TSUKUBA J. MATH.
Vol. 13 No. 2 (1989), 353–362

CORINGS AND INVERTIBLE BIMODULES

By

Akira MASUOKA

Introduction.

Let $S\subset R$ be a faithfully flat extension of commutative rings (with 1). Grothendieck's faithfully flat descent theory tells that the relative Picard group $\mathrm{Pic}(R/S)$ is isomorphic to $H^1(R/S, U)$, the Amitsur 1-cohomology group for the units-functor U. We consider the non-commutative version of this fact in this paper.

Let $S\subset R$ be (non-commutative) rings and denote by $\mathrm{Inv}_S(R)$ the group of invertible S-subbimodules of R. Sweedler defined the natural R-coring structure on $R\otimes_S R$. We define the natural group map $\Gamma: \mathrm{Inv}_S(R)\to\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$, where $\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$ denotes the group of R-coring automorphisms of $R\otimes_S R$. When is Γ an isomorphism? The answer presented here is as follows (2.10): *If either*

(a) *R is faithfully flat as a right or left S-module*

or (b) *S is a direct summand of R as a right* (resp. *left*) *S-module and the functor $-\otimes_S R$* (resp. *$R\otimes_S -$*) *reflects isomorphisms,*

then Γ is an isomorphism. Indeed we consider some monoid map $\mathbf{I}_S^l(R)\to\mathrm{End}_{R\text{-cor}}(R\otimes_S R)$, which is an extension of Γ. We have two applications (3.2) and (3.4), both of which are concerned with the Galois theory.

§ 0. Conventions.

Let T, Q be arbitrary rings with 1. We write

$$U(T)=\text{the group of units in } T.$$

All modules are assumed to be unital. A (T, Q)-bimodule means a left T-module and right Q-module M satisfying $(tm)q=t(mq)$ for $t\in T$, $m\in M$ and $q\in Q$. A T-bimodule means a (T, T)-bimodule. We denote by

$${}_T\mathcal{M},\quad \mathcal{M}_T \quad\text{and}\quad {}_T\mathcal{M}_Q$$

the category of left T-modules, of right T-modules and of (T, Q)-bimodules,

Received May 9, 1988.

respectively. For $M \in {}_T\mathcal{M}_T$,

$$M^T = \{m \in M \mid tm = mt \text{ for all } t \in T\}.$$

Throughout this paper, we fix a ring R with 1 and a subring S of R with the same unit 1. For arbitrary S-subbimodules I, $J \subset R$, we define the product by

$$IJ = \{\textstyle\sum_i x_i y_i (\text{finite sum}) \mid x_i \in I,\ y_i \in J\} (\subset R)$$

and denote by $\mathbf{m}$ the multiplication map:

$$\mathbf{m}: I \otimes_S J \longrightarrow IJ, \qquad \mathbf{m}(x \otimes y) = xy.$$

With respect to this product, S-subbimodules of R form a monoid with unit S. $\mathbf{I}_S^l(R)$ (resp. $\mathbf{I}_S^r(R)$) denotes the submonoid consisting of S-subbimodules $I \subset R$ such that

$$R \otimes_S I \cong R \text{ (resp. } I \otimes_S R \cong R) \text{ through } \mathbf{m}.$$

$\mathrm{Inv}_S(R)$ denotes the group of invertible S-subbimodules of R.

§ 1. Preliminaries.

1.1. PROPOSITION. *We have the following exact sequence, the first five terms of which can be found in* [4, PROPOSITION 1.6, p. 25]:

$$1 \longrightarrow U(S^S) \longrightarrow U(R^S) \xrightarrow[u \mapsto Su = uS]{} \mathrm{Inv}_S(R) \xrightarrow[{[-]}]{} \mathrm{Pic}(S) \xrightarrow[R \otimes_S -]{} [{}_R\mathcal{M}_S]$$

where $\mathrm{Pic}(S)$ *denotes the Picard group of* S *and* $[{}_R\mathcal{M}_S]$ *denotes the isomorphic classes* $[M]$ *of* $M \in {}_R\mathcal{M}_S$ *with a distinguished class* $[R]$.

Exactness at $\mathrm{Pic}(S)$ means that, for any invertible S-bimodule J, $R \otimes_S J \cong R$ in ${}_R\mathcal{M}_S$ iff J is isomorphic to some $I \in \mathrm{Inv}_S(R)$, which can be verified easily. Needless to say, we can get another exact sequence from the above one by replacing the last map with $\mathrm{Pic}(S) \xrightarrow[- \otimes_S R]{} [{}_S\mathcal{M}_R]$, defining $[{}_S\mathcal{M}_R]$ similarly. In particular, we have

$$\mathbf{I}_S^l(R) \cap \mathbf{I}_S^r(R) \supset \mathrm{Inv}_S(R). \tag{1.2}$$

An *R-coring* is a triple (C, Δ, ε), where $C \in {}_R\mathcal{M}_R$, and $\Delta: C \to C \otimes_R C$ and $\varepsilon: C \to R$ are maps in ${}_R\mathcal{M}_R$ satisfying the usual co-associativity and co-unitarity. Let C be an R-coring. Denote the monoid of R-coring endomorphisms (resp. the group of R-coring automorphisms) of C by

$$\mathrm{End}_{R\text{-cor}}(C) \text{ (resp. } \mathrm{Aut}_{R\text{-cor}}(C)).$$

If an automorphism f of C in ${}_R\mathcal{M}_R$ commutes with Δ, it commutes with ε automatically, since $\varepsilon\circ f=(\varepsilon\otimes\varepsilon)\circ(id\otimes f)\circ\Delta=\varepsilon\circ f^{-1}\circ(id\otimes\varepsilon)\circ(f\otimes f)\circ\Delta=\varepsilon\circ f^{-1}\circ(id\otimes\varepsilon)\circ\Delta\circ f=\varepsilon$. Denote the set of group-likes [6, 1.7, Definition] in C by $\mathrm{Gr}(C)$:

$$\mathrm{Gr}(C)=\{g\in C \mid \Delta(g)=g\otimes_R g,\ \varepsilon(g)=1\}.$$

$R\otimes_S R$ has the following R-coring structure [6, 1.2, p. 393]:

$$\Delta:\ R\otimes_S R\longrightarrow (R\otimes_S R)\otimes_R(R\otimes_S R)=R\otimes_S R\otimes_S R\,,$$

$$\Delta(x\otimes y)=x\otimes 1\otimes y\,,$$

$$\varepsilon:\ R\otimes_S R\longrightarrow R\,,\qquad \varepsilon(x\otimes y)=xy\,.$$

The natural identification

$$(R\otimes_S R)^S=\mathrm{End}_{{}_R\mathcal{M}_R}(R\otimes_S R)$$

makes the left-hand side into a ring with the following product:

$$(\Sigma_i x_i\otimes y_i)\cdot(\Sigma_j z_j\otimes w_j)=\Sigma_{i,j} z_j x_i\otimes y_i w_j \tag{1.3}$$

for $\Sigma_i x_i\otimes y_i$, $\Sigma_j z_i\otimes w_j\in(R\otimes_S R)^S$. Then we have the identification

$$(R\otimes_S R)^S\cap\mathrm{Gr}(R\otimes_S R)=\mathrm{End}_{R\text{-cor}}(R\otimes_S R)\,, \tag{1.4}$$

$$U((R\otimes_S R)^S)\cap\mathrm{Gr}(R\otimes_S R)=\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$$

as monoids and as groups, respectively.

REMARK. The product (1.3) is related closely to Sweedler's $\times_S$-product [7]. Indeed, the ring $(R\otimes_S R)^S$ equals $\tilde{R}\times_S R$ in [7, Section 3].

§ 2. Main results.

We define the monoid map

$$\Gamma:\ \mathbf{I}_S^l(R)\longrightarrow\mathrm{End}_{R\text{-cor}}(R\otimes_S R)\,. \tag{2.1}$$

Let $I\in\mathbf{I}_S^l(R)$. Define $\Gamma(I)$ to be the composition

$$R\otimes_S R\xrightarrow[\mathbf{m}^{-1}\otimes id]{\sim}R\otimes_S I\otimes_S R\xrightarrow[id\otimes\mathbf{m}]{}R\otimes_S R$$

Explicitly, if $\Sigma_i x_i\otimes y_i\in R\otimes_S I$ goes to $1\in R$ through $\mathbf{m}$,

$$\Gamma(I)(a\otimes b)=\Sigma_i a x_i\otimes y_i b$$

for $a\otimes b\in R\otimes_S R$. Clearly, $\varepsilon\circ\Gamma(I)=\varepsilon$. We have

$$\sum_i x_i\otimes 1\otimes y_i=\sum_{i,j} x_i\otimes y_i x_j\otimes y_j\qquad\text{in } R\otimes_S R\otimes_S I\,,$$

since these go to $\Sigma_i x_i\otimes y_i\in R\otimes_S R$ through $R\otimes_S R\otimes_S I\xrightarrow[id\otimes\mathbf{m}]{\sim}R\otimes_S R$. Hence $\Gamma(I)$

commutes with Δ. Thus $\Gamma(I)\in \mathrm{End}_{R\text{-cor}}(R\otimes_S R)$. It is easy to see that Γ is a monoid map.

2.2. THEOREM. *If either*

(a) *R is faithfully flat as a right S-module*

or (b) *S is a direct summand of R as an S-bimodule,*

then $\Gamma: \mathbf{I}_S^l(R)\to \mathrm{End}_{R\text{-cor}}(R\otimes_S R)$ *is an isomorphism.*

Let

$$\mathbf{J}(g)=\{x\in R \mid g(x\otimes 1)=1\otimes x\} \tag{2.3}$$

for $g\in \mathrm{End}_{R\text{-cor}}(R\otimes_S R)$. In case (a) or (b) holds, we show the map $g\mapsto \mathbf{J}(g)$ gives the inverse of Γ.

Define the maps $d_1, d_2: R\rightrightarrows R\otimes_S R$ by

$$d_1(x)=1\otimes x, \quad d_2(x)=x\otimes 1 \qquad \text{for } x\in R.$$

2.4. LEMMA. *Fix* $g\in \mathrm{End}_{R\text{-cor}}(R\otimes_S R)$ *and write*

$$\iota=\textit{inclusion}: \mathbf{J}(g) \longrightarrow R, \qquad \delta=d_1-g\circ d_2: R\longrightarrow R\otimes_S R.$$

(1) *The following is an exact sequence*:

$$0\longrightarrow \mathbf{J}(g)\xrightarrow{\iota} R\xrightarrow{\delta} R\otimes_S R.$$

(2) *The following is an exact sequence*:

$$0\longrightarrow R\xrightarrow{g\circ d_2} R\otimes_S R\xrightarrow{id\otimes\delta} R\otimes_S R\otimes_S R.$$

Moreover, we have

$$\mathbf{m}\circ(g\circ d_2)=id_R, \quad (g\circ d_2)\circ\mathbf{m}+(\mathbf{m}\otimes id_R)\circ(id_R\otimes\delta)=id_{R\otimes_S R}.$$

(3) *If R is flat as a right S-module, then* $\mathbf{J}(g)\in \mathbf{I}_S^l(R)$.

PROOF. (1) is a restatement of (2.3).

(2) is verified directly.

(3). This follows from the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & R\otimes_S \mathbf{J}(g) \arrow[r, "\mathrm{id}\otimes\iota"] \arrow[d, "\mathbf{m}"'] & R\otimes_S R \arrow[r, "\mathrm{id}\otimes\delta"] \arrow[d, equal] & R\otimes_S R\otimes_S R \arrow[d, equal] \\
0 \arrow[r] & R \arrow[r, "g\circ d_2"] & R\otimes_S R \arrow[r, "\mathrm{id}\otimes\delta"] & R\otimes_S R\otimes_S R,
\end{tikzcd} \tag{2.4.1}$$

where the upper row is exact, since R_S is flat. Q. E. D.

2.5. LEMMA. *Let g, ι, δ be as in* (2.4). *Assume S is a direct summand of R as an S-bimodule. Then we have*:

(1) *There exist $\pi: R\to \mathbf{J}(g)$ and $\phi: R\otimes_S R\to R$ in ${}_S\mathcal{M}_S$ satisfying*

$$\pi\circ\iota=id_{\mathbf{J}(g)}, \qquad \iota\circ\pi+\phi\circ\delta=id_R. \tag{2.5.1}$$

(2) $\mathbf{J}(g)\in\mathbf{I}_S^l(R)$.

PROOF. (1). Let $p: R\to S$ be a projection in ${}_S\mathcal{M}_S$ and take π, ϕ as follows:

$$\pi: R\xrightarrow{d_2} R\otimes_S R\xrightarrow{g} R\otimes_S R\xrightarrow{p\otimes id} R, \qquad \phi: R\otimes_S R\xrightarrow{p\otimes id} R.$$

We show $\pi(R)\subset\mathbf{J}(g)$. Assume $\sum_i x_i\otimes y_i\in\mathrm{Gr}(R\otimes_S R)$ corresponds to g in (1.4). Then, for $a\in R$,

$$\pi(a)=\sum_i p(ax_i)y_i$$

and

$$\begin{aligned}g(\pi(a)\otimes 1)&=\sum_{i,j} p(ax_i)y_jx_j\otimes y_j\\&=\sum_i p(ax_i)\otimes y_i \quad (\text{since } \textstyle\sum x_i\otimes y_ix_j\otimes y_j=\sum x_i\otimes 1\otimes y_i)\\&=1\otimes\pi(a).\end{aligned}$$

Thus $\pi(a)\in\mathbf{J}(g)$. The remainder is verified easily.

(2). This follows, since by (1) the sequence (2.4.1) is exact in case ${}_SS_S\oplus{}_SR_S$, too. Q. E. D.

2.6. DEFINITION. The functor $R\otimes_S-$ (resp. $-\otimes_S R$) *reflects isomorphisms*, if a map f in ${}_S\mathcal{M}$ (resp. in $\mathcal{M}_S$) is an isomorphism whenever $id_R\otimes_S f$ (resp. $f\otimes_S id_R$) is such.

If this is the case, $I\subset J$ for I, $J\in\mathbf{I}_S^l(R)$ (resp. $\in\mathbf{I}_S^r(R)$) implies $I=J$.

2.7. LEMMA. *Let g, $h\in\mathrm{End}_{R\text{-cor}}(R\otimes_S R)$, $I\in\mathbf{I}_S^l(R)$.*

(1) $\mathbf{J}(g)\mathbf{J}(h)\subset\mathbf{J}(gh)$.

(2) *If $\mathbf{J}(g)\in\mathbf{I}_S^l(R)$, then $\boldsymbol{\Gamma}\circ\mathbf{J}(g)=g$.*

(3) *$I\subset\mathbf{J}\circ\boldsymbol{\Gamma}(I)$. Hence, if $\mathbf{J}\circ\boldsymbol{\Gamma}(I)\in\mathbf{I}_S^l(R)$ and $R\otimes_S-$ reflects isomorphisms, then $I=\mathbf{J}\circ\boldsymbol{\Gamma}(I)$.*

PROOF. (1). This holds, since, if $x\in\mathbf{J}(g)$, $y\in\mathbf{J}(h)$,

$$d_1(xy)=d_1(x)y=g\circ d_2(x)y=g(d_2(x)y)=$$
$$g(xd_1(y))=g(xh\circ d_2(y))=g\circ h(xd_2(y))=g\circ h\circ d_2(xy).$$

(2). This follows from the following commutative diagram:

$$\begin{tikzcd}
R\otimes_S R \arrow[d, "\mathbf{m}^{-1}\otimes\mathrm{id}"'] \arrow[dr, equal] \arrow[dd, bend right=60, "\boldsymbol{\Gamma}\circ\mathbf{J}(g)"'] & \\
R\otimes_S \mathbf{J}(g)\otimes_S R \arrow[r, "\mathbf{m}\otimes\mathrm{id}"'] \arrow[d, "\mathrm{id}\otimes\mathbf{m}"'] & R\otimes_S R \arrow[d, "g"'] \\
R\otimes_S R \arrow[r, equal] & R\otimes_S R .
\end{tikzcd}$$

(3). Assume $\sum_i x_i\otimes y_i\in R\otimes_S I$ goes to $1\in R$ through $\mathbf{m}$. Then, for $a\in I$, $\sum_i ax_i\otimes y_i=1\otimes a$ in $R\otimes_S I$, since both sides go to a through $\mathbf{m}$. This implies $I\subset\mathbf{J}\circ\boldsymbol{\Gamma}(I)$. Q.E.D.

PROOF OF (2.2). Under (a) or (b), $R\otimes_S-$ reflects isomorphisms. Hence, by (2.7) we have only to show $\mathbf{J}(g)\in\mathbf{I}^l_S(R)$ for any $g\in\mathrm{End}_{R\text{-cor}}(R\otimes_S R)$. This is shown in (2.4)-(2.5). Q.E.D.

Symmetrically we have the *anti*-monoid map

(2.8) $$\boldsymbol{\Gamma}'\colon \mathbf{I}^r_S(R)\longrightarrow \mathrm{End}_{R\text{-cor}}(R\otimes_S R),$$

defining $\boldsymbol{\Gamma}'(I)$, $I\in\mathbf{I}^r_S(R)$, to be the composition

$$R\otimes_S R \xrightarrow[id\otimes\mathbf{m}^{-1}]{\sim} R\otimes_S I\otimes_S R \xrightarrow[\mathbf{m}\otimes id]{} R\otimes_S R .$$

Let $S^o\subset R^o$ denote the opposite rings of $S\subset R$. By the natural idetification

$$\mathbf{I}^r_S(R)=\mathbf{I}^l_{S^o}(R^o), \qquad R\otimes_S R=R^o\otimes_{S^o}R^o \quad (x\otimes y\leftrightarrow y^o\otimes x^o),$$

we can identify the $\boldsymbol{\Gamma}'$-map (2.8) with the $\boldsymbol{\Gamma}$-map for $S^o\subset R^o$. Hence (2.2) yields the following:

2.9. THEOREM. *If either*

(a) *R is faithfully flat as a left S-module*

or (b) *S is a direct summand of R as an S-bimodule,*

then $\boldsymbol{\Gamma}'\colon \mathbf{I}^r_S(R)\to\mathrm{End}_{R\text{-cor}}(R\otimes_S R)$ is an anti-isomorphism.

The inverse $\mathbf{J}'$ is given by

$$\mathbf{J}'(g)=\{x\in R\mid x\otimes 1=g(1\otimes x)\} \quad (g\in\mathrm{End}_{R\text{-cor}}(R\otimes_S R)).$$

The $\boldsymbol{\Gamma}$-map (2.1) is restricted to the group map $\mathrm{Inv}_S(R)\to\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$, which is called $\boldsymbol{\Gamma}$, too.

2.10. THEOREM. *If either*

(a) *R is faithfully flat as a right or left S-modnle*

or (b) *S is a direct summand of R as a right* (resp. *left*) *S-module and the* *functor* $-\otimes_S R$ (resp. $R\otimes_S -$) *reflects isomorphisms, then* Γ: $\mathrm{Inv}_S(R)\to\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$ *is an isomorphism and*

$$\mathbf{I}^l_S(R)\cap\mathbf{I}^r_S(R)=\mathrm{Inv}_S(R).$$

PROOF. If $I\in\mathbf{I}^l_S(R)\cap\mathbf{I}^r_S(R)$, $\Gamma(I)\in\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$. Hence, by (2.7) we have only to show $\mathbf{J}(g)\in\mathrm{Inv}_S(R)$ for any $g\in\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$. In case (a) this holds by (2.2) or (2.9). Concerning case (b), considering $S^o\subset R^o$, we have only to show the following:

2.11. LEMMA. *Assume S is a direct summand of R as a right S-module. Let* $g\in\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$. *Then we have:*

(1) $\mathbf{J}(id_{R\otimes_S R})=S$.

(2) $\mathbf{J}(g)\in\mathbf{I}^r_S(R)$.

(3) *If* $-\otimes_S R$ *reflects isomorphisms,* $\mathbf{J}(g)\in\mathrm{Inv}_S(R)$.

PROOF. (1). Easy.

(2). This follows from the following commutative diagram with exact rows, the notation being the same as in (2.4).

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{J}(g)\otimes_S R \arrow[r, "\iota\otimes\mathrm{id}"'] \arrow[d, "\mathbf{m}"] & R\otimes_S R \arrow[r, "\delta\otimes\mathrm{id}"'] \arrow[d, "g", "\wr"'] & R\otimes_S R\otimes_S R \arrow[d, "\mathrm{id}\otimes g", "\wr"'] \\
0 \arrow[r] & R \arrow[r, "d_1"'] & R\otimes_S R \arrow[r, "d_1-d_2"'] & R\otimes_S R\otimes_S R
\end{tikzcd}$$

Commutativity is verified easily. The lower row is exact by (1). Modifying the proof of (2.5) (1), we have that there exist π, ϕ in $\mathcal{M}_S$ satisfying (2.5.1), so the upper row is exact.

(3). If $-\otimes_S R$ reflects isomorphisms, by (2) and (2.7)(1) we have $\mathbf{J}(g)\mathbf{J}(h)=\mathbf{J}(gh)$ for any g, $h\in\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$. This, together with (1), implies (3).

Q. E. D.

§ 3. Applications.

Put $Z=R^R$, the center of R. The Miyashita action (see [**3**, p. 100] or [**9**, pp. 137-8])

$$\mathrm{Inv}_S(R)\longrightarrow\mathrm{Aut}_{Z\text{-alg}}(R^S)$$

decomposes as follows:

$$\mathrm{Inv}_S(R)\xrightarrow[\Gamma]{}\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)\xrightarrow[\kappa]{}\mathrm{Aut}_{Z\text{-alg}}(R^S)\tag{3.1}$$

where κ is the anti-group map induced from the "clipping"

$$(R\otimes_S R)^S \longrightarrow \mathrm{End}_{\mathcal{M}_Z}(R^S), \qquad \sum x_i\otimes y_i \longmapsto (a \mapsto \sum x_i a y_i).$$

By using (2.10) we can prove directly Corollary (6.24) in Doi and Takeuchi [1].

3.2. COROLLARY [1, (6.24)]. *Assume that R is an Azumaya algebra over a commutative ring Z and that S is a subalgebra of R such that R is a progenerator as a left or right S-module. Then, the Miyashita action* $\mathrm{Inv}_S(R)\to\mathrm{Aut}_{Z\text{-alg}}(R^S)$ *is an anti-isomorphism of groups.*

PROOF. By symmetry we may assume that ${}_SR$ is a progenerator. Condition (a) in (2.10) being satisfied, Γ in (3.1) is bijective, and so is κ, as will be shown soon. It is easy to see that $R^S\otimes_Z R\cong\mathrm{End}_{S\mathcal{M}}(R)$. Applying $\mathcal{M}_R(-, R)$ to this isomorphism, we have $R\otimes_S R\cong\mathcal{M}_Z(R^S, R)$, so

$$R\otimes_S R\otimes_S R\cong\mathcal{M}_Z(R^S, R)\otimes_S R=\mathcal{M}_Z(R^S, R\otimes_S R)$$
$$\cong\mathcal{M}_Z(R^S, \mathcal{M}_Z(R^S, R))=\mathcal{M}_Z(R^S\otimes_Z R^S, R).$$

Taking $(\ )^S$, we have

$$(R\otimes_S R)^S\cong\mathrm{End}_{\mathcal{M}_Z}(R^S), \quad (R\otimes_S R\otimes_S R)^S\cong\mathcal{M}_Z(R^S\otimes_Z R^S, R^S)$$

$$\text{and consequently} \quad \mathrm{End}_{R\text{-cor}}(R\otimes_S R)\cong\mathrm{End}_{Z\text{-alg}}(R^S)$$

through the "clipping" maps. Therefore κ is bijective. This completes the proof. Q.E.D.

From now on, we assume that $S\subset$the center of R. Hence S is commutative, and R and $R\otimes_S R$ are S-algebras.

3.3. LEMMA. *Any $g\in\mathrm{Gr}(R\otimes_S R)$ is invertible in $R\otimes_S R$.*

PROOF. Let g^- be the image of g under the twist map $x\otimes y\mapsto y\otimes x$, $R\otimes_S R\to R\otimes_S R$. Then g^- is the inverse of g in $R\otimes_S R$, since

$$gg^-=d_2\circ\mathbf{m}(g)=1\otimes 1=d_1\circ\mathbf{m}(g)=g^-g. \qquad \text{Q.E.D.}$$

Lemma does not assert $\mathrm{End}_{R\text{-cor}}(R\otimes_S R)=\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R)$, since the usual product in $\mathrm{Gr}(R\otimes_S R)$ comes from that in $R^o\otimes_S R$ (1.3). By (3.3) or (2.2), it holds that

$$\mathrm{End}_{R\text{-cor}}(R\otimes_S R)=\mathrm{Aut}_{R\text{-cor}}(R\otimes_S R),$$

if one of the following holds:

(1) there exists an S-algebra anti-automorphism of R,

(2) R is finitely generated projective as an S-module,

(3) $S=k$ is a field and (#) $R^n\cong R^m$ in ${}_R\mathcal{M}$ (or in $\mathcal{M}_R$) for any n, $m\in\mathbf{N}$

implies $n=m$,

where R^n denotes the direct sum of n copies of R. In particular, if (3) holds, then by Proposition (1.1)

$$\mathrm{Gr}\,(R\otimes_k R)=\{u^{-1}\otimes u\in R\otimes_k R \mid u\in U(R)\}.$$

If R is left (or, respectively, right) Artinian, it satisfies condition (#) (cf. [8, p. 460]).

Here we can prove the following theorem announced in [2] without proof. A bialgebra H over a field k is called a *Galois bialgebra* of an algebra R, if (R, ρ) is a right H-comodule algebra and if the β-map

$$\beta: R\otimes_k R \longrightarrow R\otimes_k H, \qquad \beta(x\otimes y)=(x\otimes 1)\rho(y)$$

is bijective.

3.4. THEOREM. *Assume that a cocommutative bialgebra (H, Δ, ε) over a field k is a Galois bialgebra of such an algebra R that satisfies condition (#). Then H is necessarily a Hopf algebra, i.e., it has the antipode.*

PROOF. The cocommutative bialgebra H has the antipode iff the monoid $\mathrm{Gr}_L(L\otimes_k H)$ of group-likes in $L\otimes_k H$ is a group for any finite extension L/k of fields. Since $L\otimes_k H$ is Galois bialgebra of $L\otimes_k R$ which satisfies condition (#), it is sufficient to see that $\mathrm{Gr}\,(H)$ is a group.

View $R\otimes_k H\in {}_R\mathcal{M}_R$ via $x\cdot(a\otimes h)\cdot y=(xa\otimes h)\rho(y)$ for $x, y\in R$, $a\otimes h\in R\otimes_k H$. As is verified easily, $R\otimes_k H$ is an R-coring with the structure

$$R\otimes_k H \xrightarrow{id\otimes\Delta} R\otimes_k H\otimes_k H=(R\otimes_k H)\otimes_R(R\otimes_k H), \quad R\otimes_k H \xrightarrow{id\otimes\varepsilon} R$$

and the β-map is an isomorphism of R-corings.

Let $g\in\mathrm{Gr}\,(H)$. Since $1\otimes g\in R\otimes_k H$ is a group-like, there exists $u\in U(R)$ such that $\beta(u^{-1}\otimes u)=1\otimes g$ by assumption on R, so $\rho(u)=u\otimes g$. Hence g should be invertible and $\rho(u^{-1})=u^{-1}\otimes g^{-1}$. This completes the proof. Q.E.D.

Acknowledgement

I thank Professor M. Takeuchi who taught me an elegant proof of the faithfully flat descent theorem.

References

[1] Doi, Y. and Takeuchi, M., Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action, and Azumaya algebras, J. Algebra, 121 (1989), 488-516.

[2] Masuoka, A., Cogalois theory for field extensions, to appear in J. Math. Soc. Japan.
[3] Miyashita, Y., On Galois extensions and crossed products, J. Fac. Sci. Hokkaido Univ. Ser. I **19** (1970), 97-121.
[4] Miyashita, Y., An exact sequence associated with a generalized crossed product, Nagoya Math. J., **49** (1973), 21-51.
[5] Sweedler, M., Hopf algebras, Benjamin, New York, 1969.
[6] Sweedler, M., The predual theorem to the Jacobson-Brourbaki theorem, Trans. Amer. Math. Soc., **213** (1975), 391-406.
[7] Sweedler, M., Groups of simple algebras, I. H. E. S. Publ., **44** (1975), 79-189.
[8] Takeuchi, M., Relative Hopf modules-equivalences and freeness criteria, J. Algebra, **60** (1979), 452-471.
[9] Ulbrich, K.-H., Vollgraduierte Algebren, Abh. Math. Sem. U. Hamburg, **51** (1981), 136-148.
[10] Waterhouse, W., Introduction to affine group schemes, GTM 66, Springer-Verlag, 1979.

Akira Masuoka
Institute of Mathematics
University of Tsukuba
Tsukuba-city, Ibaraki 305
Japan