the elements α and β which satisfy the conditions from (1) to (4).

4.2. In case of 2 is invertible. In this subsection, we always assume that 2 is invertible.

(a) **Kishimoto's product [4].** Let σ be an automorphism of B and let u be an invertible element of B such that

(A) $$\sigma(u) = u \quad \text{and} \quad \sigma^2(b) = u^{-2}bu^2.$$

We fix these σ and u. Consider the free quadratic extension $B[x; s, \sigma]$ $(= B[x_s])$ as in section 3. Then the Kishimoto's product in the set of B-ring isomorphism classes $P_\sigma(B)$ of $B[x_s]$ is defined by

$$(B[x_s])(B[x_t]) = B[x_{stu^{-1}}].$$

Then, under the suitable conditions, $P_\sigma(B)$ is an abelian group with identity $(B[x_u])$ of exponent 2. The same problem as in 4.1 for identities happens. But by his reasonable and complicated conditions [4, section 2], his product is unique in our set $\mathrm{Gal}_s(J, B)_\sigma$ and if R is the center of B and B is flat R-module, then by Th. 3.5 and [4, Cor. 2.5],

$$\mathrm{Gal}_s(J, B)_\sigma \cong P_\sigma(B) \cong U(R)/U(R)^2.$$

Finally, we give some examples of strongly J-Galois extensions and etc. in case of 2 is invertible.

(b) **Examples.** For $\alpha, \beta \in U(B)$, we set

$$S = B[x : \alpha^2, \tilde\alpha] \quad \text{and} \quad T = B[y : \beta^2, \tilde\beta].$$

Then by Ths. 3.1 and 3.2, S and T are J-Galois extensions of B and they are isomorphic as J-Galois extensions. Moreover, S and T are strongly isomorphic if and only if $\beta^{-1}\alpha \in R$.

(1) If $\alpha^2, \beta^2 \notin R$ and $\beta^{-1}\alpha \in R$, then S and T are not strongly J-Galois extensions, but they are strongly isomorphic.

(2) If $\beta^{-1}\alpha \notin R$, then S and T are not strongly isomorphic.

(3) If $\alpha^2 \notin R$, $\beta^2 \in R$ and $\beta^{-1}\alpha \notin R$, then S is not a strongly J-Galois extension and T is a strongly J-Galois extension, but S and T are isomorphic as J-Galois extensions and they are not strongly isomorphic.

(4) If $\alpha^2, \beta^2 \in R$ and $\beta^{-1}\alpha \notin R$, then S and T are strongly J-Galois extensions and are isomorphic as J-Galois extensions, but they are not strongly isomorphic.

Now if we take that B is the 2×2 matrix algebra over R, then we can easily obtain the elements α and β which satisfy the conditions from (1) to (4).

REFERENCES

[1] S. U. CHASE and M. E. SWEEDLER : Hopf Algebras and Galois Theory, Lecture Notes in Math. 97 (1969), Springer-Verlag, Berlin.

[2] P. M. COHN : Quadratic extensions of skew fields, Proc. London Math. Soc. (3) 11 (1961), 531—556.

[3] H. K. KREIMER : Quadratic Hopf algebra and Galois extensions, Contemporary Math. 13 (1982), 353−361.

[4] K. KISHIMOTO : A classification of free quadratic extensions of rings, Math. J. Okayama Univ. 18 (1976), 139−148.

[5] T. NAGAHARA : On separable polynomials of degree 2 in skew polynomial rings, Math. J.

64   A. NAKAJIMA

Okayama Univ. **19** (1976), 65 −95.

[6]   A. NAKAJIMA :   Free algebras and Galois objects of rank 2, Math. J. Okayama Univ. **23** (1981), 181 −187.

[7]   M. SWEEDLER :   Hopf Algebra, Benjamin, New York, 1969.

DEPARTMENT OF MATHEMATICS
COLLEGE OF LIBERAL ARTS AND SCIENCES
OKAYAMA UNIVERSITY
2-1-1 TSUSHIMA-NAKA, OKAYAMA 700, JAPAN