JOURNAL OF ALGEBRA 24, 80–99 (1973)

The Automorphism Class Group of the Category of Rings

W. EDWIN CLARK

University of South Florida, Tampa, Florida 33620

AND

GEORGE M. BERGMAN*

Harvard University, Cambridge, Massachusetts 02138

Communicated by P. M. Cohn

Received May 25, 1971

This paper is motivated by the observation that the property of having a left identity cannot be described "categorically" in the category of rings, since the functor $(\ )^{\mathrm{op}}$ which takes a ring into its opposite ring is a category automorphism but does not preserve this property. In general, a property of objects, morphisms, etc., in a category $\mathscr{C}$ can be characterized category-theoretically if and only if it is invariant under the automorphisms (self-equivalences) of $\mathscr{C}$. This makes it desirable to know whether $(\ )^{\mathrm{op}}$ is the only nontrivial automorphism of the category of rings up to equivalence of functors. We shall show that the answer is yes, and that in the case of commutative rings, there are no nontrivial automorphisms.

More generally, let R be a commutative integral domain with 1 and consider the following four categories of associative (!) R-algebras:

$\mathscr{A}_R$ = category of R-algebras,

$\mathscr{A}_R^1$ = category of unitary R-algebras,

$\mathscr{C}_R$ = category of commutative R-algebras,

$\mathscr{C}_R^1$ = category of commutative unitary R-algebras.

In these cases there is a wider class of obvious automorphisms, for the automorphism group of R acts on each of these categories via change of module-product. We shall show that the automorphism class groups of $\mathscr{A}_R$ and $\mathscr{A}_R^1$ are precisely $\mathrm{aut}(R) \times \{1, \mathrm{op}\}$, while those of $\mathscr{C}_R$ and $\mathscr{C}_R^1$ are simply $\mathrm{aut}(R)$.

* The second author was partly supported by NSF contract GP 9152. Permanent address: University of California, Berkeley, CA 94720.

The idea of our proof will be familiar to categorists [6, 14, 16] but perhaps not to most ring-theorists. Let $\mathscr{A}$ denote any one of our categories, and $\langle x\rangle$ the free algebra on one generator in $\mathscr{A}$. Then for any $A\in\mathscr{A}$, the set of homomorphisms $[\langle x\rangle, A]$ is in natural 1–1 correspondence with the set $|A|$ of elements of A. Further, one can define a family Λ of maps of $\langle x\rangle$ into coproducts of copies of itself, which make $\langle x\rangle$ a *coalgebra* in $\mathscr{A}$, and with the help of which one can recover the algebra structures on the sets $[\langle x\rangle, A]\cong|A|$. Precisely, these sets become algebras $[\langle x\rangle, A]_\Lambda$, and this functor of $\mathscr{A}$ into itself is equivalent to the identity. Thus, the coalgebra $(\langle x\rangle, \Lambda)$ "determines" the identity representation of the abstract category $\mathscr{A}$ as a category of R-algebras.

It follows that to show an automorphism T of $\mathscr{A}$ is equivalent to the identity, it suffices to show that it preserves the isomorphism class of $(\langle x\rangle, \Lambda)$, and to prove that all automorphisms of $\mathscr{A}$ are isomorphic to members of a given "known" set, it will suffice to show that every automorphism of $\mathscr{A}$ sends $(\langle x\rangle, \Lambda)$ to one of the same coalgebras to which the "known" ones take it.

Our "known" automorphisms of $\mathscr{A}$ all preserve the isomorphism class of the object $\langle x\rangle$, but alter the coalgebra structure on it. (This corresponds to the fact that they preserve the underlying set of an algebra of A, but change its algebra structure.) In Section 3, we study all possible coalgebra structures on $\langle x\rangle$. These are easy to classify, and those inducing automorphisms of $\mathscr{A}$ indeed give those described above. (The situation is complicated by the fact that the automorphism group of $\langle x\rangle$ also acts on the class of coalgebra structures, sending coalgebras to isomorphic ones.) Hence every automorphism of $\mathscr{A}$ that preserves the isomorphism class of $\langle x\rangle$ will be equivalent to one of these, and it remains to prove that $\langle x\rangle$ can be characterized categorically in $\mathscr{A}$, so that every automorphism of $\mathscr{A}$ does indeed preserve it.

We obtain this characterization in Section 5, after arming ourselves in the preceding section with category-theoretic characterizations of a number of simple ring-theoretic properties. When R is a field, $\langle x\rangle$ can be characterized (in any of our four categories of R-algebras) as the unique nontrivial projective object that is embeddable in every nontrivial projective object; for R a general integral domain we get a more complicated characterization, making use, among other things, of the field case just stated.

In Section 6 we give some related examples, and in Section 7 discuss some open questions, in particular, what modification of our result we can expect to be true if the base ring R is not a domain.

For all unexplained terms of universal algebra, see [5] and for category-theory, [8]. We shall write $[A, B]$ for hom(A, B).

We begin with a review of the subject of coalgebras.

1. Coalgebras (cf. Freyd [6])

If $\mathscr{A}$ is a category, and A an object of $\mathscr{A}$, then $[A, -]$ gives a covariant functor from $\mathscr{A}$ into *Sets*. Assume $\mathscr{A}$ has arbitrary finite copowers of A, that is, coproducts $A * \cdots * A$ of n copies of A, $n \geqslant 0$. Any morphism f of A into its n-fold copower induces an n-ary operation on each set $[A, B]$ $(B \in \mathscr{A})$: n members of this set, $u_1, \ldots, u_n$, can be represented by one map $u : A * \cdots * A \to B$, which by composition with f gives a member of $[A, B]$. Hence a family Λ of maps of A into various copowers of itself gives the sets $[A, B]$ structures of algebra (in the sense of universal algebra) with operations of the corresponding arities. We shall denote these algebras $[A, B]_\Lambda$.

An equation satisfied by the morphisms in Λ (that is, an equality among their "co-compositions") induces an identity holding in all the algebras $[A, B]_\Lambda$; hence the functor $[A, -]_\Lambda$ takes $\mathscr{A}$ into the *variety* $\mathscr{V}$ of algebras that these identities define. Conversely, if some identity is satisfied by all the $[A, B]_\Lambda$, Λ must satisfy the corresponding equation, as one can see by writing down the identity for the canonical n elements of $[A, A * \cdots * A]_\Lambda$.

A pair (A, Λ) as above is called a *coalgebra* in $\mathscr{A}$.[1] It is called, specifically, a *co-$\mathscr{V}$-object*, for $\mathscr{V}$ a given variety, if the induced functor $[A, -]_\Lambda$ takes $\mathscr{A}$ into $\mathscr{V}$. Following [6] we shall call a covariant functor from $\mathscr{A}$ to $\mathscr{V}$ *representable* if it is isomorphic (= naturally equivalent) to one induced by a coalgebra.

If $\mathscr{A}$ is itself a variety, the identity functor of $\mathscr{A}$ is representable. The representing object is the free object on one generator $\langle x \rangle$. If we write the n-th copower of $\langle x \rangle$ as the free object $\langle x_1, \ldots, x_n \rangle$ on n generators, then to every n-ary operation λ of $\mathscr{A}$ we associate the map of $\langle x \rangle$ into $\langle x_1, \ldots, x_n \rangle$ sending x to $\lambda(x_1, \ldots, x_n)$; this gives us our Λ. In general, a functor S from a variety $\mathscr{A}$ to a variety $\mathscr{V}$ is representable if and only if it has a left adjoint T: the representing coalgebra is then the image under T of the coalgebra defining the identity functor of $\mathscr{V}$ (see [6, Theorem 2]). In informal terms, the representable functors S from $\mathscr{A}$ to $\mathscr{V}$ are those such that given $B \in \mathscr{A}$, $S(B)$ can be constructed as the set of all families of members of B on a certain index set, whose coordinates satisfy certain equations, and with operations defined by certain expressions in these coordinates, via the operations of $\mathscr{A}$. An example is the functor $GL_n(-)$: $\mathscr{A}_R{}^1 \to$ *Groups*. An element of $GL_n(B)$ can be described by giving a pair of $n \times n$ matrices P and Q over B (= a $2n^2$-tuple of elements) subject to the conditions $PQ = QP = I$ (= $2n^2$ equations); composition is defined by $(P, Q)(P', Q') = (PP', Q'Q)$, inverse by $(P, Q)^{-1} = (Q, P)$, and the identity element is (I, I). The representing object

[1] The reader who has encountered other uses of the term coalgebra, e.g., in the theory of Hopf algebras, should turn to the discussion in Section 8. We are grateful to Saunders MacLane for pointing out this possible source of confusion, and for several other useful suggestions.

of $\mathscr{A}_R{}^1$ is the algebra A defined by $2n^2$ generators p_{ij}, q_{ij} $(i, j = 1,..., n)$ and $2n^2$ relations $((p_{ij}))\,((q_{ij})) = ((q_{ij}))\,((p_{ij})) = I$. One can easily write down the co-multiplication and co-inverse operations. The coidentity element is given by a map of A into $R =$ the 0-th copower of A (the initial object of $\mathscr{A}_R{}^1$) which takes p_{ij} and q_{ij} to $\delta(i, j) \in R$.

An example of a nonrepresentable functor is the polynomial ring construction, $R \mapsto R[x]$.

2. Automorphisms and Categoricity—Generalities

By an *automorphism* of a category $\mathscr{A}$ we shall mean a functor $S : \mathscr{A} \to \mathscr{A}$ which has an "inverse" $T : \mathscr{A} \to \mathscr{A}$, in the sense that ST and TS are both isomorphic (naturally equivalent) to the identity functor of $\mathscr{A}$. The class of all automorphisms of $\mathscr{A}$ modulo equivalence of functors will form (setting aside set-theoretic quibbles) a group aut $\mathscr{A}$, called the automorphism class group of $\mathscr{A}$.

We shall call a property of objects, morphisms, etc., in a category $\mathscr{A}$ *categorical* if it can be characterized by conditions stateable in terms of morphisms, compositions, etc., but not assertions of equality of objects.[2] A property P is categorical if and only if it is invariant under all automorphisms of $\mathscr{A}$, that is, if and only if for every automorphism S of $\mathscr{A}$, $P(X) \Leftrightarrow P(S(X))$. "Only if" is clear. "If" is not so nice; to describe categorically an automorphism-invariant class of elements, one may have to allow propositions involving infinite conjunctions indexed by classes as large as the category. Allowing these, one can simply build up a proposition describing, up to isomorphism, the whole category, and the place that our given elements occupy in it!

More practically, in the categories considered in this paper, once we have found a categorical condition Q characterizing the orbit under aut $\mathscr{A}$ of the coalgebra representing the identity functor, we can take any proposition P about an R-algebra B (or a morphism, etc.) and replace it by the category-theoretic condition P' that there exist a coalgebra (A, Λ) satisfying the condition Q, such that the algebra $[A, B]_\Lambda$ has the ring-theoretic property P.

[2] The purpose of this last clause is to exclude conditions on the cardinality of isomorphism classes; e.g., the condition on an object A, $(\forall B, B \cong A \Rightarrow B = A)$, which says the isomorphism class of A is a singleton. To see how to make this "no assertions of equality" condition precise, cf. the concept in model theory, of a propositional calculus without equality.

We remark that some ring-theorists call a property of a ring A "categorical" if it can be expressed in terms of the properties of the abelian category of right A-modules. But a more common, and preferable term for such properties is Morita-invariant (cf. [3], [17]). Also, model theorists use the term "categorical" in a sense unrelated to category theory.

If P is invariant under aut $\mathscr{A}$, P' will be equivalent to P; if not, it will define the orbit under aut $\mathscr{A}$ of the class of objects satisfying P. (For example, our results will imply that the property of having a right *or* left unit *is* categorical.)

Neither of these considerations, of course, eliminates the interest of finding simple and elegant category-theoretic characterizations of important ring-theoretic properties.

(Alternatively, one could *define* categoricity to mean invariance under all automorphisms of $\mathscr{A}$, and consider characterizability by appropriate sorts of category-theoretic propositions as a criterion for categoricity—if one merely says a *sufficient condition*, one need not worry about getting the very most general sort of proposition. This definition would then be the motivation for studying aut $\mathscr{A}$.)

3. Automorphisms of $\mathscr{A}$ and Coalgebra Structures on $\langle x\rangle$

Let R be a commutative ring with unit, and $\mathscr{A}$ any one of the four categories of R-algebras, $\mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$. For any endomorphism $\varphi : R \to R$, let $I_\varphi : \mathscr{A} \to \mathscr{A}$ be the functor which leaves the underlying ring of each object of $\mathscr{A}$ unchanged (and likewise takes each homomorphism, as ring homomorphism, to itself) but assigns a new R-module structure to each $A \in \mathscr{A}$, given by $r \cdot a = \varphi(r)\, a$. Note that $I_\psi I_\varphi = I_{\varphi\psi}$, and $I_1 = 1$; hence if φ is an *auto*morphism of R, I_φ is an automorphism of $\mathscr{A}$, and we get a homomorphism aut $R \to$ aut $\mathscr{A}$, given by $\varphi \mapsto I_{\varphi^{-1}}$. In the noncommutative cases $\mathscr{A} = \mathscr{A}_R$, $\mathscr{A}_R{}^1$, let op denote the "opposite ring" functor. This satisfies $\mathrm{op}^2 = 1$, and commutes with the I_φ's, so we get a homomorphism aut $R \times \{1, \mathrm{op}\} \to$ aut $\mathscr{A}$.

Let us recall the structure of the free algebra $\langle x\rangle$ in one indeterminate, in each of our categories: In $\mathscr{A}_R{}^1$ and $\mathscr{C}_R{}^1$ it will be the polynomial ring $R[x]$; in the nonunitary categories $\mathscr{A}_R$ and $\mathscr{C}_R$, the subring thereof consisting of polynomials with zero constant term. Likewise, the free algebra on zero indeterminates, $\langle \varnothing \rangle$, the initial object, will be R in the unitary categories, $\{0\}$ in the others. The free algebra on two indeterminates, $\langle u, v\rangle$ will be the polynomial ring $R[u, v]$ in $\mathscr{C}_R{}^1$, the noncommuting polynomial ring $R\langle u, v\rangle$ in $\mathscr{A}_R{}^1$, and again the zero-constant-term subrings of these in the nonunitary categories.

In each of these categories, the coalgebra structure on $\langle x\rangle$ representing the identity functor is given by the following set Λ_{id} of maps:

coaddition	a:	$\langle x\rangle \to \langle u, v\rangle$	defined by	$a(x) = u + v$,
comultiplication	m:	$\langle x\rangle \to \langle u, v\rangle$		$m(x) = uv$,
scalar comultiplications	s_r:	$\langle x\rangle \to \langle x\rangle$ $(\forall r \in R)$		$s_r(x) = rx$,
cozero	z:	$\langle x\rangle \to \langle \varnothing\rangle$		$z(x) = 0$,

and in the unitary cases:

counit $\quad i\colon \langle x\rangle \to \langle \varnothing\rangle \qquad i(x) = 1.$

Suppose we apply one of the category-automorphisms I_φ ($\varphi \in \operatorname{aut} R$) to $\langle x\rangle$. The identity ring map between $\langle x\rangle$ and $I_\varphi(\langle x\rangle)$ will not be an isomorphism of R-algebras, but there will exist an isomorphism given by $\sum \alpha_i x^i \leftrightarrow \sum \alpha_i \cdot x^i = \sum \varphi(\alpha_i)\, x^i$. Hence the underlying object of $I_\psi((\langle x\rangle, \Lambda_{\mathrm{id}}))$ can be identified with $\langle x\rangle$, and the coalgebra structure will be given by the same maps as before, except that $s_r(x) = \varphi^{-1}(r)\, x$. The operation op similarly affects the coalgebra structure on $\langle x\rangle$ only by changing $m(x)$ from uv to vu.

An automorphism of $\mathscr{A}$ will be equivalent to the identity if and only if it takes the identity coalgebra $(\langle x\rangle, \Lambda_{\mathrm{id}})$ to an isomorphic one; and a coalgebra of the form $(\langle x\rangle, \Lambda)$ will be isomorphic to $(\langle x\rangle, \Lambda_{\mathrm{id}})$ if and only if it is taken to it by an automorphism of $\langle x\rangle$ (cf. [6, p. 105]).

If R is an integral domain, the automorphism group of $\langle x\rangle$ will consist of the maps defined by $x \mapsto \alpha(x+\beta)$, where α is an invertible element of R, and $\beta \in R$ is arbitrary in the unitary cases, zero in the nonunitary cases. This automorphism carries Λ_{id} to the coalgebra structure given by

$$\begin{aligned} a(x) &= u + v + \beta,\\ m(x) &= \alpha(u+\beta)(v+\beta) - \beta,\\ s_r(x) &= r(x+\beta) - \beta,\\ z(x) &= -\beta\\ i(x) &= \alpha^{-1} - \beta. \end{aligned}$$

It is easy to see that none of the coalgebras to which $(\langle x\rangle, \Lambda_{\mathrm{id}})$ is taken by functors I_φ ($\varphi \in \operatorname{aut} R - \{1\}$) or in the noncommutative cases, I_φ op ($\varphi \in \operatorname{aut} R$) agree with any of the above; hence the map of aut R, resp. aut $R \times \{1, \mathrm{op}\}$ into aut $\mathscr{A}$ is 1–1.

To test for the existence of other automorphisms of $\mathscr{A}$, let us examine all possible coalgebra structures on $\langle x\rangle$:

PROPOSITION 3.1. *Let R be a commutative integral domain, and $\mathscr{A}$ any one of the categories $\mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$. Then any $\mathscr{A}$-coalgebra structure Λ on $\langle x\rangle \in \mathscr{A}$, with nonzero comultiplication ($m(x) \neq z(x)$) is, up to an automorphism of $\langle x\rangle$, of the form*

$$\begin{aligned} a(x) &= u + v, && \\ m(x) &= \gamma uv \text{ or } \gamma vu && (\gamma \in R - \{0\};\ \gamma = 1 \textit{ if } \mathscr{A} = \mathscr{A}_R{}^1, \mathscr{C}_R{}^1),\\ s_r(x) &= \varphi(r)\, x && (\varphi \in \operatorname{end}(R)),\\ z(x) &= 0,\\ i(x) &= 1 && (\textit{for } \mathscr{A}_R{}^1, \mathscr{C}_R{}^1). \end{aligned}$$

If Λ is such that the functor $[\langle x\rangle, -]_\Lambda : \mathscr{A} \to \mathscr{A}$ is an isomorphism, then γ will be invertible (even in the nonunitary cases) and so can be taken (up to an automorphism of $\langle x\rangle$) to be 1, *and φ will be an automorphism of R.*

Proof. We shall give in detail the argument for the most complicated case, that of $\mathscr{A}_R{}^1$, then make the necessary remarks on the remaining cases.

Let $z(x) = \zeta \in R$; then adjusting by the automorphism of $\langle x\rangle$ taking x to $x + \zeta$, we are reduced to the case $\zeta = 0$. We also note that if $i(x)$ turns out to be an invertible element $\iota \in R$, then by applying the automorphism $x \to \iota x$, we can take $\iota = 1$.

Now as to a and m: it is known[3] that every coassociative binary cooperation $b: \langle x\rangle \to \langle u, v\rangle$ has one of the forms $b(x) = \alpha + \beta(u + v) + \gamma uv$, or $b(x) = \alpha + \beta(u + v) + \gamma vu$, with $\alpha\gamma + \beta - \beta^2 = 0$, or $b(x) = u$ or v.

Now suppose that $m(x)$ is written in one of these forms, and consider the condition that $z : \langle x\rangle \to \langle \varnothing\rangle$, given by $z(x) = 0$, be a two-sided cozero for this operation. This immediately eliminates the possibilities $m(x) = u, v$; and substituting into the remaining formulas, we get $0 = \alpha + \beta(0 + x) + \gamma 0x$, so $\alpha = \beta = 0$, and m has one of the forms γuv, γvu $(\gamma \in R)$. By symmetry of our hypothesis and conclusions, let us assume the former. For the operation to be nonzero, we must have $\gamma \neq 0$.

Writing down the conditions for z to be a coidentity with respect to our coaddition map a, we again find the possibilities $a(x) = u, v$ eliminated; and in the remaining formulas $a(x) = \alpha' + \beta'(u + v) + \gamma' uv$ (resp. vu) we get the restrictions $\alpha' = 0$, $\beta' = 1$. The condition of distributivity with respect to m finally yields $\gamma' = 0$, so $a(x) = u + v$.

Next, given $r \in R$, let us write $s_r(x) = P(x)$, P a polynomial. By the associativity of the scalar and internal comultiplications of Λ, we must have $P(\gamma uv) = \gamma P(u)\, v$; hence as $\gamma \neq 0$, P is homogeneous of, degree 1, and $P(x)$ can be written $\varphi(r)\, x$, for some unique $\varphi(r) \in R$. It is easy to check that $\varphi : R \to R$ must be a ring endomorphism.

Finally, the fact that i is a coidentity for m tells us $\gamma\iota x = x$, hence $\gamma\iota = 1$;

[3] See [5, p. 169, Exercise 2]. This exercise is not quite correct as it stands; a correct version would be:

"If K is a commutative integral domain, and $f(x, y)$ is a derived operator in the variety of associative K-algebras with 1, such that $f(x, f(y, z)) = f(f(x, y), z)$, show that f is of one of the forms $x, y, \alpha + \beta(x + y) + \gamma xy, \alpha + \beta(x + y) + \gamma yx$, where $\alpha\gamma + \beta - \beta^2 = 0$."

Idea of proof. Simply by considering degrees in x, y, z, one can show that the degree of $f(x, y)$ in both x and y must be $\leqslant 1$. By looking at leading terms, one sees that it cannot have both xy and yx terms; say it has no yx terms. Then writing $f(x, y) = \alpha + \beta x + \beta' y + \gamma xy$, it is easy to equate coefficients in the associativity formula and check that the condition given is necessary and sufficient.

but as we observed, if ι was invertible we could take it equal to to 1, giving the desired representation of Λ.

The same arguments all go over easily to the three other cases, except that various observations may be dropped: the reduction to $z(x) = 0$ and $\gamma = 1$ in the nonunitary cases, of which the first is automatic ($\langle \varnothing \rangle = \{0\}$) and the second not asserted; the distinction between uv and vu in the commutative case.

It is also easy to check that every system Λ of the sort listed does give an $\mathscr{A}$-coalgebra structure on $\langle x \rangle$. This proves the first claim of our Proposition.

Now consider the functor $[\langle x \rangle, -]_\Lambda : \mathscr{A} \to \mathscr{A}$ induced by Λ. If $\mathscr{A}$ is one of the nonunitary categories, and γ is not invertible, let us form in $\mathscr{A}$ the ring $R/\gamma R$, and the ring having the same R-module structure, but zero (internal) multiplication. These rings are nonisomorphic in $\mathscr{A}$, but their images under our functor will be isomorphic, so this functor is not an automorphism of categories.

Hence if Λ is such that our functor is invertible, γ will be invertible, and we can take $\gamma = 1$. Further, since our functor takes $\langle x \rangle$ to $\langle x \rangle$, its inverse must also do so, hence will be of the same form, but involving some other endomorphism φ'. Their compositions will similarly involve $\varphi'\varphi$ and $\varphi\varphi'$; but for such a coalgebra structure on $\langle x \rangle$ to be isomorphic to the identity, we have previously observed that the endomorphism involved must be 1; so $\varphi'\varphi = \varphi\varphi' = 1$. Hence φ must be an automorphism of R, establishing our last assertion. ∎

COROLLARY 3.2. *Let R be an integral domain. Then any automorphism of $\mathscr{A}$ preserving the isomorphism class of $\langle x \rangle$ is isomorphic to one of the form I_φ or (in the noncommutative cases) I_φ* op, *where $\varphi \in$* aut *R; and all these automorphisms are pairwise nonisomorphic.* ∎

Remark. To see why we excluded coalgebra structures with zero comultiplication in Proposition 3.1, suppose R is of characteristic $p \neq 0$, and on any algebra $A \in \mathscr{C}_R$ or $\mathscr{C}_R{}^1$, let $\mathbf{p} : A \to A$ denote the Frobenius map $t \mapsto t^p$. This will be an endomorphism of A as a ring, and hence any R-linear combination of powers of $\mathbf{p}$, that is, any Φ in the polynomial ring $R[\mathbf{p}]$, will be an endomorphism of A as an additive group. One can show that these are the only derived operations of $\mathscr{C}_R$ and $\mathscr{C}_R{}^1$ with this property; while when char $R = 0$, or $\mathscr{A} = \mathscr{A}_R$ or $\mathscr{A}_R{}^1$, there are no such operations but the scalar multiplications. We can now sketch the proof of a result rounding off Proposition 3.1; the interested reader should be able to fill in the details without much difficulty.

COROLLARY 3.3 (to the proof of Proposition 3.1). *If R is a commutative* *ring, and* $\mathscr{A} = \mathscr{A}_R$ *or* $\mathscr{C}_R$, *then the* $\mathscr{A}$*-coalgebra structures on* $\langle x \rangle \in \mathscr{A}$ *having* zero *comultiplication are given by the same formulas as in Proposition* 3.1 *with* 0 *for* γ, *except that if* $\mathscr{A} = \mathscr{C}_R$, *and* char $R = p \neq 0$, *for* $\varphi(r)\, x$ *we must read* $\Phi_r(x)$, *where* Φ *is a ring homomorphism of* R *into* $R[\mathbf{p}]$.

Idea of proof. In the proof of Proposition 3.1, we used the hypothesis of nonzero comultiplication, which is equivalent to $\gamma \neq 0$, to show that the coefficient γ' in $a(x)$ was zero, and to show that the $s_r(x)$ were scalar multiples of x. To obtain the first of these conclusions here we can argue instead from the fact that there exists a coinverse with respect to a, namely s_{-1}. For the second case, if we use the fact that the maps s_r codistribute with respect to a, then by our preceeding observations we find that $s_r(x)$ will have the form $\Phi_r(x)$ ($\Phi_r \in R[\mathbf{p}]$) if char $R \neq 0$ and $\mathscr{A} = \mathscr{C}_R$; the form $\varphi(r)x$ ($\varphi(r) \in R$) otherwise. It is easy to check that we get a coalgebra if and only if Φ (resp. φ) is a ring homomorphism (e.g., if $R = \mathbf{Z}_p[t]$, Φ could send t to $\mathbf{p}$). ∎

4. Category-Theoretic Characterizations of Ring Properties

We now prepare for the proof of our main result by showing how various algebraic concepts can be expressed categorically. The verifications of most of the assertions below are straightforward and we omit them. Let R be a commutative integral domain with unit. When the contrary is not stated, our observations apply to all of the categories $\mathscr{A} = \mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$. Asterisks mark results which in fact hold in every variety $\mathscr{A}$ of algebras in the sense of universal algebra.

*4.1. A morphism f of algebras is one-one if and only if it is a monomorphism. Hence we may speak "categorically" of *subalgebras* and *embeddings*.

*4.2. A morphism f in $\mathscr{A}$ will be *surjective* if and only if for any factorization $f = pq$, $A \xrightarrow{q} C \xrightarrow{p} B$, if p is a monomorphism then p is an isomorphism. Hence we may speak of *homomorphic images*, or *quotient* algebras. (Morphisms f with the above property in an arbitrary category are called extremal epimorphisms by Isbell [7].) Surjections can also be characterized as difference-cokernels.

*4.3. An algebra $P \in \mathscr{A}$ will be called *projective* if, given any surjection $f\colon A \to B$, every homomorphism of P into B can be factored through f. (More precisely, such P are "projective with respect to surjections;" one can similarly define in any category algebras "projective with respect to epimorphisms", etc.; but the latter class, for instance, is trivial in our categories.) Using the fact that any algebra P is a surjective image of a free algebra, one finds that an algebra P is projective if and only if it is a retract (the image of an idempotent endomorphism) of a free algebra. Thus we get our first toehold on characterizing the free algebras in $\mathscr{A}$.

*4.4. The free algebra on the empty set, $\langle \varnothing \rangle$, is characterizable as the initial object of $\mathscr{A}$. We shall call this the trivial algebra. Any other algebra, even, say, the final algebra $\{0\}$ in the unitary cases, will be called nontrivial.

4.5. Note that because R is an integral domain, any nonscalar element of a free algebra in $\mathscr{A}$ generates a subalgebra isomorphic to $\langle x \rangle$. It follows that the class of algebras A embeddable in $\langle x \rangle$ can be characterized category-theoretically as those algebras embeddable in all nontrivial projective objects of $\mathscr{A}$.

(We now have enough information to characterize $\langle x \rangle$ in the case where R is a field—see Proposition 5.1 below.)

*4.6. If S is any class of algebras in $\mathscr{A}$, the *subvariety* of $\mathscr{A}$ *generated* by S can be characterized as the class of all algebras which are homomorphic images of subalgebras of direct products of algebras in S (a corollary of a theorem of Birkhoff: [5, Theorem IV 3.5]).

4.7. In particular, in $\mathscr{A}_R$ and $\mathscr{A}_R{}^1$, the subvariety generated by $\langle x \rangle$, which by 4.5 will be the subvariety generated by those algebras embeddable in all nontrivial projectives, can be characterized categorically. But this subvariety is easily seen to be $\mathscr{C}_R$, respectively, $\mathscr{C}_R{}^1$. Hence if we can identify the object $\langle x \rangle$ in these commutative categories, we will have a way of finding them in $\mathscr{A}_R$ and $\mathscr{A}_R{}^1$ as well.

4.8. For $\mathscr{A} = \mathscr{A}_R{}^1$ or $\mathscr{C}_R{}^1$, let us define $\mathscr{A}^{\cdot}$, the category of "augmented" objects of $\mathscr{A}$, to have for objects the pairs (A, z), where A is an object of $\mathscr{A}$, and z, the "augmentation map," a homomorphism of A to $\langle \varnothing \rangle = R$; with morphisms defined as homomorphisms of the first components, that form commutative triangles with the augmentations. Then $\mathscr{A}_R^{1\cdot}$ and $\mathscr{C}_R^{1\cdot}$ are naturally isomorphic to $\mathscr{A}_R$ and $\mathscr{C}_R$. The map one way, given by $(A, z) \mapsto \ker z$ (considered an algebra without 1), and the map back, given by the "adjunction of unit" functor, sending an algebra A to the set of pairs (r, a) $(r \in R,\ a \in A)$ with component-wise addition, and with $(r, a)(r', a') = (rr', ra' + r'a + aa')$, are easily shown to be inverses. Since the augmented algebra $(\langle x \rangle, z) \in \mathscr{A}_R^{1\cdot}$ or $\mathscr{C}_R^{1\cdot}$ $(z(x) = 0)$ clearly corresponds to the algebra $\langle x \rangle$ of $\mathscr{A}_R$, respectively $\mathscr{C}_R$, if we can show how to identify this algebra in the latter categories, we will be able to give a description of $\langle x \rangle$ in $\mathscr{A}_R{}^1$ and $\mathscr{C}_R{}^1$, by saying "an algebra for which there exists an augmentation z, such that certain conditions hold."

The above two remarks reduce our task to that of identifying the object $\langle x \rangle$ in $\mathscr{C}_R$. We shall henceforth concentrate on this category, and state results in more general contexts only when convenient.

4.9. In $\mathscr{C}_R$ or $\mathscr{A}_R$, the *kernel* of a map $f: A \to B$ can be characterized as the maximal subalgebra C of A annihilated by f (i.e., such that $f \mid C$ factors through the initial/final object $\{0\}$.) The *ideal* of A generated by the image of some map $g: C' \to A$ is thus the minimal subalgebra C through which g factors, and which is the kernel of a morphism f.

4.10. In $\mathscr{C}_R$, the coproduct A^* of two algebras has the form $A \oplus B \oplus (A \otimes B)$, with componentwise addition, and multiplication given by

$$(a, b, c)\,(a', b', c') = (aa', bb', \text{all 7 other terms}),$$

i.e., $A * B$ consists of elements of A plus elements of B plus products of these, with multiplication defined as it must be. Hence $A \otimes B$ may be constructed as the kernel of the natural map $A * B \to A \times B$. ($A \otimes B$ can easily be shown functorial in A and B, but, in the absence of units, there are no natural maps of A and B into $A \otimes B$. In $\mathscr{C}_R{}^1$, $A * B = A \otimes B$, and *ipso facto*, we get natural maps. In $\mathscr{A}_R$ and $\mathscr{A}_R{}^1$, coproducts are more complicated to describe.)

4.11. An object of a variety is called *simple* if it is nonfinal, but has no proper homomorphic images but the final object. The simple objects of $\mathscr{C}_R$ are the fields, and the simple R-modules with zero multiplication. Hence if $A \in \mathscr{C}_R$ is an integral domain, its field of fractions will be the unique minimal simple R-algebra in which A embeds. Now the fields of fractions of nontrivial projective objects in $\mathscr{C}_R$ will all have the same unique minimal simple subobject, the field of fractions K of R. Hence we have characterized K in $\mathscr{C}_R$.

(4.12. In fact, it is not hard to distinguish fields from zero-multiplication rings. A ring A will have zero multiplication if and only if diagram (1) can be completed so that both compositions are the identity. More generally, two subrings I, $J \subseteq A$ have zero product if and only if diagram (2) can be

$$A \underset{(0,\, \mathrm{id}_A)}{\overset{(\mathrm{id}_A,\, 0)}{\rightrightarrows}} A \times A \dashrightarrow A. \tag{1}$$

$$\begin{matrix} I \xrightarrow{(\mathrm{id}_I,\, 0)} \\ J \xrightarrow[(0,\, \mathrm{id}_J)]{} \end{matrix} I \times J \dashrightarrow A. \tag{2}$$

completed so that both compositions are the inclusions.)

4.13. Thus, we can now characterize the category $\mathscr{C}_K \subseteq \mathscr{C}_R$, as consisting of all objects isomorphic in $\mathscr{C}_R$ to objects of the form $A \otimes K$, $A \in \mathscr{C}_R$. If $f: A \to B$ is a morphism in $\mathscr{C}_R$, from an arbitrary R-algebra to a K-algebra, then $f(A)$ will generate B as a K-algebra if and only if f cannot be factored through any nonisomorphic monomorphism in $\mathscr{C}_K$.

*4.14. In any category $\mathscr{A}$, a *generator* is defined as an object G such that, given any two maps $f \neq f' : A \to B$, there exists a map $g : G \to A$ with $fg \neq f'g$. (More generally, one can define a generating family. For $\mathscr{A}$ a variety, this is *not* the same as a family generating $\mathscr{A}$ as a variety! For example, $\langle x \rangle$ is a generator in $\mathscr{A}_R$ or $\mathscr{A}_R{}^1$, but does not generate it as a variety; if $R \neq K$, K generates $\mathscr{C}_R{}^1$ as a variety, but is not a generator. Rather, in any category with arbitrary coproducts, a set of objects $\mathscr{G}$ will be a generating set if and only if for every $A \in \mathscr{A}$, some coproduct of objects in $\mathscr{G}$, with repetitions allowed, can be mapped epimorphically into A.) In any variety, any free object on > 0 indeterminates is a generator.

5. The Main Result

Proposition 5.1. *Let K be a field. Then in any of the categories $\mathscr{A} = \mathscr{A}_K, \mathscr{A}_K{}^1, \mathscr{C}_K, \mathscr{C}_K{}^1$, the free object $\langle x \rangle$ on one generator can be characterized as the unique nontrivial projective object A that is embeddable in all nontrivial projective objects.*

Proof. Clearly $\langle x \rangle$ has these properties. Now let A be any object with these properties. We know that A is embeddable in $\langle x \rangle$, hence commutative, hence even if our category is one of the noncommutative ones, A can be written as an image, and hence, being projective, as a retract, of some free *commutative* K-algebra F (with or without unit). Assume we are in a category of algebras with unit. We know the polynomial ring F is integrally closed, hence so is the retract A. But any integrally closed nontrivial K-algebra embeddable in a polynomial algebra $K[x]$ is isomorphic to $K[x]$ (Cohn [4, Proposition 2.1]; an application of Lüroth's Theorem). Hence $A \cong \langle x \rangle$. For the case without unit, one may either extend the results quoted to rings without unit, which is fairly easy, or demonstrate that the adjunction-of-unit functor from $\mathscr{C}_K$ to $\mathscr{C}_K{}^1$ (cf. 4.8) preserves projectives, and the isomorphism class of $\langle x \rangle$, and so allows us to carry over our result. ∎

If R is a commutative integral domain with field of fractions K, and A a nontrivial projective R-algebra embeddable in all nontrivial projective R-algebras, then one can show from the above result that $A \otimes K$ is isomorphic to the free K-algebra $\langle x \rangle_K$ ($\in \mathscr{A}_K, \mathscr{A}_K{}^1, \mathscr{C}_K, \mathscr{C}_K{}^1$ as the case may be). If R is in fact a unique factorization domain, one can show by factorization-arguments that any commutative R-algebra A which is a retract of a polynomial ring and satisfies $A \otimes K \cong \langle x \rangle_K$ is isomorphic to $\langle x \rangle$. We omit details because we shall not use the result; let us merely record.

Corollary 5.2. *The result of Proposition 5.1 holds with K replaced by an arbitrary commutative UFD, R.* ∎

But, as we shall see in the next section, this criterion fails for R a general commutative integral domain, hence we shall need more complicated conditions.

Let R be a commutative integral domain and K its field of fractions. By 4.13 we can characterize the subcategory $\mathscr{C}_K \subseteq \mathscr{C}_R$, so by Proposition 5.1 we can identify the isomorphism class of the free K-algebra $\langle x \rangle_K$. Also, by the proof of Proposition 3.1, the map m_K: $\langle x \rangle_K \to \langle x \rangle_K * \langle x \rangle_K = \langle u, v \rangle_K$ sending x to uv is determined, up to isomorphism, by the properties of being coassociative and nonzero, and having as left and right cozero the (unique) map z: $\langle x \rangle_K \to \langle \varnothing \rangle = \{0\}$. Given these observations, the categoricity of $\langle x \rangle$ follows from the following ring-theoretic result:

PROPOSITION 5.3. *Let $A \in \mathscr{C}_R$ be an R-subalgebra of $\langle x \rangle_K$ such that*

(i) *A generates $\langle x \rangle_K$ as a K-algebra,*

(ii) *A is a generator in $\mathscr{C}_R$ (cf. 4.14),*

(iii) *m_K extends to A; that is, there exists a map m making the diagram*

$$\begin{tikzcd} A \arrow[r, dashed, "m"] \arrow[d] & A * A \arrow[d] \\ \langle x \rangle_K \arrow[r, "m_K"] & \langle x \rangle_K * \langle x \rangle_K = \langle u, v \rangle_K \end{tikzcd}$$

commutative; and further:

(iv) *The ideal of $A * A = A \oplus A \oplus (A \otimes A)$ generated by $m(A)$ is precisely $A \otimes A$ (cf. 4.10).*

Then A is precisely the subalgebra $\langle x \rangle \subseteq \langle x \rangle_K$.

Proof. For each positive integer n, let I_n denote the R-submodule of K consisting of all elements of K occurring as coefficients of x^n in elements of $A \subseteq \langle x \rangle_K$. Now by hypothesis (i), A must contain some element of the form cx, $0 \neq c \in K$. Let M be any torsion-free R-module and $\overline{M} \in \mathscr{C}_R$ this same module considered as an R-algebra with zero multiplication. Any algebra homomorphism $f : A \to \overline{M}$ will satisfy $0 = f(cx)^n = f(c^n x^n)$ $(n > 1)$, hence, as M is torsion-free, f must annihilate any element of the form $\alpha_2 x^2 + \cdots + \alpha_n x^n \in A$ $(\alpha_i \in K)$, hence is described uniquely by a module-homomorphism of I_1 into M. Taking $M = R$, the free R-module of rank 1, we see from hypothesis (ii) that R is generated as an R-module by homomorphic images of I_1. This means I_1 is an invertible fractional ideal of R.

To make use of hypotheses (iii) and (iv), let us denote by $A(u)$, $A(v)$ and $A(uv)$ the images in $\langle u, v\rangle_K$ of $A \subsetneq \langle x\rangle_K$ under the substitutions $x \mapsto u$, $x \mapsto v$, and $x \mapsto uv$, respectively. Thus, in the diagram of (iii), the image of A (upper left corner) in $\langle u, v\rangle_K$ is $A(uv)$, that of $A * A$ is $A(u) + A(v) + A(u)\,A(v)$, and that of $A \otimes A \subseteq A * A$ is $A(u)\,A(v)$. Note that if S is a subset of an algebra $U \in \mathscr{C}_R$, the ideal of U generated by S may be written $S(R + U)$, where "R" denotes scalar multiplications. Hence if we take condition (iv) and look at images in $\langle u, v\rangle_K$, we get

$$A(uv)\,(R + A(u) + A(v) + A(u)\,A(v)) = A(u)\,A(v). \tag{3}$$

Taking the coefficient of uv^n in (3), we get

$$I_1 I_{n-1} = I_1 I_n \qquad (n = 2, 3, \ldots),$$

where, we see, to make this equation hold for $n = 1$ as well, we should define $I_0 = R$. We thus get $I_1 R = I_1 I_1 = I_1 I_2 = \cdots$, and since I_1 is an *invertible* fractional ideal, we conclude $R = I_1 = I_2 = \cdots$. In particular, $A \subseteq \langle x\rangle$. Further, since $I_1 = R$, we can choose $f(x) \in A$ in which the coefficient of x is 1. By (3) [or by hypothesis (iii)], $f(uv) \in A(u)\,A(v)$. Taking the $A(v)$-coefficient of u, we get $v \in I_1 A(v) = A(v)$, which means $x \in A$, so $A = \langle x\rangle$. ∎

It is clear that, conversely, the subring $\langle x\rangle \subseteq \langle x\rangle_K$ satisfies the hypotheses of the above Proposition. All the conditions of these hypotheses have category-theoretic characterizations, by Section 4, so we get

COROLLARY 5.4. *The isomorphism class of* $\langle x\rangle$ *can be described categorically in* $\mathscr{C}_R$. *Hence* (*by* 4.7, 4.8) *the same is true in* $\mathscr{C}_R{}^1$, $\mathscr{A}_R$, $\mathscr{A}_R{}^1$. ∎

Combining with Corollary 3.2, we get

THEOREM 5.5. *Let R be any commutative integral domain. Then the automorphism class groups of* $\mathscr{A}_R$ *and* $\mathscr{A}_R{}^1$ *are given by* aut $R \times \{1, \mathrm{op}\}$ (*as described in Section* 2); *those of* $\mathscr{C}_R$, $\mathscr{C}_R{}^1$ *by* aut R. ∎

6. COUNTEREXAMPLES

Let us show why such a complicated set of conditions was needed in Proposition 5.1.

EXAMPLE 6.1. Let R be any commutative integral domain having a nonprincipal invertible fractional ideal I, e.g., any Dedekind domain that is not a PID. Without loss of generality we shall assume $I \subset R$. Let $A \in \mathscr{C}_R$

be the R-subalgebra of $\langle x\rangle_K$ generated by xI^{-1}. This is the symmetric algebra on the R-module I^{-1}. The latter is a projective generator of the category of R-modules; it will in fact be a direct summand in the free module of rank 2; one can deduce that A will be a projective generator of the category $\mathscr{C}_R$, a retract of the free algebra on two generators. It is not isomorphic to $\langle x\rangle$, because $A/AA \cong_{R\text{-module}} I^{-1} \not\cong R \cong_{R\text{-module}} \langle x\rangle/\langle x\rangle\langle x\rangle$ (where AA means the square of A as an ideal of A.)

It is not hard to show that not only m_K, but the whole $\mathscr{C}_R$-coalgebra structure on $\langle x\rangle_K$ extends to A. (The corresponding functor sends any *R-torsion-free* $B \in \mathscr{C}_R$ to the subalgebra IB. The description for algebras with R-torsion is a bit more complicated.)

Thus this example shows that in $\mathscr{C}_R$, $\langle x\rangle$ cannot be characterized by the condition of being a nontrivial projective, embeddable in all nontrivial projectives, *plus* the first three conditions of Proposition 5.3! The analogous construction in $\mathscr{A}_R$ has similar properties.

Though we have shown the class of coalgebra structures on $\langle x\rangle$ (in $\mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$) quite small, the class of *all* coalgebras (in any of these categories), and hence the class of representable *endo*morphisms, is quite large and diverse, cf. the exposition of the Witt-ring functor in [9, Lecture 26] and the other examples given there. Here are some further examples.

EXAMPLE 6.2. Let $\mathbf{Z}$ be the ring of integers, $\mathbf{Q}$ the field of rational numbers, and $A \in \mathscr{C}_{\mathbf{Z}}{}^1$ the subring of $\langle x\rangle_{\mathbf{Q}} = \mathbf{Q}[x]$ consisting of all "integral polynomials," that is, polynomials whose values at integral arguments are integers. A is known to have for additive basis the elements $1 = \binom{x}{0}$, $x = \binom{x}{1}$, $x(x-1)/2 = \binom{x}{2}$,... . It is not hard to show that any integral polynomial in two indeterminates, $f(u, v)$, can be written $\sum g_i(u)\, h_i(v)$ $(g_i, h_i \in A)$. In particular, if $f \in A$, then $f(u+v)$ and $f(uv) \in A * A$; from these, and the analogous observations on inverse, 0 and 1, one can conclude that the coalgebra structure on $\langle x\rangle$ induces one on A as well.

If B is a $\mathbf{Z}$-algebra with torsion-free additive group, the ring $[A, B]_\Lambda$ can be identified with the subring of B consisting of all elements b such that $\forall n$, $\binom{b}{n} \in B$. E.g., if B is a $\mathbf{Q}$-algebra, $[A, B]_\Lambda \cong B$, while if $B = \mathbf{Z}[x]$ or $\mathbf{Z}[\sqrt{-1}]$, then $[A, B]_\Lambda \cong \mathbf{Z}$! If B is not torsion-free, $[A, B]_\Lambda$ can be thought of as the ring of "elements $b \in B$, together with formal evaluations in B of the binomial polynomials $\binom{b}{2}$, $\binom{b}{3}$,... ." One can show that if B is *any* field of characteristic $p \neq 0$, then $[A, B]_\Lambda$ is isomorphic to the ring of p-adic integers.

The existence of this example seems to result from the fact that $\mathbf{Z}$ is a subdirect product of finite fields.

EXAMPLE 6.3. Coalgebras (A, Λ) with A not torsion-free over R: Let R be a commutative ring, $\mathscr{A}$ any of $\mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$, and I a proper nonzero ideal of R. The functor associating to every $B \in \mathscr{A}$ the algebra of all formal power series $b_0 + b_1 t + \cdots \in B[\![t]\!]$, such that $b_i I = 0$ for $i > 0$, is represented by a coalgebra whose underlying algebra is $\langle x_0, x_1, \ldots\rangle/(x_1 I, \ldots)$.

EXAMPLE 6.4. If k is a perfect field of characteristic $p \neq 0$, the functor associating to $B \in \mathscr{C}_k{}^1$ (or $\mathscr{C}_k$) the algebra of all sequences $(b_0, b_1, \ldots)$ with $b_i = b_{i+1}^p$, where addition and multiplication are defined coordinate-wise, and scalar multiplication by $\alpha(b_0, b_1, \ldots) = (\alpha b_0, \alpha^{1/p} b_1, \ldots)$, is representable by a coalgebra whose underlying algebra is $\langle x, x^{1/p}, \ldots\rangle$. If the hypothesis that k be perfect is weakened to: k is embeddable in a perfect subfield of itself, $\varphi : k \to F \subseteq k$, we can still get a functor with this underlying algebra by defining $\alpha(b_0, b_1, \ldots) = (\varphi(\alpha)\, b_0, \varphi(\alpha)^{1/p}\, b_1, \ldots)$.

EXAMPLE 6.5. If k is a finite field of q elements, and n a positive integer, the functor associating to $B \in \mathscr{C}_k{}^1$ or $\mathscr{C}_k$ the subalgebra of all elements $b \in B$ satisfying $b^{q^n} = b$ is represented by a coalgebra whose underlying algebra is of the form $\langle x\rangle/(x^{q^n} - x)$.

Note that all of the above examples involved either a category of *commutative* algebras, or a base ring that was not a field. In [11] it will be shown that representable functors on categories $\mathscr{A}_K$ and $\mathscr{A}_K{}^1$ are much better behaved.

7. FURTHER QUESTIONS

If the commutative ring R has zero-divisors, the formula quoted in Section 3 no longer gives the most general coassociative map b: $\langle x\rangle \to \langle u, v\rangle$ in $\mathscr{A}_R{}^1$, e.g., if $\gamma\gamma' = 0$, the map sending x to $\gamma uv + \gamma' vu$ is coassociative. However, if Λ is an $\mathscr{A}_R{}^1$-coalgebra structure on $\langle x\rangle \in \mathscr{A}_R{}^1$, then for every prime ideal $p \subseteq R$, Λ will induce an $\mathscr{A}_R{}^1$-coalgebra structure on $\langle x\rangle_{R/p} \in \mathscr{A}^1_{R/p}$ (and similarly in our other categories). If R has no nonzero nilpotents, so that the intersection of all prime ideals is zero, this gives us enough information to describe all such coalgebra structures: Reducing, as in Proposition 3.1, to the case $z(x) = 0$, we can show by the method of that Proposition that for $\mathscr{A} =$ any of our four categories, any coalgebra structure on $\langle x\rangle$ that does not send any of the subcategories $\mathscr{A}_{R/p}$ (p prime) into the category of zero-multiplication rings will be given by the same bank of formulas as in that Proposition, except (1) the condition on γ is that it not lie in any p, hence that it be invertible, hence we can take $\gamma = 1$, and (2) (more important!) the formula for $m(x)$, in the noncommutative case, instead of being "*uv or vu*", becomes $(1 - \eta)\, uv + \eta\, vu$, where η is an arbitrary idempotent element of R.

Let us denote by $B(R)$ the Boolean ring of idempotent elements of R, with addition $\eta(+)\,\eta' = \eta + \eta' - 2\eta\eta'$, and multiplication as in R. For any $\eta \in B(R)$, define the functor $\mathrm{op}^{\eta}\colon \mathscr{A}_R \to \mathscr{A}_R$ to send every ring to the ring with the same elements, and the same operations except that the new multiplication is defined by $x \cdot y = (1-\eta)\,xy + \eta yx$. The symbolism is suggested by looking at η as a $\{0, 1\}$-valued function on spec R; op^{η} then acts as the identity "over" the set where $\eta = 0$, and as op over the set where $\eta = 1$. These functors compose by the rule $\mathrm{op}^{\eta}\mathrm{op}^{\eta'} = \mathrm{op}^{\eta(+)\eta'}$, and thus form an abelian group of exponent 2.

Thus one can show that every coalgebra structure on $\langle x\rangle$ which induces an automorphism of $\mathscr{A}_R$ or $\mathscr{A}_R{}^1$ will induce one of the form $I_\varphi \mathrm{op}^{\eta}$. The functors I_φ and op^{η} do not in general commute; rather, aut R acts on $B(R)$, and we have $\mathrm{op}^{\eta} I_\varphi = I_\varphi \mathrm{op}^{\varphi(\eta)}$. So the group of automorphisms of $\mathscr{A}_R$ or $\mathscr{A}_R{}^1$ that preserve $\langle x\rangle$, is a semidirect product, aut R Ⓢ $\mathrm{op}^{B(R)}$. Of course, for $\mathscr{C}_R$ and $\mathscr{C}_R{}^1$, we again just get aut R.

We expect that the results of Sections 4–5 can likewise be extended easily to rings R without nilpotent elements. In place of the field of fractions of R, one would introduce the enveloping von Neumann regular ring K; $\langle x\rangle_K$ can probably be characterized as the unique projective generator of $\mathscr{C}_K$ embeddable in all projective generators, and the proof that all automorphisms of $\mathscr{A}$ have the form described completed with the equivalent of Proposition 5.3.

If R has nilpotents, things are very different. We do not know of any new automorphisms of our categories; but the automorphism group of the object $\langle x\rangle$ becomes very large: the map taking x to $\alpha_0 + \alpha_1 x \cdots + \alpha_n x^n$ is an automorphism if (and only if) α_1 is invertible, and $\alpha_2, \ldots, \alpha_n$ are nilpotent. This group acts on the class of coalgebra structures on $\langle x\rangle$, making it so large that we do not see how to determine whether all coalgebra structures which induce automorphisms of $\mathscr{A}$ are isomorphic to known ones. Likewise, the problem of characterizing $\langle x\rangle$ seems much more difficult, because we do not have a well-behaved analog of the field of fractions of R.

Hence we can merely state

PROBLEM 7.1. *If R is any commutative ring, will every automorphism of one of our four categories of R-algebras be of the form $I_\varphi \mathrm{op}^{\eta}$ in the noncommutative cases, or I_φ in the commutative cases ($\varphi \in$ aut R, $\eta \in B(R)$)?*

Our characterization of the free object on one generator in Proposition 5.1 suggests the question: in the categories $\mathscr{A}_K$, $\mathscr{A}_K{}^1$, $\mathscr{C}_K$, $\mathscr{C}_K{}^1$, are all projective objects free? This is a special case of a more general question of interest:

PROBLEM 7.2. *Let K be a field, $\mathscr{A}$ any of the categories $\mathscr{A}_K$, $\mathscr{A}_K{}^1$, $\mathscr{C}_K$, $\mathscr{C}_K{}^1$. What conditions on a subalgebra G of a free algebra $F \in \mathscr{A}$ imply that G is also free?*

Thus our question about projectives asks whether being a *retract* of F in $\mathscr{A}$ is such a condition. (When $\mathscr{A} = \mathscr{A}_K{}^1$ it is easy to prove that such a retract will be a *free ideal ring*. It can also be deduced from [13, Cor. to Prop. 6.8.2] that any projective object on $\leqslant 2$ generators in $\mathscr{A}_K{}^1$ is free.)

Another condition, suggested by Alan G. Waterman for the category $\mathscr{A}_K{}^1$ (oral communication) is that as right G-modules, G be a direct summand in F, with a free complementary summand. (He in fact conjectures that if F is free of rank $n < \infty$ and the complement of G is a free module of rank $r < \infty$, then the rank of G as a free algebra will be given by the Schreier formula, $r(n - 1) + 1$.) There are numerous possible variants of this conjecture: one might assume *only* that G is a direct summand in F as a G-module, or that F is free as a G-module, or that F or F/G is flat as a right G-module. Waterman also conjectures that G will be free if it is a direct summand in F as a G-bimodule. This and its one-sided analog both include the case of G a retract of F as algebras.

Still other plausible conditions are that G be the fixed ring of an automorphism of F, or of an arbitrary family of endomorphisms (cf. [10, Section 2]).

On the other hand, the second author has examples showing that the kernel of a derivation on $F \in \mathscr{A}_K{}^1$ need not even be a 2-fir, and that a subring of F that is a fir need not be free. Note also that some of the conditions proposed above for $\mathscr{A}_K{}^1$ are definitely not sufficient in $\mathscr{C}_K{}^1$: $G = \langle x^2, xy, y^2 \rangle \subseteq \langle x, y \rangle = F$ is not free, but it is both the fixed ring of the automorphism $x \to -x$, $y \to -y$, and a direct summand as G-modules.

Recall that by a theorem of Birkhoff [3, IV.3.1] a class of algebras of a given type forms a variety if and only if it is closed under arbitrary direct products, subalgebras, and homomorphic images. Similar characterizations are known for classes of algebras closed under other combinations of operations (e.g., [3, IV.4.3, 4]).

PROBLEM 7.6 (G.-C. Rota). *What can be said, in the same vein, about classes of "coalgebras" (of given cotype, in a given variety) satisfying appropriate closure conditions, or characterized by appropriate sorts of predicates?*

8. REMARKS ON THE CONCEPT OF COALGEBRA

The idea of coalgebra used in this article, and the dual concept of an algebra object in a category, can be put in a more general context. If $\mathscr{C}$ is any category, and $\diamondsuit : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ a coherently associative bifunctor [15, Ch. 7, Sec. 1], then one may define a $(\mathscr{C}, \diamondsuit)$-algebra or coalgebra as an object $A \in \mathscr{C}$ given with a family of maps $A \diamondsuit \cdots \diamondsuit A \to A$, respectively, $A \to A \diamondsuit \cdots \diamondsuit A$.

Clearly, the concept of coalgebra used here was a special case of this, with $*$ for $\diamondsuit$. Another important family of coherently associative bifunctors is given by the operations $\otimes$ on the categories $\mathscr{M}_R$ of modules over a commutative ring R, as well as $\mathscr{A}_R$, $\mathscr{A}_R{}^1$, $\mathscr{C}_R$, $\mathscr{C}_R{}^1$. In particular, an associative R-algebra can be described as an $(\mathscr{M}_R, \otimes)$-semigroup! Hence the term "coalgebra" has been used to refer to an $(\mathscr{M}_R, \otimes)$-cosemigroup, i.e., a module A with a coassociative map $A \to A \otimes A$. These are introduced in the study of Hopf algebras, which are, more or less, $(\mathscr{A}_R, \otimes)$-cosemigroups. The class of Hopf algebras partly overlaps the concept of coalgebra discussed in Section 1 above: Because tensor product equals coproduct in $\mathscr{C}_R{}^1$, *commutative* Hopf algebras are, in the language of Section 1, cosemigroup objects of $\mathscr{C}_R{}^1$.

We remark that to write down for a $(\mathscr{C}, \diamondsuit)$-algebra or coalgebra an identity involving reordering of terms, e.g., commutativity, one must have $\diamondsuit$ symmetric, i.e., one must have a functorial isomorphism between $A \diamondsuit B$ and $B \diamondsuit A$ $(A, B \in \mathscr{C})$. To express an identity in which some variable occurs more than once on one side, e.g., $(xy)\, x = x(yx)$ or $x \cdot (x^{-1}) = e$, one must have a (co)diagonal map $\Delta : A \to A \diamondsuit A$, resp., $A \diamondsuit A \to A$; or some reasonable substitute. These conditions *are* satisfied by the operation of product, respectively coproduct, in any category (for which products or coproducts exist.)

References

1. G. M. Bergman, Centralizers in free associative algebras, *Trans. Amer. Math. Soc.* **137** (1969), 327–344.
2. P. M. Cohn, Factorization in noncommuting power series rings, *Proc. Cambridge Philos. Soc.* **58** (1962), 452–464.
3. P. M. Cohn, Morita equivalence and duality, Queen Mary College Mathematics Notes. (Out of print.)
4. P. M. Cohn, Subalgebras of free associative algebras, *Proc. London Math. Soc.* **14** (1964), 618–632.
5. P. M. Cohn, "Universal Algebra," Harper and Row, New York, 1965.
6. P. Freyd, Algebra valued functors in general and tensor products in particular, *Colloq. Math.* **14** (1966), 89–106.
7. J. R. Isbell, Subobjects, adequacy, completeness, and categories of algebras, *Rozprawy Matematyczne* **36** (1964), 33 pp.
8. B. Mitchell, "Theory of Categories," Academic Press, New York, 1965.
9. D. Mumford, "Lectures on Curves on an Algebraic Surface" (with a section by G. M. Bergman), Princeton Annals of Mathematics Studies, No. 59, Princeton University, Princeton, NJ, 1966.
10. G. M. Bergman, Groups acting on hereditary rings, *Proc. London Math. Soc.* (3) **23** (1971), 70–82. (Erratum to Theorem 4.2 at (3) **24** (1972), 192.)
11. G. M. Bergman, Co-abelian-groups and co-rings in the category of associative algebras, in preparation.

12. G. M. Bergman and P. M. Cohn, Symmetric elements in free powers of rings, *J. London Math. Soc.* **1** (1969), 525–534.
13. P. M. Cohn, "Free rings and their relations," Academic Press, New York, 1972.
14. F. W. Lawvere, Functional semantics and algebraic theories, *Proc. Nat. Acad. Sci. USA* **50** (1963), 869–872.
15. S. MacLane, "Categories for the working mathematician," Springer Graduate Texts in Mathematics, No. 5, 1972.
16. B. Pareigis, "Categories and Functors," Academic Press, New York, 1970.
17. H. Bass, "Algebraic K-theory," Benjamin, New York, 1968.