On Galois corings

R. WISBAUER University of Düsseldorf, Germany
e-mail address: wisbauer@math.uni-duesseldorf.de

Abstract. For a long period the theory of modules over rings on the one hand and comodules and Hopf modules for coalgebras and bialgebras on the other side developed quite independently. In this talk we want to outline how ideas from module theory can be applied to enrich the theory of comodules and vice versa. For this we consider A-corings $\mathcal{C}$ with grouplike elements over a ring A, in particular Galois corings. If A is right self-injective it turns out that $\mathcal{C}$ is a Galois coring if and only if for any injective comodule N the canonical map $\mathrm{Hom}^{\mathcal{C}}(A,N)\otimes_B A \to N$ is an isomorphism, where $B = \mathrm{End}^{\mathcal{C}}(A)$, the ring of coinvariants of A. Together with flatness of ${}_BA$ this characterises A as generator in the category of right $\mathcal{C}$-comodules. This is a special case of the fact that over any ring A, an A-module M is a generator in the category $\sigma[M]$ (objects are A-modules subgenerated by M) if and only if M is flat as module over its endomorphism ring S and the evaluation map $M \otimes_S \mathrm{Hom}(M,N) \to N$ is an isomorphism for injective modules N in $\sigma[M]$.

1. Introduction

Not being born as a member of the Hopf family I lived for many years with modules and rings without paying attention to the developments in the theory of Hopf algebras. Somehow I had the impression that in the coalgebra world additive categories are not of central importance and that the inversion of arrows in the definition of comodules also turned the interest of researchers to different directions. It was only in recent years that - by comments of colleagues - I became aware of the fact that the central notion of my own work, the subgenerator of a module category, could also be of interest to comodule theory. In fact it was known from Sweedler's book that for coalgebras over fields, every comodule is contained in a direct sum of copies of C showing that C is a cogenerator as well as a subgenerator for the comodules. While for coalgebras C over rings in general the cogenerator property of C is lost, it is easy to see that C is still a subgenerator. This was the motivation for me to have a closer look at this theory and to investigate how my experience from module theory could contribute to a better understanding of the coalgebraic world.

Seeing things from a different angle, it was not surprising that I sometimes came up with interesting answers to questions which native Hopf people had not previously considered. General (co-)module theory cannot make new contributions to the classification of finite dimensional (co-) algebras since in this special case the general notions coincide with more familiar ones. Probably because of this, quite a

2000 *Mathematics Subject Classification.* 16W30.
Key words and phrases. Coring; semisimple coring; module categories; coinvariants functor; structure theorem; Hopf algebras.

few traditionalists doubted if it makes any sense to study Hopf algebras over rings instead of fields. The situation is reminiscent of Jacobson's definition of a radical for any ring, extending the nilpotent radical for finite dimensional algebras. While his radical did not contribute to the classification of simple algebras, it certainly deepened and widened the understanding of ring and module theory.

Familiarity with coalgebras over commutative rings needs only a small step to non-commutative base rings, leading to the notion of corings. The formalism and results from module theory readily apply to this more general situation and in what follows I'll try to give some idea of how they can be used. Many of the observations to be reported result from cooperation and discussions with Tomasz Brzeziński and other colleagues.

2. Modules and comodules

Let A be any associative ring and denote by $\mathbf{M}_A$ and ${}_A\mathbf{M}$ the categories of unital right and left A-modules, respectively.

Let $\mathcal{C}$ be an A-coring, i.e., an (A,A)-bimodule with coassociative comultiplication $\Delta : \mathcal{C} \to \mathcal{C} \otimes_A \mathcal{C}$ and counit $\varepsilon : \mathcal{C} \to A$.

Right $\mathcal{C}$-comodules are right A-modules M with a *right coaction*

$$\varrho^M : M \to M \otimes_A \mathcal{C},$$

which is coassociative and counital. The categories of left and right $\mathcal{C}$-comodules are denoted by ${}^{\mathcal{C}}\mathbf{M}$ and $\mathbf{M}^{\mathcal{C}}$, respectively.

The investigation of a ring A is strongly influenced by the fact that A is a projective generator for the left and for the right A-modules. An A-coring $\mathcal{C}$ need not be a generator or cogenerator for the $\mathcal{C}$-comodules nor is it projective or injective in general. However, every comodule is a subcomodule of a comodule which is generated by $\mathcal{C}$ and hence structural properties of $\mathcal{C}$ may transfer to comodules.

2.1. **$\mathcal{C}$ is a subgenerator in $\mathbf{M}^{\mathcal{C}}$.** *For $X \in \mathbf{M}_A$, $X \otimes_A \mathcal{C}$ is a right $\mathcal{C}$-comodule by*

$$I_X \otimes \Delta : X \otimes_A \mathcal{C} \longrightarrow X \otimes_A \mathcal{C} \otimes_A \mathcal{C}\,,$$

and for any $M \in \mathbf{M}^{\mathcal{C}}$, the structure map $\varrho^M : M \to M \otimes_A \mathcal{C}$ is a comodule morphism.

Moreover any epimorphism $A^{(\Lambda)} \to M$ of A-modules yields a diagram in $\mathbf{M}^{\mathcal{C}}$ with exact bottom row

$$\begin{tikzcd} & M \arrow[d, "\varrho^M"] & \\ A^{(\Lambda)} \otimes_A \mathcal{C} \arrow[r] & M \otimes_A \mathcal{C} \arrow[r] & 0\,, \end{tikzcd}$$

showing that M is a subcomodule of a $\mathcal{C}$-generated comodule, i.e., $\mathcal{C}$ is a subgenerator in $\mathbf{M}^{\mathcal{C}}$.

Let us mention that over a quasi-Frobenius (QF) ring A, any A-coring $\mathcal{C}$ is an injective cogenerator in $\mathbf{M}^{\mathcal{C}}$ and in ${}^{\mathcal{C}}\mathbf{M}$. In fact any comodule is contained in a direct sum of copies of $\mathcal{C}$.

Both the duals of $\mathcal{C}$ as left A-module and as right A-module can be defined and are of importance for comodule theory. We concentrate on one side.

2.2. **The dual rings.** *Let $\mathcal{C}$ be an A-coring. ${}^*\mathcal{C} = {}_A\mathrm{Hom}(\mathcal{C}, A)$ is a ring with unit ε with respect to the product (for $f, g \in {}^*\mathcal{C}$, $c \in \mathcal{C}$)*

$$f *^l g \ : \ \mathcal{C} \xrightarrow{\Delta} \mathcal{C} \otimes_A \mathcal{C} \xrightarrow{I_{\mathcal{C}} \otimes g} \mathcal{C} \xrightarrow{f} A, \quad f *^l g(c) = \sum f(c_{\underline{1}} g(c_{\underline{2}})),$$

and there is a ring anti-homomorphism $\quad \iota : A \to {}^*\mathcal{C}, \ a \mapsto \varepsilon(-a)$.

The bridge from comodules to modules is provided by the following observation.

2.3. **$\mathcal{C}$-comodules and ${}^*\mathcal{C}$-modules.** *Any $M \in \mathbf{M}^{\mathcal{C}}$ is a (unital) left ${}^*\mathcal{C}$-module by*

$$\rightharpoonup : {}^*\mathcal{C} \otimes_A M \to M, \quad f \otimes m \mapsto (I_M \otimes f) \circ \varrho^M(m).$$

Any morphism $h : M \to N$ in $\mathbf{M}^{\mathcal{C}}$ is a left ${}^*\mathcal{C}$-module morphism, so

$$\mathrm{Hom}^{\mathcal{C}}(M, N) \subset {}_{^*\mathcal{C}}\mathrm{Hom}\,(M, N),$$

and there is a faithful functor from $\mathbf{M}^{\mathcal{C}}$ to $\sigma[{}_{^*\mathcal{C}}\mathcal{C}]$, the full subcategory of ${}_{^*\mathcal{C}}\mathbf{M}$ whose objects are submodules of $\mathcal{C}$-generated ${}^*\mathcal{C}$-modules.

Given the basic constructions we pause to think about what we can learn from module theory for comodules.

(1) In case $\mathbf{M}^{\mathcal{C}} = \sigma[{}_{^*\mathcal{C}}\mathcal{C}]$ we can transfer all theorems from module categories of type $\sigma[M]$ to comodules without extra proofs.
(2) More generally we can focus on the situation when $\mathcal{C}$ is flat as left A-module, in which case $\mathbf{M}^{\mathcal{C}}$ is a Grothendieck category. Many results and proofs in $\sigma[M]$ can then easily be transferred in this case.
(3) We may study $\mathbf{M}^{\mathcal{C}}$ without any conditions on the A-module structure of $\mathcal{C}$ and ask which notions still make sense and which problems can be handled in this general situation. Here the tranfer of results from $\sigma[M]$ needs more caution since monomorphisms in $\mathbf{M}^{\mathcal{C}}$ need no longer be injective maps.

We will take a brief look at the first two situations and then concentrate on certain aspects of the third one in the last section.

To describe the coincidence of $\mathbf{M}^{\mathcal{C}}$ and $\sigma[{}_{^*\mathcal{C}}\mathcal{C}]$ recall that an A-module M is said to be *locally projective* if, for any diagram of left A-modules with exact rows

$$\begin{tikzcd} 0 \arrow[r] & F \arrow[r, "i"] & M \arrow[d, "g"] & \\ & L \arrow[r, "f"] & N \arrow[r] & 0, \end{tikzcd}$$

where F is finitely generated, there exists $h : M \to L$ such that $g \circ i = f \circ h \circ i$.

2.4. **$\mathbf{M}^{\mathcal{C}}$ as full subcategory of ${}_{^*\mathcal{C}}\mathbf{M}$.** *The following are equivalent:*

(a) $\mathbf{M}^{\mathcal{C}} = \sigma[{}_{^*\mathcal{C}}\mathcal{C}]$;
(b) *for all $M, N \in \mathbf{M}^{\mathcal{C}}$, $\mathrm{Hom}^{\mathcal{C}}(M, N) = {}_{^*\mathcal{C}}\mathrm{Hom}(M, N)$;*
(c) *$\mathcal{C}$ is locally projective as left A-module;*
(d) *every left ${}^*\mathcal{C}$-submodule of $\mathcal{C}^n$, $n \in \mathbb{N}$, is a subcomodule of $\mathcal{C}^n$;*
(e) *the inclusion functor $i : \mathbf{M}^{\mathcal{C}} \to {}_{^*\mathcal{C}}\mathbf{M}$ has a right adjoint.*

Proof. We refer to [10, 3.5], [2], or [3]. □

In the situation considered in 2.4 all theorems known for module categories of type $\sigma[M]$ can be formulated for comodules. In particular the decomposition theorems for module categories yield decompositions of comodule categories and coalgebras (e.g., [8]).

In the following case $\mathbf{M}^{\mathcal{C}}$ is a Grothendieck category.

2.5. **$\mathcal{C}$ as a flat A-module.** *The following are equivalent:*

(a) *$\mathcal{C}$ is flat as a left A-module;*
(b) *every monomorphism in $\mathbf{M}^{\mathcal{C}}$ is injective;*
(c) *every monomorphism $U \to \mathcal{C}$ in $\mathbf{M}^{\mathcal{C}}$ is injective;*
(d) *the forgetful functor $(-)_A : \mathbf{M}^{\mathcal{C}} \to \mathbf{M}_A$ respects monomorphisms.*

If these conditions hold then $\mathbf{M}^{\mathcal{C}}$ is a Grothendieck category.

Proof. See [10, 3.4] or [2]. □

We note that if the category $\mathbf{M}^{\mathcal{C}}$ is Grothendieck then $\mathcal{C}$ need not be flat as left A-module (e.g., [3]).

3. Generators in module categories

In any (additive) category a generator P is characterised by the faithfulness of the functor $\mathrm{Hom}(P, -)$. In full module categories the following characterization (due to C. Faith) is well known (e.g., [6, 18.8]).

3.1. **Generator in ${}_A\mathbf{M}$.** *For an A-module M with $S = \mathrm{End}({}_AM)$, the following are equivalent:*

(a) *M is a generator in ${}_A\mathbf{M}$;*
(b) (i) *M_S is finitely generated and S-projective, and*
 (ii) *$A \simeq \mathrm{End}(M_S)$.*

The characterisation of generators in $\sigma[M]$ is more involved.

3.2. **Generator in $\sigma[M]$.** *For an A-module M with $S = \mathrm{End}({}_AM)$, the following are equivalent:*

(a) *M is a generator in $\sigma[M]$;*
(b) *for every $N \in \sigma[M]$, the following evaluation map is an isomorphism:*

$$M \otimes_S \mathrm{Hom}(M, N) \to N\,, \quad m \otimes f \mapsto f(m)\,;$$

(c) (i) *M_S is flat,*
 (ii) *for every injective module $V \in \sigma[M]$, the canonical map*

$$M \otimes_S \mathrm{Hom}(M, V) \to V\,, \quad m \otimes f \mapsto f(m)\,,$$

is injective (bijective).

If (any of) these conditions are satisfied the canonical map $A \to \mathrm{End}(M_S)$ is dense.

Proof. Most of the implications are well-known (see [6, 15.7,15.9], [2]). Because of its relevance for what follows, we show

$(c) \Rightarrow (a)$ For any $K \in \sigma[M]$, there exists an exact sequence $0 \to K \to Q_1 \to Q_2$, where Q_1, Q_2 are injectives in $\sigma[M]$. We construct an exact commutative diagram (tensoring over S)

$$\begin{tikzcd}
0 \arrow[r] & M \otimes_A \mathrm{Hom}(M,K) \arrow[r] \arrow[d, "\mu_K"] & M \otimes_A \mathrm{Hom}(M,Q_1) \arrow[r] \arrow[d, "\simeq"] & M \otimes_A \mathrm{Hom}(M,Q_2) \arrow[d, "\simeq"] \\
0 \arrow[r] & K \arrow[r] & Q_1 \arrow[r, "g"] & Q_2 \ ,
\end{tikzcd}$$

showing that μ_K is an isomorphism and so K is M-generated. □

For a better understanding of condition (c)(ii) recall the following special case (e.g., [6, 25.5]).

3.3. **Hom-tensor relation.** Given $M, V \in {}_A\mathbf{M}$, $S = \mathrm{End}(M)$, and $L \in \mathbf{M}_S$, consider the map

$$L \otimes_S \mathrm{Hom}(M,V) \to \mathrm{Hom}_A(\mathrm{Hom}_S(L,M),V), \quad l \otimes f \mapsto [g \mapsto (g(l))f].$$

This is an isomorphism provided L_S is finitely presented and V is M-injective.

If $A \to \mathrm{End}(M_S)$ is dense, setting $M = L$ yields the map

$$M \otimes_S \mathrm{Hom}(M,V) \to \mathrm{Hom}_A(\mathrm{Hom}_S(M,M),V) \simeq V\,, \quad m \otimes f \mapsto mf\,.$$

Since every M-injective module $V \in \sigma[M]$ is M-generated, this map is surjective for such modules. To make the map injective, it suffices, for example, to have M_S finitely presented or pure projective, and no flatness condition on M_S is needed.

More generally (c)(ii) can be related to descending chain conditions on certain matrix subgroups of M. For details we refer to [7] and [11].

Projectivity of a generator M is also reflected by properties of M as a module over its endomorphism ring.

3.4. **Projective generator in** $\sigma[M]$**.** *For an A-module M with $S = \mathrm{End}({}_AM)$, the following are equivalent:*

(a) *M is a projective generator in $\sigma[M]$;*

(b) (i) *M_S is faithfully flat,*

(ii) *for every injective module $V \in \sigma[M]$, the canonical map*

$$M \otimes_S \mathrm{Hom}(M,V) \to V\,, \quad m \otimes f \mapsto f(m)\,,$$

is injective (bijective).

Proof. $(a) \Rightarrow (b)$ By the generator property M is a flat module over S (see 3.2). Projectivity of M in $\sigma[M]$ implies $\mathrm{Hom}(M, MI) = I$, for every left ideal $I \subset S$, hence $MI \neq M$ if $I \neq S$. This shows that M is faithfully flat (e.g., [6, 12.17]).

$(b) \Rightarrow (a)$ In view of 3.2 it remains to show that M is projective in $\sigma[M]$. For this consider any epimorphism $L \xrightarrow{f} N$ in $\sigma[M]$. We obtain the commutative diagram with exact rows

$$\begin{tikzcd}
M \otimes_S \mathrm{Hom}(M,L) \arrow[r] \arrow[d, "\simeq"] & M \otimes_S \mathrm{Hom}(M,N) \arrow[r] \arrow[d, "\simeq"] & M \otimes_S \mathrm{Coke}\,\mathrm{Hom}(M,f) \arrow[r] & 0 \\
L \arrow[r, "f"] & N \arrow[r] & 0 \ ,
\end{tikzcd}$$

where the vertical maps are the canonical isomorphisms (see 3.2). From this we conclude $M \otimes_S \operatorname{Coke}\operatorname{Hom}(M, f) = 0$ and faithfulness of M_S implies $\operatorname{Coke}\operatorname{Hom}(M, f) = 0$ which means that $\operatorname{Hom}(M, f)$ is surjective. $\square$

4. Galois corings

Given an A-coring $\mathcal{C}$ we may ask when A is a $\mathcal{C}$-comodule.

4.1. **Grouplike elements.** A non-zero element g of an A-coring $\mathcal{C}$ is said to be a *grouplike* element if $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1_A$.

An A-coring $\mathcal{C}$ has a grouplike element g if and only if A is a right or left $\mathcal{C}$-comodule, by the coactions

$$\varrho^A : A \to \mathcal{C},\ a \mapsto ga, \quad {}^A\varrho : A \to \mathcal{C},\ a \mapsto ag.$$

For a proof we refer to [1] or [2]. We write A_g or ${}_gA$, when we consider A with the right or left comodule structure induced by g.

Example. Let $B \to A$ be a ring extension, and let $\mathcal{C} = A \otimes_B A$ be the Sweedler A-coring. Then $g = 1_A \otimes 1_A$ is a grouplike element in $\mathcal{C}$.

4.2. **Coinvariants.** Given an A-coring $\mathcal{C}$ with a grouplike element g and $M \in \mathbf{M}^{\mathcal{C}}$, the *$g$-coinvariants* of M are defined as the R-module

$$M_g^{co\mathcal{C}} = \{m \in M \mid \varrho^M(m) = m \otimes g\} = \operatorname{Ke}(\varrho^M - (- \otimes g)),$$

and there is an isomorphism

$$\psi_M : \operatorname{Hom}^{\mathcal{C}}(A_g, M) \to M_g^{co\mathcal{C}}, \quad f \mapsto f(1_A).$$

The isomorphism is derived from the fact that any A-linear map with source A is uniquely determined by the image of 1_A.

4.3. **Coinvariants of A and $\mathcal{C}$.** *Let $\mathcal{C}$ be an A-coring with a grouplike element g. Then:*

(1) $\operatorname{End}^{\mathcal{C}}(A_g) \simeq A_g^{co\mathcal{C}} = \{a \in A_g \mid ga = ag\}$,
i.e., subalgebra of A given by the centraliser of g in A.

(2) *For any $X \in \mathbf{M}_A$, $(X \otimes_A \mathcal{C})^{co\mathcal{C}} \simeq \operatorname{Hom}^{\mathcal{C}}(A_g, X \otimes_A \mathcal{C}) \simeq X$, and for $X = A$,*

$$\mathcal{C}^{co\mathcal{C}} \simeq \operatorname{Hom}^{\mathcal{C}}(A_g, \mathcal{C}) \simeq \operatorname{Hom}_A(A_g, A) \simeq A,$$

which is a left A- and right $\operatorname{End}^{\mathcal{C}}(A_g)$-morphism.

4.4. **The induction functor.** *For an A-coring $\mathcal{C}$ with grouplike element g, let $B = A_g^{co\mathcal{C}}$. Given any right B-module M, $M \otimes_B A$ is a right $\mathcal{C}$-comodule via the coaction*

$$\varrho^{M \otimes_B A} : M \otimes_B A \to M \otimes_B A \otimes_A \mathcal{C} \cong M \otimes_B \mathcal{C}, \quad m \otimes a \mapsto m \otimes ga.$$

For any morphism $f : M \to N$ in $\mathbf{M}_B$,

$$f \otimes I_A : M \otimes_A \mathcal{C} \to N \otimes_A \mathcal{C}, \quad m \otimes a \mapsto f(m) \otimes a,$$

is a morphism in $\mathbf{M}^{\mathcal{C}}$ and hence the assignment $M \to M \otimes_B A$ and $f \to f \otimes_B I_A$ defines a functor $- \otimes_B A : \mathbf{M}_B \to \mathbf{M}^{\mathcal{C}}$ known as an induction functor.

The g-coinvariants provide a functor in the opposite direction.

4.5. **The g-coinvariants functor.** *Let $\mathcal{C}$ be an A-coring with a grouplike element g and $B = A^{co\mathcal{C}}$. The functor*

$$\mathrm{Hom}^{\mathcal{C}}(A_g, -) : \mathbf{M}^{\mathcal{C}} \to \mathbf{M}_B,$$

is the right adjoint of the induction functor $- \otimes_B A : \mathbf{M}_B \to \mathbf{M}^{\mathcal{C}}$. Notice that for $M \in \mathbf{M}^{\mathcal{C}}$, the right B-module structure of $\mathrm{Hom}^{\mathcal{C}}(A_g, M)$ is given by $f \cdot b(a) = f(ba)$.

This functor is isomorphic to the coinvariant functor

$$G_g := (-)^{co\mathcal{C}}_g : \mathbf{M}^{\mathcal{C}} \to \mathbf{M}_B, \quad M \mapsto M^{co\mathcal{C}},$$

which acts on morphisms by restriction of the domain, i.e.,

$$\text{for any } f : M \to N \text{ in } \mathbf{M}^{\mathcal{C}},\ G_g(f) = f\,|_{M^{co\mathcal{C}}_g}.$$

For $N \in \mathbf{M}_B$ the unit of the adjunction is given by

$$\eta_N : N \to (N \otimes_B A)^{co\mathcal{C}}, \quad n \mapsto n \otimes 1_A,$$

and for $M \in \mathbf{M}^{\mathcal{C}}$, the counit reads

$$\sigma_M : M^{co\mathcal{C}} \otimes_B A \to M, \quad m \otimes a \mapsto ma.$$

Notice that for any right B-module N, there is a left A-module isomorphism

$$\mathrm{Hom}^{\mathcal{C}}(N \otimes_B A, \mathcal{C}) \cong \mathrm{Hom}_A(N \otimes_B A, A) \cong \mathrm{Hom}_B(N, A).$$

The structure of an A-coring $\mathcal{C}$ with a grouplike element g involves two rings, the algebra A itself and its g-coinvariants algebra B, and a ring map $B \to A$. On the other hand, to any ring extension $B \to A$ one can associate its canonical Sweedler A-coring $A \otimes_B A$ which also has a grouplike element. Thus we have two corings with grouplike elements: the original A-coring $\mathcal{C}$ we started with and the canonical coring associated to the related algebra extension $B \to A$. It is natural to study the relationship between these corings, and, in particular, to analyse corings for which this relationship is given by an isomorphism. This leads to the notion of a *Galois coring* introduced in [1].

Recall that $M \in \mathbf{M}^{\mathcal{C}}$ is said to be $(\mathcal{C}, A)$-*injective* if for every $\mathcal{C}$-comodule map $i : N \to L$ which is a coretraction in $\mathbf{M}_A$, every diagram

$$\begin{tikzcd} N \arrow[rr, "i"] \arrow[dr, "f"'] & & L \\ & M & \end{tikzcd}$$

in $\mathbf{M}^{\mathcal{C}}$ can be completed commutatively by some $g : L \to M$ in $\mathbf{M}^{\mathcal{C}}$. This is equivalent to $\varrho^M : M \to M \otimes_A \mathcal{C}$ being a coretraction in $\mathbf{M}^{\mathcal{C}}$.

4.6. **Galois corings.** *For an A-coring $\mathcal{C}$ with a grouplike element g and $B = A^{co\mathcal{C}}_g$, the following are equivalent:*

(a) *The following evaluation map is an isomorphism:*

$$\varphi_{\mathcal{C}} : \mathrm{Hom}^{\mathcal{C}}(A_g, \mathcal{C}) \otimes_B A \to \mathcal{C}, \quad f \otimes a \mapsto f(a);$$

(b) *the (A,A)-bimodule map defined by*

$$\chi : A \otimes_B A \to \mathcal{C}, \quad 1_A \otimes 1_A \mapsto g,$$

is a (coring) isomorphism;

(c) *for every $(\mathcal{C},A)$-injective comodule $N \in \mathbf{M}^{\mathcal{C}}$, the evaluation*

$$\varphi_N : \mathrm{Hom}^{\mathcal{C}}(A_g, N) \otimes_B A \to N, \quad f \otimes a \mapsto f(a),$$

is an isomorphism.

$(\mathcal{C}, g)$ is called a *Galois coring* if it satisfies the above conditions.

Proof. $(a)\Leftrightarrow(b)$ Observe that the canonical isomorphism

$$h : \mathrm{Hom}^{\mathcal{C}}(A_g, \mathcal{C}) \to A, \quad f \mapsto \varepsilon \circ f(1_A),$$

is right B-linear, and we get the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}^{\mathcal{C}}(A_g,\mathcal{C}) \otimes_B A & \xrightarrow{\varphi} & \mathcal{C}, \\ {\scriptstyle h\otimes I}\downarrow & & \downarrow{\scriptstyle =} \\ A \otimes_B A & \xrightarrow{\chi} & \mathcal{C}\,, \end{array} \qquad \begin{array}{ccc} f \otimes a & \longmapsto & f(a) \\ \downarrow & & \downarrow{\scriptstyle =} \\ \varepsilon \circ f(1_A) \otimes a & \longmapsfrom & \varepsilon \circ f(1_A) g a\,, \end{array}$$

where the last equality is obtained by colinearity of f, which implies

$$\varepsilon \circ f(1_A) ga = (\varepsilon \otimes I)(f(1_A) \otimes ga) = (\varepsilon \otimes I) \circ \Delta\, f(a) = f(a).$$

$(b)\Rightarrow(c)$ First observe that for any $X \in \mathbf{M}_A$, χ yields the isomorphisms

$$\mathrm{Hom}^{\mathcal{C}}(A_g, X \otimes_A \mathcal{C}) \otimes_B A \simeq X \otimes_B A \simeq X \otimes_A (A \otimes_B A) \simeq X \otimes_A \mathcal{C}.$$

Now assume $N \in \mathbf{M}^{\mathcal{C}}$ to be $(\mathcal{C},A)$-injective and consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}^{\mathcal{C}}(A_g, N) \otimes_B A & \longrightarrow & N \otimes_B A & \longrightarrow & (N \otimes_A \mathcal{C}) \otimes_B A \\ & & \downarrow{\scriptstyle \varphi_N} & & \downarrow{\scriptstyle \simeq} & & \downarrow{\scriptstyle \simeq} \\ 0 & \longrightarrow & N & \longrightarrow & N \otimes_A \mathcal{C} & \longrightarrow & N \otimes_A \mathcal{C} \otimes_A \mathcal{C}\,, \end{array}$$

where the top row is exact by the purity (splitting) property shown in 4.7 below, and bijectivity of the two vertical maps follows from the preceding remark. From this, bijectivity of φ_N follows.

$(c)\Rightarrow(a)$ This is obvious since $\mathcal{C}$ is always $(\mathcal{C},A)$-injective. □

Let us mention that *weak Galois corings* are considered in [9, 2.4]. For such corings the action of A on $\mathcal{C}$ is not required to be unital.

The purity condition needed above arises from the following splitting property (for $L = A$).

4.7. **Splitting induced by $(\mathcal{C},A)$-injectivity.** *For an A-coring $\mathcal{C}$, let $M \in \mathbf{M}^{\mathcal{C}}$ be $(\mathcal{C},A)$-injective. Then for any $L \in \mathbf{M}^{\mathcal{C}}$, the canonical sequence*

$$0 \longrightarrow \mathrm{Hom}^{\mathcal{C}}(L,M) \xrightarrow{i} \mathrm{Hom}_A(L,M) \xrightarrow{\gamma} \mathrm{Hom}_A(L, M \otimes_A \mathcal{C}),$$

splits in $\mathbf{M}_B$, where $B = \mathrm{End}^{\mathcal{C}}(L)$ and $\gamma(f) = \varrho^M \circ f - (f \otimes I_{\mathcal{C}}) \circ \varrho^L$.

A similar result holds for relative injective left comodules.

Proof. Denote by $h : M \otimes_A \mathcal{C} \to M$ the splitting map of ϱ^M in $\mathbf{M}^{\mathcal{C}}$. Then the map

$$\mathrm{Hom}_A(L, M) \simeq \mathrm{Hom}^{\mathcal{C}}(L, M \otimes_A \mathcal{C}) \to \mathrm{Hom}^{\mathcal{C}}(L, M), \quad f \mapsto h \circ (f \otimes I_{\mathcal{C}}) \circ \varrho^L,$$

splits the first inclusion in $\mathbf{M}_B$, and the map

$$\mathrm{Hom}_A(L, M \otimes_A \mathcal{C}) \to \mathrm{Hom}_A(L, M), \quad g \mapsto h \circ g,$$

yields a splitting map $\mathrm{Hom}_A(L, M \otimes_A \mathcal{C}) \to \mathrm{Hom}_A(L, M)/\mathrm{Hom}^{\mathcal{C}}(L, M)$, since for any $f \in \mathrm{Hom}_A(L, M)$,

$$h \circ \gamma(f) = f - h \circ (f \otimes I_{\mathcal{C}}) \circ \varrho^L \in f + \mathrm{Hom}^{\mathcal{C}}(L, M).$$

□

The next theorem shows which additional condition on A is sufficient to make A_g a comodule generator for a Galois A-coring $(\mathcal{C}, g)$. The second part is essentially [1, Theorem 5.6].

4.8. **The Galois Coring Structure Theorem.** *Let $\mathcal{C}$ be an A-coring with grouplike element g and $B = A_g^{co\mathcal{C}}$.*

(1) *The following are equivalent:*
   (a) *$(\mathcal{C}, g)$ is a Galois coring and ${}_BA$ is flat;*
   (b) *${}_A\mathcal{C}$ is flat and A_g is a generator in $\mathbf{M}^{\mathcal{C}}$.*

(2) *The following are equivalent:*
   (a) *$(\mathcal{C}, g)$ is a Galois coring and ${}_BA$ is faithfully flat;*
   (b) *${}_A\mathcal{C}$ is flat and A_g is a projective generator in $\mathbf{M}^{\mathcal{C}}$;*
   (c) *${}_A\mathcal{C}$ is flat and $\mathrm{Hom}^{\mathcal{C}}(A_g, -) : \mathbf{M}^{\mathcal{C}} \to \mathbf{M}_B$ is an equivalence with inverse $- \otimes_B A : \mathbf{M}_B \to \mathbf{M}^{\mathcal{C}}$ (cf. 4.5).*

Proof. (1) $(a) \Rightarrow (b)$ Assume $(\mathcal{C}, g)$ to be a Galois coring. Then in the diagram of the proof of 4.6, $(c) \Rightarrow (b)$, the top row is exact by flatness of ${}_BA$ without any condition on $N \in \mathbf{M}^{\mathcal{C}}$. So $\mathrm{Hom}^{\mathcal{C}}(A_g, N) \otimes_B A \to N$ is surjective (bijective) showing that A_g is a generator. Moreover the isomorphism $- \otimes_A \mathcal{C} \simeq - \otimes_A (A \otimes_B A)$ implies that ${}_A\mathcal{C}$ is flat.

$(b) \Rightarrow (a)$ If ${}_A\mathcal{C}$ is flat then monomorphisms in $\mathbf{M}^{\mathcal{C}}$ are injective. As for module categories one can show that the generator A_g in the category $\mathbf{M}^{\mathcal{C}}$ is flat over its endomorphism ring B, and $\mathrm{Hom}^{\mathcal{C}}(A_g, M) \otimes_B A \simeq M$, for all $M \in \mathbf{M}^{\mathcal{C}}$.

(2) The proof for 3.4 also works for comodules. □

If the ring A is right self-injective, then $\mathcal{C}$ is injective in $\mathbf{M}^{\mathcal{C}}$ and the reformulation of the characterization of Galois corings and the Structure Theorem is just the description of generators in module categories (compare 3.2, 3.4).

4.9. **Corollary.** *Assume A to be a right self-injective ring and let $\mathcal{C}$ be an A-coring with grouplike element g.*

(1) *The following are equivalent:*
   (a) *$(\mathcal{C}, g)$ is a Galois coring;*
   (b) *for every injective comodule $N \in \mathbf{M}^{\mathcal{C}}$, the evaluation*

$$\varphi_N : \mathrm{Hom}^{\mathcal{C}}(A_g, N) \otimes_B A \to N, \quad f \otimes a \mapsto f(a),$$

   is an isomorphism.

(2) *The following are equivalent:*
   (a) $(\mathcal{C}, g)$ *is a Galois coring and* ${}_BA$ *is (faithfully) flat;*
   (b) ${}_BA$ *is (faithfully) flat and for every injective comodule* $N \in \mathbf{M}^{\mathcal{C}}$*, the following evaluation map is an isomorphism:*

$$\varphi_N : \mathrm{Hom}^{\mathcal{C}}(A_g, N) \otimes_B A \to N, \quad f \otimes a \mapsto f(a).$$

We call a right $\mathcal{C}$-comodule N *semisimple* (in $\mathbf{M}^{\mathcal{C}}$) if every $\mathcal{C}$-monomorphism $U \to N$ is a coretraction, and N is called *simple* if all these monomorphisms are isomorphisms. Semisimplicity of N is equivalent to the fact that every right $\mathcal{C}$-comodule is N-injective. Simple and semisimple left $\mathcal{C}$-comodules and $(\mathcal{C}, \mathcal{C})$-bicomodules are defined similarly.

The coring $\mathcal{C}$ is said to be *left (right) semisimple* if it is semisimple as a left (right) comodule. $\mathcal{C}$ is called a *simple coalgebra* if it is simple as a $(\mathcal{C}, \mathcal{C})$-bicomodule.

From [2, 3] we recall:

4.10. **Semisimple corings.** *For an* A*-coring* $\mathcal{C}$ *the following are equivalent:*
(a) $\mathcal{C}$ *is right semisimple;*
(b) ${}_A\mathcal{C}$ *is projective and* $\mathcal{C}$ *is a semisimple left* ${}^*\mathcal{C}$*-module;*
(c) $\mathcal{C}_A$ *is projective and* $\mathcal{C}$ *is a semisimple right* $\mathcal{C}^*$*-module;*
(d) $\mathcal{C}$ *is left semisimple.*

Note that not every canonical coring associated to an algebra extension $B \to A$ is a Galois coring with respect to a grouplike $1_A \otimes 1_A$. However, if the extension $B \to A$ is faithfully flat than $(A \otimes_B A, 1_A \otimes_B 1_A)$ is a Galois-coring. As a particular example of this one can consider a Galois coring provided by Sweedler's Fundamental Lemma (cf. [5, 2.2 Fundamental Lemma]).

4.11. **Fundamental Lemma.** *Let* A *be a division ring. Suppose that* $\mathcal{C}$ *is an* A*-coring generated by a grouplike element* g *as an* (A, A)*-bimodule. Then* $(\mathcal{C}, g)$ *is a Galois coring.*

Proof. Under the given condition A is simple as left $\mathcal{C}$-comodule and it subgenerates $\mathcal{C}$ and hence $\mathbf{M}^{\mathcal{C}}$. This implies that $\mathcal{C}$ is a simple and right semisimple coring and A is a projective generator in $\mathbf{M}$. So $(\mathcal{C}, g)$ is a Galois coring by 4.8. $\square$

More general simple corings with grouplike elements can be characterised (compare also [3]) in the following way.

4.12. **Simple corings.** *Let* $\mathcal{C}$ *be an* A*-coring with grouplike element* g*. Then the following are equivalent:*
(a) $\mathcal{C}$ *is a simple and left (or right) semisimple coring;*
(b) $(\mathcal{C}, g)$ *is Galois and* $\mathrm{End}^{\mathcal{C}}(A_g)$ *is simple and left semisimple;*
(c) $\chi : A \otimes_B A \to \mathcal{C}$ *is an isomorphism and* B *is a simple left semisimple subring of* A*;*
(d) $\mathcal{C}_A$ *is flat,* ${}_gA$ *is a projective generator in* ${}^{\mathcal{C}}\mathbf{M}$*, and* $\mathrm{End}^{\mathcal{C}}({}_gA)$ *is simple and left semisimple.*

Proof. Let $\mathcal{C}$ be simple and left semisimple. Then there exists only one simple comodule (up to isomorphism) and so every non-zero comodule is a projective generator in $\mathbf{M}^{\mathcal{C}}$. In particular A_g is a finite direct sum of isomorphic simple comodules and hence $\mathrm{End}^{\mathcal{C}}(A_g)$ is simple and left (and right) semisimple. So the assertions follow by 4.8 and 4.6. □

As a special case we will consider Hopf algebras. For this we recall the conditions for bialgebras.

4.13. **Bialgebras.** Let R be a commutative ring. An R-module B which is an algebra and a coalgebra is called a *bialgebra* if $B \otimes_R B$ is a B-coring with bimodule structure

$$a'(a \otimes b)b' = \sum a'ab_{\underline{1}}{}' \otimes bb_{\underline{2}}{}', \text{ for } a, a', b, b' \in B,$$

comultiplication

$$\underline{\Delta} : B \otimes_R B \to (B \otimes_R B) \otimes_B (B \otimes_R B) \simeq B \otimes_R B \otimes_R B, \quad a \otimes b \mapsto \sum a \otimes b_{\underline{1}} \otimes b_{\underline{2}},$$

and counit $\underline{\varepsilon} : B \otimes_R B \to B,\ a \otimes b \mapsto a\varepsilon(b)$.

Clearly $1_B \otimes 1_B$ is a grouplike element and the ring of $B \otimes_R B$-covariants of B is isomorphic to R.

$B \otimes_R B$ is a subgenerator in the category $\mathbf{M}^{B \otimes_R B}$ which can be identified with the category of $\mathbf{M}_B^B$ right Hopf modules, the subcategory of $\mathbf{M}^B$ consisting of those comodules M whose structure maps are right B-module morphism, i.e.,

$$\varrho^M(mb) = \varrho^M(m)\Delta(b), \text{ for } m \in M,\ b \in B.$$

By 4.6 and [9, 5.10] we obtain:

4.14. **Hopf algebras.** *For a bialgebra B the following are equivalent:*

(a) *$B \otimes_R B$ is a Galois B-coring;*

(b) *the following canonical map is an isomorphism:*

$$\gamma_B : B \otimes_R B \to B \otimes_R B, \quad a \otimes b \mapsto (a \otimes 1)\Delta(b);$$

(c) *B is a Hopf algebra (has an antipode);*

(d) $\mathrm{Hom}_B^B(B, -) : \mathbf{M}_B^B \to \mathbf{M}_R$ *is an equivalence (with inverse $- \otimes_R B$).*

If (any of) these conditions hold, B is a projective generator in $\mathbf{M}_B^B$.

Notice that the coinvariants $B^{B \otimes_R B} = R$ and we get the generator property of B without requiring any flatness condition for B_R. Characterization (d) is essentially the Fundamental Theorem for Hopf algebras (e.g., [2]). Of course there are examples of Hopf algebras which are not flat over the base ring (e.g., [4, Beispiel 1.2.7]).

REFERENCES

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

[2] T. Brzeziński and R. Wisbauer, "Corings and Comodules", *London Math. Soc. Lect. Note Ser.* **309**, Cambridge University Press, Cambridge, 2003.

[3] L. El Kaoutit, J. Gómez Torrecillas, and F.J. Lobillo, Semisimple corings, preprint 2001.

[4] Ch. Lomp, Primeigenschaften von Algebren in Modulkategorien über Hopf Algebren, Dissertation, Universität Düsseldorf (2002).

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

[6] R. Wisbauer, “Foundations of Module and Ring Theory”, Gordon and Breach, Reading, Paris, 1991.

[7] R. Wisbauer, Static modules and equivalences, in “Interactions Between Ring Theory and Representations of Algebras”, F. Van Oystaeyen and M. Saorin (eds), *Lect. Notes Pure Appl. Math.* **210**. Dekker, New York (2000), 423–449.

[8] R. Wisbauer, Decompositions of modules and comodules, *Contemp. Math.* **259** (2000), 547–561.

[9] R. Wisbauer, Weak corings, *J. Algebra* **245** (2001), 123–160.

[10] R. Wisbauer, On the category of comodules over corings, in ”Mathematics and Mathematics Education”, Proc. 3rd Palestinian conf., Elyadi et al. (eds), World Sci. Publishing, River Edge, NJ, 2002, 325–336.

[11] W. Zimmermann, Modules with chain conditions for finite matrix subgroups, *J. Algebra* **190** (1997), 68–87.