Acta Mathematica Sinica, English Series
Jan., 2012, Vol. 28, No. 1, pp. 195–204
Published online: December 15, 2011
DOI: 10.1007/s10114-012-9074-x
Http://www.ActaMath.com

Acta Mathematica Sinica, English Series

On the Set of Grouplikes of a Coring

L. EL KAOUTIT
Departamento de Álgebra. Facultad de Educación y Humanidades,
*Universidad de Granada, El Greco N*º 10, *E*-51002 *Ceuta, España*
E-mail: *kaoutit@ugr.es*

J. GÓMEZ-TORRECILLAS
Departamento de Álgebra. Facultad de Ciencias,
*Universidad de Granada, E*18071 *Granada, España*
E-mail: *gomezj@ugr.es*

Abstract We focus our attention to the set $\mathbf{Gr}(\mathfrak{C})$ of grouplike elements of a coring $\mathfrak{C}$ over a ring A. We do some observations on the actions of the groups $U(A)$ and $\mathbf{Aut}(\mathfrak{C})$ of units of A and of automorphisms of corings of $\mathfrak{C}$, respectively, on $\mathbf{Gr}(\mathfrak{C})$, and on the subset $\mathbf{Gal}(\mathfrak{C})$ of all Galois grouplike elements. Among them, we give conditions on $\mathfrak{C}$ under which $\mathbf{Gal}(\mathfrak{C})$ is a group, in such a way that there is an exact sequence of groups $\{1\} \to U(A^g) \to U(A) \to \mathbf{Gal}(\mathfrak{C}) \to \{1\}$, where A^g is the subalgebra of coinvariants for some $g \in \mathbf{Gal}(\mathfrak{C})$.

Keywords Galois corings, division ring extensions, non-abelian cohomology

MR(2000) Subject Classification 16D20, 16K20, 16W30

1 Introduction

The concept of non-abelian cohomology of groups has been extended to the framework of Hopf algebras by Nuss and Wambst in [1, 2]. Given a Hopf algebra H, a right H-comodule algebra A, and a right Hopf $(H-A)$-module M, the first descent cohomology set $\mathscr{D}^1(H, M)$ of H with coefficients in M is defined in terms of all Hopf module structures on M. When $B \subseteq A$ is a G-Galois extension, where G is a finite group acting on A by automorphisms, then by [1, Proposition 2.5] there is an isomorphism of pointed sets $\mathscr{D}^1(K^G, M) \cong \mathscr{H}^1(G, \mathbf{Aut}(M_A))$, where the last stands for the first non-abelian cohomology set of G with coefficients in $\mathbf{Aut}(M_A)$ [3]. Here, K^G is the Hopf algebra of functions on the group G in a commutative base ring K. In [4], Brzeziński has shown that this descent cohomology can be satisfactorily extended to the framework of comodules over corings, introducing the first descent cohomology set $\mathscr{D}^1(\mathfrak{C}, M)$, where $\mathfrak{C}$ is a coring over a ring A, and M is a right $\mathfrak{C}$-comodule. Since the definition of descent cohomology of [1] is a special case of [4, Definition 2.2], we know that there must be an interpretation of the aforementioned non-abelian cohomology set $\mathscr{H}^1(G, \mathbf{Aut}(M_A))$ in terms of descent cohomology of a coring with coefficients in a comodule. The first remark in this note

Received February 11, 2009, revised March 9, 2010, accepted October 8, 2010
Supported by grant MTM2007-61673 from the Ministerio de Educación y Ciencia of Spain, and P06-FQM-01889 from Junta de Andalucía

(see Theorem 2.7) gives such an interpretation, in the case $M = A$. Our approach uses the fact that the comodule structures on A over an A-coring $\mathfrak{C}$ are parametrized by the set $\mathbf{Gr}(\mathfrak{C})$ of all grouplike elements of $\mathfrak{C}$ [5]. We thus consider the particular case of [4, Definition 2.2] of the first descent cohomology set $\mathscr{D}^1(\mathfrak{C}, g)$ of the A-coring $\mathfrak{C}$ at a grouplike element $g \in \mathbf{Gr}(\mathfrak{C})$ (see Definition 2.4).

We focus our attention to the set $\mathbf{Gr}(\mathfrak{C})$. We do some observations on the actions of the groups $U(A)$ and $\mathbf{Aut}(\mathfrak{C})$ of units of A and of automorphisms of corings of $\mathfrak{C}$, respectively, on $\mathbf{Gr}(\mathfrak{C})$. Among them, let us mention that if $\mathscr{D}^1(\mathfrak{C}, g) = \{1\}$, then $\mathbf{Aut}(\mathfrak{C})$ is isomorphic to a quotient group $U(A)_g/U(A^g)$, where A^g (see Definition 2.1) is the subring of g-coinvariants of A, and $U(A)_g$ is a subgroup of $U(A)$ (see Corollary 3.4). We also give (see Theorem 3.6) conditions under which the set $\mathbf{Gal}(\mathfrak{C})$ of all Galois grouplike elements is a group, in such a way that there is an exact sequence of groups

$$\{1\} \to U(A^g) \to U(A) \to \mathbf{Gal}(\mathfrak{C}) \to \{1\}.$$

We also give some conditions on $g \in \mathbf{Gal}(\mathfrak{C})$ to have that $\mathscr{D}^1(\mathfrak{C}, g) = \{1\}$. Our approach here makes use of the theory of cosemisimple corings developed in [6] and [7].

Some examples illustrate our results.

2 Grouplikes, Non-Abelian Cohomology and Descent Cohomology

Let $(\mathfrak{C}, \Delta_{\mathfrak{C}}, \varepsilon_{\mathfrak{C}})$ be a coring over a K–algebra A (K is a commutative ring). Thus, $\mathfrak{C}$ is an A-bimodule, and $\Delta_{\mathfrak{C}} : \mathfrak{C} \to \mathfrak{C} \otimes_A \mathfrak{C}$ and $\varepsilon_{\mathfrak{C}} : \mathfrak{C} \to A$ are homomorphisms of A-bimodules subject to axioms of coassociativity and counitality: $(\mathfrak{C} \otimes_A \Delta_{\mathfrak{C}}) \circ \Delta_{\mathfrak{C}} = (\Delta_{\mathfrak{C}} \otimes_A \mathfrak{C}) \circ \Delta_{\mathfrak{C}}$ and $(\mathfrak{C} \otimes_A \varepsilon_{\mathfrak{C}}) \circ \Delta_{\mathfrak{C}} = (\varepsilon_{\mathfrak{C}} \otimes_A \mathfrak{C}) \circ \Delta_{\mathfrak{C}} = \mathfrak{C}$. A morphism of A-corings is an A-bilinear map $\varphi : \mathfrak{C} \to \mathfrak{C}'$ satisfying $\Delta_{\mathfrak{C}'} \circ \varphi = (\varphi \otimes_A \varphi) \circ \Delta_{\mathfrak{C}}$ and $\varepsilon_{\mathfrak{C}'} \circ \varphi = \varepsilon_{\mathfrak{C}}$.

A right $\mathfrak{C}$-comodule is a pair (M, ρ_M) consisting of a right A-module and a right A-linear map $\rho_M : M \to M \otimes_A \mathfrak{C}$, called right $\mathfrak{C}$-coaction, such that $(M \otimes_A \Delta_{\mathfrak{C}}) \circ \rho_M = (\rho_M \otimes_A \mathfrak{C}) \circ \rho_M$ and $(M \otimes_A \varepsilon_{\mathfrak{C}}) \circ \rho_M = M$. A morphism of right $\mathfrak{C}$-comodules $f : (M, \rho_M) \to (N, \rho_N)$ is a right A-linear map $f : M \to N$ such that $\rho_N \circ f = (f \otimes_A \mathfrak{C}) \circ \rho_M$. With these morphisms, right $\mathfrak{C}$-comodules form a category. Details on corings and their comodules are easily available in [8].

Definition 2.1 *An element $g \in \mathfrak{C}$ is said to be a* grouplike element *if $\Delta_{\mathfrak{C}}(g) = g \otimes_A g$ and $\varepsilon_{\mathfrak{C}}(g) = 1$. The set of all grouplike elements of $\mathfrak{C}$ will be denoted by $\mathbf{Gr}(\mathfrak{C})$. The subring of* g-coinvariant *elements is defined by*

$$A^g = \{a \in A \,|\, ag = ga\}.$$

Example 2.2 If $B \to A$ is any ring extension, and $A \otimes_B A$ is its associated Sweedler's A-coring with comultiplication $a \otimes_B a' \mapsto (a \otimes_B 1) \otimes_A (1 \otimes_B a')$ and counit the multiplication map $a \otimes_B a' \mapsto aa'$, $a, a' \in A$, then it is clear that $1 \otimes_B 1 \in \mathbf{Gr}(A \otimes_B A)$. Given an SBN (Single Basis Number) ring A, then by [9, p. 113], there exist elements $a, a', b, b' \in A$ such that

$$ab + a'b' = 1, \quad ba = b'a' = 1 \quad \text{and} \quad b'a = ba' = 0.$$

Clearly $g = a \otimes_{\mathbb{Z}} b + a' \otimes_{\mathbb{Z}} b'$ is a grouplike element of the Sweedler A-coring $A \otimes_{\mathbb{Z}} A$.

Example 2.3 Consider a coring $\mathfrak{C}$ (resp. $\mathfrak{C}'$) over a ring A (resp. A'). Let $\rho : A \to A'$ be a homomorphism of rings, and consider a homomorphism of corings $\varphi : \mathfrak{C} \to \mathfrak{C}'$ in the sense of [10]. This morphism restricts to a map $\varphi : \mathbf{Gr}(\mathfrak{C}) \to \mathbf{Gr}(\mathfrak{C}')$. Moreover, for each $g \in \mathbf{Gr}(\mathfrak{C})$, ρ induces a homomorphism of rings $\rho : A^g \to A'^{\varphi(g)}$.

It is known [5, Lemma 5.1] that there is a bijection between $\mathbf{Gr}(\mathfrak{C})$ and the set of all right $\mathfrak{C}$-coactions on the right module A_A. Let $[g]A$ denote the right $\mathfrak{C}$-comodule structure defined on A by $g \in \mathbf{Gr}(\mathfrak{C})$. The right $\mathfrak{C}$-coaction $\rho_{[g]A} : [g]A \to [g]A \otimes_A \mathfrak{C} \cong \mathfrak{C}$ is given by sending $a \mapsto ga$. Conversely any right $\mathfrak{C}$-coaction ρ_A determines a unique element $\rho_A(1) \in \mathbf{Gr}(\mathfrak{C})$. A similar bijection exists taking left $\mathfrak{C}$-coactions on the left module ${}_AA$. We denote by $A[g]$ the left $\mathfrak{C}$-comodule induced by $g \in \mathbf{Gr}(\mathfrak{C})$.

It is easily checked that the subring A^g of A can be identified with both rings of endomorphisms of the right $\mathfrak{C}$-comodule $[g]A$ and of the left $\mathfrak{C}$-comodule $A[g]$. That is, $A^g = \mathrm{End}([g]A_{\mathfrak{C}}) = \mathrm{End}({}_{\mathfrak{C}}A[g])$. In fact, for two grouplike elements $g, h \in \mathbf{Gr}(\mathfrak{C})$, we have

$$\mathrm{Hom}_{\mathfrak{C}}([g]A,\, [h]A) = \{\alpha \in A \mid \alpha g = h\alpha\}.$$

Therefore, $[g]A \cong [h]A$ as right $\mathfrak{C}$-comodules if and only if g and h are *conjugated* in the sense that there exists $\alpha \in U(A)$ such that $h = \alpha g \alpha^{-1}$. These remarks suggest, in view of [4], the following definition, due to Brzeziński.

Definition 2.4 *Consider the action of the group of units $U(A)$ of A on $\mathbf{Gr}(\mathfrak{C})$*

$$\begin{aligned} U(A) \times \mathbf{Gr}(\mathfrak{C}) &\longrightarrow \mathbf{Gr}(\mathfrak{C}) \\ (\alpha, g) &\longmapsto \alpha g \alpha^{-1}. \end{aligned} \tag{2.1}$$

Let $\overline{\mathbf{Gr}}(\mathfrak{C})$ denote the quotient set of $\mathbf{Gr}(\mathfrak{C})$ under the action (2.1). *If $\mathbf{Gr}(\mathfrak{C})$ is not empty, then for each $g \in \mathbf{Gr}(\mathfrak{C})$ we can define the* pointed set of descent 1-cocycles on $\mathfrak{C}$ with coefficients in $[g]A$ *as*

$$Z^1(\mathfrak{C}, [g]A) := (\mathbf{Gr}(\mathfrak{C}), g),$$

and the first cohomology pointed set of $\mathfrak{C}$ with coefficients in $[g]A$ *as*

$$\mathscr{D}^1(\mathfrak{C}, [g]A) := (\overline{\mathbf{Gr}}(\mathfrak{C}), \overline{g}),$$

where (X, x) means a pointed set with a distinguished element $x \in X$. We shall use the simplified notations $Z^1(\mathfrak{C}, g)$ and $\mathscr{D}^1(\mathfrak{C}, g)$, respectively, and we will refer to them as the pointed set of descent 1-cocycles on $\mathfrak{C}$ at g, *and the* first descent cohomology of $\mathfrak{C}$ at g, *respectively. The* zeroth descent cohomology group *of $\mathfrak{C}$ at g is defined to be the group of $\mathfrak{C}$-comodules automorphisms of $[g]A$, and can be identified with the group of units $U(A^g)$ of the ring A^g, i.e.,*

$$\mathscr{D}^0(\mathfrak{C}, g) = U(A^g).$$

Our first aim is to exhibit a direct evidence of the fact that $\mathscr{D}^1(\mathfrak{C}, g)$ is a genuine version for corings of Serre's nonabelian cohomology of groups.

Example 2.5 Let G be a finite group acting by automorphisms on a ring A. Consider $R = G * A$ the associated crossed product. As R is a free right A-module with basis G, its right dual $R^* = \mathrm{Hom}_A(R,\, A)$ is an A-coring according to [11, Theorem 3.7] (with comultiplication and counit induced by the duals of the multiplication and the unit of the A-ring R). Our next aim is to establish a bijection between $\mathbf{Gr}(R^*)$ and the set of all non-abelian 1-cocycles $Z^1(G^{\mathrm{op}},\, U(A))$ in the sense of [3]. Of course here the action of the opposite group G^{op} on the group $U(A)$ is induced by the given action of the group G on the ring A. So we denote this action by α^x for every $\alpha \in U(A)$ and $x \in G^{\mathrm{op}}$.

Proposition 2.6 *The map $\Theta : \mathbf{Gr}(R^*) \to Z^1(G^{\mathrm{op}}, U(A))$ which sends $h \in \mathbf{Gr}(R^*)$ to its restriction to G is a bijection. Under this bijection, the trivial 1-cocycle corresponds to the grouplike given by the trace map $\mathfrak{t} : R \to A$ defined by $\mathfrak{t}(\sum_{x\in G} x a_x) = \sum_{x\in G} a_x$. Moreover, $A^{\mathfrak{t}}$ coincides with the subring of the G-invariant elements of A.*

Proof Let us denote by $\{x, x^*\}_{x\in G} \subseteq R \times R^*$ the finite dual basis of the right free A-module R_A given by G. The comultiplication and the counit of the A-coring R^* are defined as follows:

$$R^* \xrightarrow{\Delta} R^* \otimes_A R^* \qquad\qquad R^* \xrightarrow{\varepsilon} A$$
$$\varphi \longmapsto \sum_{x\in G} \varphi x \otimes_A x^*, \qquad\qquad \varphi \longmapsto \varphi(1_R),$$

where $\varphi\, x : R \to A$ sends $r \mapsto \varphi(xr)$. We have an isomorphism

$$\Upsilon : R^* \otimes_A R^* \longrightarrow (R \otimes_A R)^*, \quad \varphi \otimes_A \psi \longmapsto [r \otimes_A t \mapsto \varphi(\psi(r)t)].$$

Now, a right A-linear map $h : R \to A$ belongs to $\mathbf{Gr}(R^*)$ if and only if

$$h(1_R) = 1_A \quad \text{and} \quad \sum_{x\in G} h\, x \otimes_A x^* = h \otimes_A h. \tag{2.2}$$

So given $h \in \mathbf{Gr}(R^*)$, and applying Υ to the second equality in (2.2), we obtain the equality $h(xy) = h(y)\, h(x)^y$, for every pair of elements $x, y \in G$. Taking $y = x^{-1}$, we get $h(x^{-1})h(x)^{x^{-1}} = 1_A = h(x)h(x^{-1})^x$, since $h(1_R) = 1_A$. Applying x to the equality

$$h(x^{-1})h(x)^{x^{-1}} = 1_A,$$

we obtain $h(x)h(x^{-1})^x = h(x^{-1})^x h(x) = 1_A$. That is, $h(x) \in U(A)$, for every $x \in G$. In conclusion, we have defined a map

$$\mathbf{Gr}(R^*) \xrightarrow{\Theta} Z^1(G^{\mathrm{op}}, U(A))$$
$$h \longmapsto [\Theta(h) : x \longmapsto h(x)]. \tag{2.3}$$

It is clear that Θ is injective, since G is a basis for the right A-module R. Let us check that it is also surjectivity. Consider any 1-cocycle $f : G^{\mathrm{op}} \to U(A)$, and define $\widehat{f} : R \to A$ by sending $x * a \mapsto f(x)a$ for $x \in G$ and $a \in A$. Clearly $\widehat{f}$ is a right A-linear map, and $\varepsilon(\widehat{f}) = \widehat{f}(1_R) = f(\mathsf{e})1_A = f(\mathsf{e})$ (here e is the neutral element of G). By the 1-cocycle condition on f, we know that $f(\mathsf{e}) = f(\mathsf{e})^2$, that is, $f(\mathsf{e}) = 1_A$ and so $\varepsilon(\widehat{f}) = 1_A$. Now an easy computation using again the 1-cocycle condition shows that

$$\Upsilon\bigg(\sum_{x\in G} \widehat{f}x \otimes_A x^*\bigg)(y \otimes_A z) = \Upsilon(\widehat{f} \otimes_A \widehat{f})(y \otimes_A z),$$

for every pair of elements $y, z \in G$, which implies that $\Delta(\widehat{f}) = \widehat{f} \otimes_A \widehat{f}$. Therefore, $\widehat{f} \in \mathbf{Gr}(R^*)$. Obviously, we have $\Theta(\widehat{f}) = f$, and this establishes the desired surjectivity. Clearly the distinguished 1-cocycle $\mathfrak{e} : G^{\mathrm{op}} \to U(A)$ sending $x \mapsto 1$ corresponds then to the grouplike element $\mathfrak{t} : R \to A$ defined by $\sum_{x\in G} x a_x \mapsto \sum_{x\in G} a_x$. The coinvariant ring $A^{\mathfrak{t}}$ coincides with the invariant subring of A with respect to the G-action, i.e., $A^{\mathfrak{t}} = \{a \in A \,|\, x(a) = a, \forall\, x \in G\}$. $\square$

Recall from [3], that two 1-cocycles f and h are cohomologous if there exists $\alpha \in U(A)$ such that $f(x) = \alpha^{-1}h(x)\alpha^x$, for every $x \in G^{\rm op}$. Using the bijection (2.3), we can easily check that two 1-cocycles are cohomologous if and only if their corresponding grouplike elements are conjugated. On the other hand, the equality $A^{\mathfrak{t}} = A^G$ clearly implies that $U(A^{\mathfrak{t}}) = U(A)^{G^{\rm op}}$, where the latter stands for $\mathscr{H}^0(G^{\rm op}, U(A))$ the zeroth non-abelian cohomology group as in [3]. Therefore, we deduce from Proposition 2.6:

Theorem 2.7 *The map* Θ *of Proposition* 2.6 *induces an isomorphism of pointed sets*

$$\mathscr{D}^1(R^*, \mathfrak{t}) \cong \mathscr{H}^1(G^{\rm op}, U(A)),$$

and there is an equality of groups

$$\mathscr{D}^0(R^*, \mathfrak{t}) = \mathscr{H}^0(G^{\rm op}, U(A)).$$

Remark 2.8 Since the coring R^* is finitely generated and projective as a left A-module, its category of right comodules is isomorphic to the category of right R-modules. Taking this into account, one can adapt the proof of Proposition 2.6 in order to show that for every right $A^{\mathfrak{t}}$-module N, there are an isomorphism of pointed sets

$$\mathscr{D}^1(R^*, N \otimes_{A^{\mathfrak{t}}} [\mathfrak{t}]A) \;\cong\; \mathscr{H}^1(G^{\rm op}, \mathbf{Aut}_A(N \otimes_{A^{\mathfrak{t}}} A)),$$

and an equality of groups

$$\mathscr{D}^0(R^*, N \otimes_{A^{\mathfrak{t}}} [\mathfrak{t}]A) = \mathscr{H}^0(G^{\rm op}, \mathbf{Aut}_A(N \otimes_{A^{\mathfrak{t}}} A)),$$

where for every right $\mathfrak{C}$-comodule M, $\mathscr{D}^{\bullet}(\mathfrak{C}, M)$ are defined as in [4], and $\mathbf{Aut}_A(M)$ is the group of all automorphisms of the underlying right A-module of M.

3 Groups Acting on Grouplikes

The maps defined in the following lemma will be used in the sequel where the role of the extension $B \to A$ will be played by the inclusions $A^g \subseteq A$, and where g runs $\mathbf{Gr}(\mathfrak{C})$ whenever $\mathbf{Gr}(\mathfrak{C}) \neq \emptyset$.

Lemma 3.1 *Let* $B \to A$ *be any ring extension.*

(a) *Let* $\alpha \in U(A)$ *and consider the subring* $\alpha^{-1}B\alpha$ *of* A. *Then the map*

$$\begin{aligned} \psi_\alpha : A \otimes_B A &\longrightarrow A \otimes_{\alpha^{-1}B\alpha} A \\ a \otimes_B a' &\longmapsto a\alpha \otimes_{\alpha^{-1}B\alpha} \alpha^{-1}a' \end{aligned}$$

is an isomorphism of A*-corings.*

(b) *The map*

$$\psi_{-} : \{\alpha \in U(A) \,|\, \alpha^{-1}B\alpha = B\} \to \mathbf{Aut}(A \otimes_B A)$$

defines an anti-homomorphism of groups.

Proof (a) We only prove that ψ_α is a well-defined map. So, for every $a, a' \in A$ and $b \in B$, we have

$$\begin{aligned} \psi_\alpha(ab \otimes_K a') &= ab\alpha \otimes_{\alpha^{-1}B\alpha} \alpha^{-1}a' \\ &= a\alpha(\alpha^{-1}b\alpha) \otimes_{\alpha^{-1}B\alpha} a' \\ &= a\alpha \otimes_{\alpha^{-1}B\alpha} (\alpha^{-1}b\alpha)\alpha^{-1}a' \end{aligned}$$

$$= a\alpha \otimes_{\alpha^{-1}B\alpha} \alpha^{-1}ba' = \psi_\alpha(a \otimes_K ba'),$$

that is, ψ_α is a well-defined map.

(b) Straightforward. □

Every grouplike element $g \in \mathbf{Gr}(\mathfrak{C})$ of the A-coring $\mathfrak{C}$ defines a *canonical morphism* of A-corings:

$$\mathsf{can}_g : A \otimes_{A^g} A \to \mathfrak{C}, \quad a \otimes_{A^g} a' \longmapsto aga'.$$

On the other hand, a straightforward computation shows that

$$A^{\alpha g \alpha^{-1}} = \alpha A^g \alpha^{-1}, \quad \text{for all } \alpha \in U(A). \tag{3.1}$$

Moreover, for every $\alpha \in U(A)$, we have the commutative diagram of homomorphisms of A-corings:

$$\begin{array}{ccc} A \otimes_{A^{\alpha g \alpha^{-1}}} A & & \\ \uparrow {\scriptstyle \psi_{\alpha^{-1}}} \cong & \searrow^{\mathsf{can}_{\alpha g \alpha^{-1}}} & \\ & & \mathfrak{C} \\ & \nearrow_{\mathsf{can}_g} & \\ A \otimes_{A^g} A. & & \end{array} \tag{3.2}$$

Recall from [5] that a grouplike $g \in \mathbf{Gr}(\mathfrak{C})$ is said to be *Galois* if can_g is bijective. It follows from diagram (3.2) that g is Galois if and only if $\alpha g \alpha^{-1}$ is Galois. Thus, if we denote by $\mathbf{Gal}(\mathfrak{C})$ the set of all Galois grouplike elements of $\mathfrak{C}$, then the action (2.1) restricts to an action

$$\begin{aligned} U(A) \times \mathbf{Gal}(\mathfrak{C}) &\longrightarrow \mathbf{Gal}(\mathfrak{C}) \\ (\alpha, g) &\longmapsto \alpha g \alpha^{-1}. \end{aligned}$$

The group $\mathbf{Aut}(\mathfrak{C})$ of all A-coring automorphisms of $\mathfrak{C}$ acts obviously on $\mathbf{Gr}(\mathfrak{C})$:

$$\begin{aligned} \mathbf{Aut}(\mathfrak{C}) \times \mathbf{Gr}(\mathfrak{C}) &\longrightarrow \mathbf{Gr}(\mathfrak{C}) \\ (\varphi, g) &\longmapsto \varphi \cdot g := \varphi(g). \end{aligned} \tag{3.3}$$

Since every $\varphi \in \mathbf{Aut}(\mathfrak{C})$ is, in particular, a homomorphism of A-bimodules, it follows that the actions (3.3) and (2.1) commute, that is,

$$\varphi \cdot (\alpha \cdot g) = \alpha \cdot (\varphi \cdot g), \quad \forall\, g \in \mathbf{Gr}(\mathfrak{C}), \forall\, \alpha \in U(A), \forall\, \varphi \in \mathbf{Aut}(\mathfrak{C}).$$

The action (3.3) restricts to an action

$$\begin{aligned} \mathbf{Aut}(\mathfrak{C}) \times \mathbf{Gal}(\mathfrak{C}) &\longrightarrow \mathbf{Gal}(\mathfrak{C}) \\ (\varphi, g) &\longmapsto \varphi(g), \end{aligned} \tag{3.4}$$

as the following proposition shows.

Proposition 3.2 (1) *For every element $g \in \mathbf{Gr}(\mathfrak{C})$ and $\varphi \in \mathbf{Aut}(\mathfrak{C})$, we have $A^g = A^{\varphi(g)}$. Moreover, the following diagram of morphisms of A-coring commutes*:

$$\begin{array}{ccc} A \otimes_{A^g} A & \xrightarrow{\mathsf{can}_g} & \mathfrak{C} \\ \| & & \downarrow {\scriptstyle \varphi} \\ A \otimes_{A^{\varphi(g)}} A & \xrightarrow{\mathsf{can}_{\varphi(g)}} & \mathfrak{C}\, . \end{array}$$

Therefore, $g \in \mathbf{Gal}(\mathfrak{C})$ *if and only if* $\varphi(g) \in \mathbf{Gal}(\mathfrak{C})$.

(2) *If* $g, h \in \mathbf{Gal}(\mathfrak{C})$*, then* $A^g = A^h$ *if and only if there exists* $\varphi \in \mathbf{Aut}(\mathfrak{C})$ *such that* $\varphi(h) = g$.

Proof (1) We only prove that $A^g = A^{\varphi(g)}$. Start with an element $b \in A^g$, then $b\varphi(g) = \varphi(bg) = \varphi(gb) = \varphi(g)b$ because φ is a homomorphism of A-bimodules, which implies that $b \in A^{\varphi(g)}$. Thus

$$A^g \subseteq A^{\varphi(g)} \subseteq A^{\varphi^{-1}(\varphi(g))} = A^g.$$

(2) Assume that $A^g = A^h$ for $g, h \in \mathbf{Gal}(\mathfrak{C})$. Then $\varphi = \mathsf{can}_g \circ \mathsf{can}_h^{-1} \in \mathbf{Aut}(\mathfrak{C})$ and $\varphi(h) = g$. The converse follows from (1). □

For every element $g \in \mathbf{Gr}(\mathfrak{C})$, we define

$$U(A)_g = \{\alpha \in U(A) \mid \alpha A^g = A^g \alpha\} = \{\alpha \in U(A) \mid A^{\alpha g \alpha^{-1}} = A^g\},$$

where in the second equality, we have used equation (3.1). It is clear that $U(A)_g$ is a subgroup of $U(A)$ which contains the group of units $U(A^g)$ of the subring A^g.

Proposition 3.3 *Let* $\mathfrak{C}$ *be an* A*-coring.*

(a) *For every element* $g \in \mathbf{Gr}(\mathfrak{C})$, $U(A^g)$ *is a normal subgroup of* $U(A)_g$.

(b) *For every* $g \in \mathbf{Gr}(\mathfrak{C})$ *and* $\beta \in U(A)$*, we have*

$$\beta U(A)_g \beta^{-1} = U(A)_{\beta g \beta^{-1}}.$$

(c) *If* $g \in \mathbf{Gal}(\mathfrak{C})$*, then there exists an exact sequence of groups*

$$1 \to U(A^g) \to U(A)_g \xrightarrow{\phi_g} \mathbf{Aut}(\mathfrak{C})$$
$$\alpha \longmapsto \mathsf{can}_g \circ \psi_{\alpha^{-1}} \circ \mathsf{can}_g^{-1}.$$

(d) *If* $\mathbf{Gal}(\mathfrak{C})$ *is non-empty and the action of* $U(A)$ *on* $\mathbf{Gal}(\mathfrak{C})$ *is transitive, then, for every* $g \in \mathbf{Gal}(\mathfrak{C})$, ϕ_g *is surjective and, thus, we have an isomorphism of groups*

$$\mathbf{Aut}(\mathfrak{C}) \cong U(A)_g / U(A^g).$$

Proof (a) Let β be an arbitrary element in $U(A)_g$. Given an element $\alpha \in U(A^g)$, by definition there exists $\gamma \in A^g$ such that $\beta\alpha\beta^{-1} = \gamma$, and so $\gamma \in U(A^g)$. Therefore, $\beta U(A^g)\beta^{-1} \subseteq U(A^g)$.

(b) It follows from the fact that $U(A)_g$ is the stabilizer in $U(A)$ of A^g for the action by conjugation of $U(A)$ on the set of all subalgebras of A.

(c) An element $\alpha \in U(A)_g$ is such that $\phi_g(\alpha) = 1$ if and only if $\mathsf{can}_g \circ \psi_{\alpha^{-1}} = \mathsf{can}_g$ if and only if $\mathsf{can}_g \circ \psi_{\alpha^{-1}}(1 \otimes_{A^g} 1) = \mathsf{can}_g(1 \otimes_{A^g} 1)$ if and only if $\alpha^{-1} g \alpha = g$ if and only if $\alpha \in U(A^g)$, and the exactness follows.

(d) Let $g \in \mathbf{Gal}(\mathfrak{C})$ and $\varphi \in \mathbf{Aut}(\mathfrak{C})$. Obviously, $\varphi(g) \in \mathbf{Gal}(\mathfrak{C})$ and, since $\mathbf{Gal}(\mathfrak{C}) = \{\beta g \beta^{-1} : \beta \in U(A)\}$, there exists $\alpha \in U(A)$ such that $\varphi(g) = \alpha^{-1} g \alpha$. We know that

$$A^g = A^{\varphi(g)} = A^{\alpha^{-1} g \alpha} = \alpha^{-1} A^g \alpha,$$

that is, $\alpha \in U(A)_g$. Moreover, it is easily checked that $\phi_g(\alpha)(g) = \alpha^{-1} g \alpha$ and, since g generates $\mathfrak{C}$ as an A-bimodule, this implies that $\varphi = \phi_g(\alpha)$. Therefore, ϕ_g is surjective. □

Corollary 3.4 *If* g *is a Galois grouplike element of* $\mathfrak{C}$ *such that* $\mathscr{D}^1(\mathfrak{C}, g) = \{1\}$*, then*

$$\mathbf{Aut}(\mathfrak{C}) \cong U(A)_g / U(A^g).$$

Remark 3.5 When A is commutative, Corollary 3.4 says that $\mathbf{Aut}(\mathfrak{C})$ is the *coGalois group* of the extension $A^g \subseteq A$, see [12] for the case of field extensions.

Theorem 3.6 *Let $\mathfrak{C}$ be an A-coring such that there exists $g \in \mathbf{Gal}(\mathfrak{C})$ and the action of $U(A)$ on $\mathbf{Gal}(\mathfrak{C})$ is transitive (e.g. $\mathscr{D}^1(\mathfrak{C}, g) = \{1\}$). The following statements are equivalent:*

(i) $U(A)_g = U(A)$ *(i.e., $\alpha A^g = A^g \alpha$ for every $\alpha \in U(A)$);*

(ii) $U(A)_h = U(A)$ *for every $h \in \mathbf{Gal}(\mathfrak{C})$;*

(iii) *the action of $\mathbf{Aut}(\mathfrak{C})$ on $\mathbf{Gal}(\mathfrak{C})$ is transitive. Furthermore, if one of these equivalent conditions is satisfied, then $A^h = A^g$ for every $h \in \mathbf{Gal}(\mathfrak{C})$, and the map $\xi_g : \mathbf{Aut}(\mathfrak{C}) \to \mathbf{Gal}(\mathfrak{C})$ defined by $\xi_g(\varphi) = \varphi(g)$ for $\varphi \in \mathbf{Aut}(\mathfrak{C})$ is bijective and, thus, $\mathbf{Gal}(\mathfrak{C})$ can be endowed with the structure of a group. Moreover, there exists a short exact sequence of groups*

$$\{1\} \to U(A^g) \to U(A) \to \mathbf{Gal}(\mathfrak{C}) \to \{1\}.$$

Proof (i) $\Rightarrow$ (iii) By assumption, we have $U(A)_g = U(A)$. On the other hand, every grouplike is of the form $\alpha g \alpha^{-1}$ for some $\alpha \in U(A)$. Now, $\alpha g \alpha^{-1} = \phi_g(\alpha^{-1})(g)$, where $\phi_g(\alpha^{-1}) \in \mathbf{Aut}(\mathfrak{C})$ is given by Proposition 3.3 (c). This means that each grouplike element is in the orbit of g under the action (3.3).

(iii) $\Rightarrow$ (ii) Given $h \in \mathbf{Gal}(\mathfrak{C})$ and $\alpha \in U(A)$, we know from (3.2) that $\alpha h \alpha^{-1} \in \mathbf{Gal}(\mathfrak{C})$. Since the action of $\mathbf{Aut}(\mathfrak{C})$ on $\mathbf{Gal}(\mathfrak{C})$ is transitive, there is $\varphi \in \mathbf{Aut}(\mathfrak{C})$ such that $\varphi(h) = \alpha h \alpha^{-1}$. Proposition 3.2 (2) and equation (3.1) now give that

$$A^h = A^{\varphi(h)} = A^{\alpha h \alpha^{-1}} = \alpha A^h \alpha^{-1},$$

that is, $\alpha \in U(A)_h$.

Since (ii) $\Rightarrow$ (i) is obvious, the proof of the equivalence between the three statements is done.

If $h \in \mathbf{Gal}(\mathfrak{C})$, then $A^h = A^{\varphi(g)} = A^g$ for some $\varphi \in \mathbf{Aut}(\mathfrak{C})$. On the other hand, it is clear from assumption that ξ_g is surjective. Since g, being Galois, generates $\mathfrak{C}$ as an A-bimodule, it follows that the action of every automorphism of $\mathfrak{C}$ on g determines it completely. Thus, ξ_g is injective. Finally, the short exact sequence of groups is given by Proposition 3.3 (c)–(d). □

A ring A is said to be a *right invariant basis number ring* (right IBN ring for short), if $A^{(n)} \cong A^{(m)}$ (direct sums of copies of A) as right A-modules for n, $m \in \mathbb{N}$ implies that $n = m$, see [9, p. 114]. An A-coring $\mathfrak{C}$ is said to *cosemisimple* if ${}_A\mathfrak{C}$ is a flat module and every right $\mathfrak{C}$-comodule is semisimple, equivalently, $\mathfrak{C}_A$ is flat and every left $\mathfrak{C}$-comodule is semisimple. A *simple cosemisimple* coring is a cosemisimple coring with one type of simple right comodule or equivalently with one type of simple left comodule; see [7, Therorem 4.4] for a structure theorem of all cosemisimple corings over an arbitrary ring. By [6, Theorem 4.3], every grouplike of a simple cosemisimple coring $\mathfrak{C}$ is Galois, that is, $\mathbf{Gr}(\mathfrak{C}) = \mathbf{Gal}(\mathfrak{C})$.

Theorem 3.7 *Let $\mathfrak{C}$ be an A-coring, and assume that there exists $g \in \mathbf{Gal}(\mathfrak{C})$. Assume that either A^g is a division ring and A is a right (or left)* IBN *ring, or A is a division ring. Then*

$$\mathbf{Gr}(\mathfrak{C}) = \mathbf{Gal}(\mathfrak{C}) = \{\alpha g \alpha^{-1} \mid \alpha \in U(A)\},$$

and, in particular, $\mathscr{D}^1(\mathfrak{C}, g) = \{1\}$.

Proof Assume first that A^g is a division ring and A is left or right IBN. By [6, Theorem 4.4] (see also [7, Theorem 3.10, Proposition 4.2]), $\mathfrak{C}$ is a simple cosemisimple A-coring and the functor $-\otimes_{A^g}[g]A : \mathsf{Mod}_{A^g} \to \mathsf{Comod}_{\mathfrak{C}}$ is an equivalence of categories. Thus, $[g]A \cong A^g \otimes_{A^g} [g]A$ is a simple right comodule. Given $h \in \mathbf{Gr}(\mathfrak{C})$, we have the right $\mathfrak{C}$-comodule $[h]A$. Since $\mathfrak{C}$ is cosemisimple with a unique type of simple right comodule represented by $[g]A$, there is an isomorphism of right $\mathfrak{C}$-comodules $[h]A \cong ([g]A)^{(n)}$ (direct sum of copies of $[g]A$), for some non zero natural number n. This isomorphism is, in particular, an isomorphism of right free A-modules. Hence, $n = 1$ since A is a right IBN ring. Therefore, $[h]A \cong [g]A$, as comodules, which means that $h = \alpha g \alpha^{-1}$ for some $\alpha \in U(A)$, and we have done. In the case that A is a division ring, it is easy to show that A^g is a division ring. □

Corollary 3.8 *Let $B \subseteq A$ be a ring extension, and $A \otimes_B A$ its canonical Sweedler's coring.*

(1) *If B is a division ring and A is a right or left* IBN *ring, then*

$$\mathbf{Gr}(A \otimes_B A) = \{\alpha \otimes_B \alpha^{-1} \mid \alpha \in U(A)\}.$$

(2) *If $B \subseteq A$ is an extension of division rings and $\alpha B = B\alpha$ for every $\alpha \in A$, then $\mathbf{Gr}(A \otimes_B A)$ is a group isomorphic to $A^\times / B^\times$.*

Proof By [6, Proposition 4.2], $B = A^{1\otimes_B 1}$. The corollary follows now from Theorem 3.7. □

Example 3.9 Let G be a finite group acting on a division ring A as in Example 2.5, and let T be the (division) subring of all G-invariant elements of A. We know that $T = A^{\mathfrak{t}}$. Assume that the trace map $\mathfrak{t}$ is a Galois grouplike of R^*, where $R = G * A$. This means that $T \subseteq A$ is Galois in the sense that the canonical map $G * A \to \mathrm{End}({}_T A)$ is bijective [13]. Then, by Theorems 2.7 and 3.7, $\mathscr{H}^1(G^{\mathrm{op}}, A^\times) = \{1\}$. This is a version of Hilbert's 90 theorem for division rings.

Remark 3.10 The condition $\alpha B = B\alpha$ for every $\alpha \in A$ in Corollary 3.8 is rather strong. An easy example is the following. Let $A = \mathbb{C}_q(X,Y)$ the (noncommutative) field of fractions of the complex quantum plane $\mathbb{C}_q[X,Y]$, and $B = \mathbb{C}(X)$, the field of complex rational functions in the variable X (here, $q \neq 1$ is a complex number). It is easy to show that $(1+Y)B \neq B(1+Y)$. In fact, $(1+aY)B \neq B(1+aY)$ for infinitely many $a \in \mathbb{C}^\times$. Of course, Corollary 3.8 says that $\mathscr{D}^1(\mathbb{C}_q(X,Y) \otimes_{\mathbb{C}(X)} \mathbb{C}_q(X,Y), 1 \otimes_{\mathbb{C}(X)} 1) = \{1\}$. Thus, $\mathscr{D}^1$ does not distinguish between the commutative case ($q = 1$), and the noncommutative case. We propose then the following definition: Given $g \in \mathbf{Gr}(\mathfrak{C})$, we define the *noncommutative first descent cohomology of $\mathfrak{C}$ at g* as the set of orbits of the action of $U(A)_g$ on $\mathbf{Gr}(\mathfrak{C})$, notation $N^1(\mathfrak{C}, g)$. There is an obvious surjective map of pointed sets $N^1(\mathfrak{C}, g) \to \mathscr{D}^1(\mathfrak{C}, g)$.

Example 3.11 Let H be a Hopf algebra over a commutative ring K and consider any right H-comodule algebra A with right coaction $\rho^A : A \to A \otimes_K H$ sending $a \mapsto a_{(0)} \otimes_K a_{(1)}$ (summation understood). Endow $A \otimes_K H$ with the A-coring structure given in [8, Subsection 33.2]. Then $1_A \otimes_K 1_H$ is a grouplike of $A \otimes_K H$ and

$$B := A^{1_A \otimes_K 1_H} = \{a \in A : \rho^A(a) = a \otimes_K 1\}.$$

Moreover, $1_A \otimes_K 1_H$ is Galois if and only if $B \subseteq A$ is a Hopf–Galois H-extension. Brzeziński has pointed out [4, Subsection 2.6] that $\mathscr{D}^1(A \otimes_K H, 1_A \otimes_K 1_H) = \mathscr{D}^1(H, A)$, where the last one refers to the the first descent cohomology set of H with coefficients in A defined in [1]. We get then the following consequences of Theorems 3.7 and 3.6:

Corollary 3.12 *Let $B \subseteq A$ be a Hopf–Galois H-extension, and assume that A is left or right* IBN. *If B is a division ring, then $\mathscr{D}^1(H, A) = \{1\}$. If, in addition, $B\alpha = \alpha B$ for every $\alpha \in A$ (e.g., $B \subseteq \mathrm{Center}(A)$), then*

$$\mathbf{Gr}(A \otimes_K H) = \{\alpha^{-1}\alpha_{(0)} \otimes_K \alpha_{(1)} : \alpha \in A^{\times}\}$$

is a group with the multiplication

$$(\alpha^{-1}\alpha_{(0)} \otimes_K \alpha_{(1)})(\beta^{-1}\beta_{(0)} \otimes_K \beta_{(1)}) = \beta^{-1}\alpha^{-1}\alpha_{(0)}\beta_{(0)} \otimes_K \alpha_{(1)}\beta_{(1)}.$$

We have the isomorphism of groups

$$U(A)/B^{\times} \xrightarrow{\cong} \mathbf{Gr}(A \otimes_K H), \quad \alpha B^{\times} \longmapsto \alpha^{-1}\alpha_{(0)} \otimes_K \alpha_{(1)}.$$

Example 3.13 A particular case of Example 3.11 occurs when $A = H^a$ the underlying algebra of H, and $\rho^H = \Delta$; the comultiplication of H. When K is a field, $A^{1 \otimes_K 1} = K$ and, therefore, $\mathscr{D}^1(H, H^a) = \{1\}$ if H^a is an IBN ring. Moreover, in this case, $\mathbf{Gr}(H^a \otimes_K H)$ is a group with the multiplication given in Corollary 3.12. It is easy to check that the map

$$\mathbf{Gr}(H) \to \mathbf{Gr}(H^a \otimes_K H), \quad g \mapsto 1 \otimes_K g$$

is a monomorphism of groups. For instance, if $H = K[C_2]$ is the group algebra of the cyclic group C_2 of order 2 generated by an element g. Then the group of units of the ring H^a is described as follows:

$$U(H^a) = \{k + l\mathsf{g} \,|\, k, l \in K, \text{ such that } k^2 - l^2 \neq 0\};$$

the inverse of $\alpha = k + l\mathsf{g} \in U(H^a)$ is given by the element $\alpha^{-1} = (k^2 - l^2)^{-1}(k - l\mathsf{g})$. Of course H^a is a right and left IBN ring, but not a division ring. Therefore, Corollary 3.12 gives a complete description of the group $\mathbf{Gr}(H^a \otimes_K H)$ which is

$$\{(k^2 - l^2)^{-1}(k^2 \otimes_K 1 - kl\mathsf{g} \otimes_K 1 - l^2 \otimes_K \mathsf{g} + kl\mathsf{g} \otimes_K \mathsf{g}) \,|\, k, l \in K, \text{ such that } k^2 - l^2 \neq 0\}.$$

References

[1] Nuss, P., Wambst, M.: Non-abelian Hopf cohomology. *J. Algebra*, **312**, 733–754 (2007)

[2] Nuss, P., Wambst, M.: Non-abelian Hopf cohomology II — The general case. *J. Algebra*, **319**, 4621–4645 (2008)

[3] Serre, J. P.: Corps Locaux, Deuxième edition, Hermann, Paris, 1968

[4] Brzeziński, T.: Descent cohomology and corings. *Commun. Algebra*, **36**, 1894–1900 (2008)

[5] Brzeziński, T.: The structure of corings. Induction functors, Maschke-type theorem, and Frobenius and Galois-type properties. *Alg. Rep. Theory*, **5**, 389–410 (2002)

[6] El Kaoutit, L., Gómez-Torrecillas, J., Lobillo, F. J.: Semisimple corings. *Alg. Colloq.*, **11**(4), 427–442 (2004)

[7] El Kaoutit, L., Gómez-Torrecillas, J.: Comatrix corings: Galois corings, descent theory, and a structure theorem for cosemisimple corings. *Math. Z.*, **244**, 887–906 (2003)

[8] Brzeziński, T., Wisbauer, R.: Corings and Comodules, LMS, Vol. 309, Cambridge University Press, 2003

[9] Anderson, F. W., Fuller, K. R.: Rings and Categories of Modules, Springer-Verlag, New York, 1974

[10] Gómez-Torrecillas, J.: Separable functors in corings. *Int. J. Math. Math. Sci.*, **30**, 203–225 (2002)

[11] Sweedler, M.: The predual theorem to the Jacobson–Bourbaki theorem. *Trans. Amer. Math. Soc.*, **213**, 391–406 (1975)

[12] Masuoka, A.: Cogalois theory for field extensions. *J. Math. Soc. Japan*, **41**(4), 576–592 (1989)

[13] Kanzaki, T.: On commutor rings and Galois theory of separable algebras. *Osaka J. Math.*, **1**, 103–115 (1964)