JOURNAL OF ALGEBRA 15, 81–88 (1970)

Residual Finiteness and the Hopf Property in Rings

MORRIS ORZECH AND LUIS RIBES

Department of Mathematics, Queen's University, Kingston, Ontario

Communicated by I. N. Herstein

Received May 13, 1969

1. INTRODUCTION

An associative ring (respectively, a group) is said to be *residually finite* if for each nonzero (respectively, nonidentity) element x there is a two-sided ideal (respectively, normal subgroup) not containing x and such that the residue class ring (respectively, group) is finite. Residually finite groups and rings seem to have analogous properties. For example, it is known that free groups are residually finite ([5], p. 414) and correspondingly, that free rings are residually finite. (This result, communicated to us by J. Lewin, appears to be unpublished, and we have included a proof of it in Section 3.) In Section 2 we prove that if A is a suitable ring (e.g., $\mathbb{Z}$), then a finitely generated A-algebra is residually finite; the corresponding fact for groups is a consequence of the Fundamental Theorem for Abelian groups.

In Section 4 we prove a sharpened version of J. Lewin's theorem that a finitely generated residually finite ring is Hopfian (i.e., it admits no proper onto endomorphisms). It is shown that a finitely generated commutative A-algebra is Hopfian with respect to A-algebra maps, and using a similar technique, a new proof is constructed for a theorem of Vasconcelos.

In Section 5 some criteria are noted which imply that a group algebra is Hopfian or co-Hopfian.

2. A-ALGEBRAS

Unless specified, rings need not have a unity element 1. We first discuss the fact that for questions of residual finiteness, requiring the existence of 1 is not a serious restriction.

Let A and R be rings, possibly without 1. If R is an A-module, and $a(rs) = (ar)s = r(as)$ for all a in A and r, s in R, we will say that R is an A-algebra. R will be said to be *A-residually finite* if for each nonzero element r of R, there is a two-sided ideal I of R not containing r, and such that I is an A-submodule of R having finite index in R.

We note the following sharpened version of a result of J. Lewin ([4], Lemma 1), correcting a minor error in the estimate given there.

LEMMA 1. *Let A and R be rings, and let R be an A-algebra. Let S be a sub-A-algebra of R of finite index in R (as a subgroup of the additive group of R). Then there exists an A-submodule I in S, with I an ideal in R and of finite index in R. In fact, if the index of S in R is m, then I may be chosen having index less than or equal to mk, where k is $(m + 1)^q$, $q = (m + 1)^2$.*

Proof. In [4] it is shown that if the requirement that I be an A-module is removed, then there is indeed an ideal I' of R contained in S and of stipulated index. Then $I' + AI'$ may be chosen to be the required ideal I.

Taking A to be $\mathbb{Z}$ in the proposition below, we see that a residually finite ring may be embedded in a residually finite ring having a unit.

PROPOSITION 1. *Let A be a commutative ring with 1 which is residually finite. Let R be a unitary A-algebra, possibly without 1. Then R is A-residually finite if, and only if, R can be embedded as a sub-A-algebra of a unitary A-algebra, T, with 1, which is A-residually finite. Specifically, T may be chosen to be the A-module $R \times A$.*

Proof. Suppose R is A-residually finite and let $T = R \times A$. The multiplication in T is given by the familiar formula $(r, \mathbf{a})(r', \mathbf{a}') = (rr' + \mathbf{a}'r + \mathbf{a}r', \mathbf{aa}')$. The unit of T is $(0, 1)$; R is embedded in T as $R \times 0$ and A is embedded in T as $0 \times A$. Let $(r, \mathbf{a})$ be a nonzero element of T. If $\mathbf{a}$ is not zero, there is an ideal J in A such that J is of finite index in A and such that $\mathbf{a}$ is not in J. $R \times J$ is then an ideal of T which is an A-submodule and does not contain $(r, \mathbf{a})$, and is of finite index in T. If, on the other hand, the given element of T is $(r, 0)$, then by hypothesis there is an A-submodule S of R which is also an ideal of R not containing r, and is of finite index in R. Then $S \times A$ is a subring of T which does not contain $(r, 0)$, which is an A-submodule of T, and which has finite index in T. By Lemma 1, $S \times A$ may be replaced by an ideal of T and, thus, T is A-residually finite.

The converse statement is an immediate consequence of the following trivial lemma, which we state for future reference.

LEMMA 2. *Let A and R be rings with R an A-algebra. If R is A-residually finite, so is any A-subalgebra of R. In particular, any subring of a residually finite ring is residually finite.*

DEFINITION. Let A be a commutative ring with 1. A is said to be *m-finite* if every maximal ideal M of A is of finite index in A, i.e., A/M is a finite field.

It is an immediate consequence of the definition that if A is m-finite, so is every residue class ring A/I.

DEFINITION. A commutative ring A with 1 will be called a *Hilbert ring* if every prime ideal of A is an intersection of maximal ideals.

PROPOSITION 2. *If A is m-finite and a Hilbert ring, then the polynomial ring $A[X]$ is m-finite and a Hilbert ring.*

Proof. That $A[X]$ is a Hilbert ring if A is a Hilbert ring is proved in [1]. It is also shown there that if M is a maximal ideal of $A[X]$, then $M' = M \cap A$ is a maximal ideal of A. Then A/M' is a finite field, and $A[X]/M$ is a field extension of A/M'. But $A[X]$ is not a field, so the image of X in $A[X]/M$ satisfies any polynomial in M; so $A[X]/M$ is a simple algebraic extension of a finite field, and is thus finite.

Let $A[X_1, ..., X_n]$ denote the polynomial ring over A in the (commuting) variables $X_1, ..., X_n$. By an induction argument and use of the remark above, we draw the following conclusion.

COROLLARY. *If A is m-finite and a Hilbert ring, so is $A[X_1, ..., X_n]/I$ for any ideal I of the polynomial ring.*

LEMMA 3. *Let A be a Noetherian commutative ring with* 1, *and let* $\mathbf{a}$ *be a nonzero element of A. Then there is a maximal ideal M of A and an integer n such that* $\mathbf{a}$ *is not in M^n.*

Proof. Let M be a maximal ideal containing the annihilator of $\mathbf{a}$. Let A' denote the localization of A at M, and let M' denote the maximal ideal of A'. Since A is Noetherian, so is A' ([8], Corollary 1, p. 224), so that the intersection of the ideals M'^n is 0 ([8], Corollary 2, p. 217). Thus, if $\mathbf{a}$ is in M^n for all n, $\mathbf{a}/1$ is 0 in A', so that $\mathbf{a}$ is annihilated by an element not in M, a contradiction.

THEOREM 1. *Let A be a commutative ring with* 1 *which is m-finite, Noetherian, and Hilbert. Suppose that R is a commutative A-algebra, possibly without* 1, *which is finitely generated as an A-algebra. Then R is A-residually finite. In particular, any finitely generated commutative ring is residually finite.*

Proof. Since R is a finitely generated A-algebra, so is $R \times A$ when given the ring structure defined in the proof of Proposition 1. By this proposition, we may then assume that $R = A[X_1, ..., X_n]/I$ for some ideal I of the polynomial ring in n variables over A. Let r be a nonzero element of R. By Lemma 3 there is a maximal ideal M of R and an integer n such that r is not in M^n. Now, R is m-finite by the corollary to Proposition 2, so R/M is a finite field. Because R is Noetherian, each quotient M^i/M^{i+1} is a finite dimensional, and therefore finite, vector space over R/M. So M^n is of finite index in R.

3. Free Algebras and Group Algebras

We first state a result which is basic to the proof of Theorem 3 below (as communicated by J. Lewin).

THEOREM 2. *Let A be a residually finite ring, and let G be a residually finite group. Then the group algebra AG is A-residually finite.*

Proof. Let $x = a_1 g_1 + \cdots + a_n g_n$ be a nonzero element of AG, with the g_i's distinct elements of G and the a_i's nonzero elements of A. Choose a normal subgroup H in G of finite index, and such that if $g_i^{-1} g_j$ is not e (the identity of G), then it is not in H, for i, j running from 1 to n. (H may be G if $n = 1$ and $g_1 = e$). Choose an ideal I of A with $a_1, \ldots, a_n$ not in I and $A' = A/I$ a finite ring. Since the g_i's have distinct images in G/H, the image of x in $A'(G/H)$ is nonzero; the latter ring is a finite A-algebra, and this completes the proof.

Let S be any set, and let F denote the free group on S. It is well-known that F is residually finite ([5], p. 414). For A an arbitrary ring, let $A[(S)]$ denote the free polynomial algebra over A with the elements of S as non-commuting indeterminates. (We may wish to consider only polynomials of degree greater than 0, or all polynomials; the conclusion below is clearly unaffected by the interpretation.) Now, $A[(S)]$ is an A-subalgebra of the group algebra AF, so from Lemma 2 and Theorem 2 we conclude that the following result holds.

THEOREM 3. *Let A be a residually finite ring, and let S be any set. Then the free A-algebra on S is A-residually finite.*

Let A be a commutative residually finite ring with 1. In view of Theorem 2, and of the fact that if G and H are residually finite groups so is their direct product $G \times H$, it follows that for G and H residually finite groups, $AG \otimes_A AH = A(G \times H)$ is A-residually finite. We then pose the following question: If R and S are A-residually finite, is $R \otimes_A S$ also A-residually finite?

4. The Hopf Property

Let C be a concrete category, i.e., the objects of C are sets and each morphism in C is a set map. An object X of C will be called *C-Hopfian* if every endomorphism of X *onto* itself is an isomorphism. As pointed out in ([4], Theorem 3), a finitely generated residually finite ring is ring-Hopfian. A somewhat sharper version of this result is proved in Theorem 4. First, we isolate a result which is used later several times.

LEMMA 3. *Let A be a ring and let R be an A-algebra generated by $x_1, \dots, x_n$. Suppose f is an A-algebra endomorphism of R, and let r be an element of R. Then there exists a finitely generated subring A' of A such that if R' is the A'-subalgebra of R generated by $x_1, \dots, x_n$, then* (i) *r is in R'*; (ii) *f maps R' into R'*; (iii) *if f is an onto map, f maps R' onto R'. Moreover, R' is a finitely generated ring.*

Proof. For each $i = 1, 2, \dots, n$ choose z_i in R as follows: if x_i is in the image of f, $f(z_i) = x_i$; if not, $z_i = 0$. Each of the elements $f(x_1), \dots, f(x_n)$, r, $z_1, \dots, z_n$ can be expressed as a polynomial in the elements $x_1, \dots, x_n$, with coefficients in A. Let A' be the subring of A generated by the finite set of coefficients that arise in this way. It is clear that this A' satisfies all the required conditions. R' is a finitely generated ring, since it is finitely generated as an algebra over a finitely generated ring.

THEOREM 4. *Let A be a ring, and let R be a residually finite ring which is a finitely generated A-algebra. Then R is A-algebra-Hopfian.*

Proof. Let $f : R \to R$ be an onto A-algebra map, and let r in R be in the kernel of f. Choose A' and R' as in Lemma 3. Then R' is a finitely generated (as a ring) sub-ring of R. By Lemma 2, R' is residually finite. So by the result from [4] quoted above, R' is ring-Hopfian. Thus, since f maps R' onto R', and r is in R', r must be zero.

THEOREM 5. *Let A be a commutative ring, and let $R = A[(X_1, \dots, X_n)]$ be the free A-algebra of polynomials in n noncommuting indeterminates. Then R is A-algebra-Hopfian.*

Proof. Let $f : R \to R$ be an onto A-algebra map, and let r in R be in the kernel of f. Let A' be as in Lemma 3. Then $R' = A'[(X_1, \dots, X_n)]$, and r is in R'. By Theorem 1, A' is residually finite; so, by Theorem 3, R' is A'-residually finite. In particular, R' is a residually finite ring. Hence, since R' is finitely generated it is ring-Hopfian. Since $f(R') = R'$, we must have $r = 0$.

THEOREM 6. *Let A be a commutative ring with* 1, *and let R be a finitely generated commutative A-algebra. Then R is A-algebra-Hopfian.*

Proof. Let $f : R \to R$ be an onto A-algebra map, and let r be in R with

$f(r) = 0$. Let A' and R' be as in Lemma 3. Since R' is a finitely generated commutative ring, it is residually finite by Theorem 1 and, hence, ring-Hopfian. Since $f(R') = R'$, we have that $r = 0$.

We note that if R has a unit, then a proof can be given without using residual finiteness. For the Hilbert Basis Theorem implies that A' is Noetherian and, thus, R' is Noetherian as well. Thus, if f' denotes the restriction of f to R', there is an integer n such that $\ker(f'^n) = \ker(f'^{n+1})$. Now, $r = f'^n(y)$ for some y in R', and $f(r) = 0$ implies that $r = 0$.

The type of argument used above may be applied to proving the following result due to Vasconcelos ([6], Proposition 1.1).

PROPOSITION 3. *Let R be a commutative ring, and let M be a finitely generated R-module. If f is an R-module homomorphism of M onto M, then f is an isomorphism.*

Proof. Let $x_1, ..., x_n$ generate M as an R-module, and suppose that $f(y) = 0$. Let z_i be such that $f(z_i) = x_i$ for $i = 1, ..., n$ and let $f(z) = y$. Let S be the finite set of elements of R which arise as coefficients when z_i, $z, y, f(x_i)$ are expressed as R-linear combinations of $x_1, ..., x_n$ for $i = 1, ..., n$. Let $R' = \mathbb{Z}[S]$, the subring of R of all polynomials in the elements of S with integer coefficients. Let M' be the R'-submodule of M generated by $x_1, ..., x_n$. Then f restricts to an R'-homomorphism f' from M' onto M'. Since R' is Noetherian, so is M' and, thus, for some integer n $\ker(f'^n) = \ker(f'^{n+1})$. This implies that $\ker(f') = 0$ and, thus, $y = 0$ since y is in M'.

5. THE HOPF PROPERTY FOR GROUP ALGEBRAS

It is clear that if a group G is not Hopfian, then the group algebra AG is not A-algebra-Hopfian. In a recent correspondence, W. L. May has pointed out that one can construct an infinite Abelian group G which is Hopfian, but such that the group algebra CG over the complex numbers is not C-algebra-Hopfian. We treat only special cases of the question as to when AG is A-algebra-Hopfian, but we cannot even resolve the question as to whether $\mathbb{Z}G$ is a Hopfian ring when G is a Hopfian group. First, consider the case when G is Hopfian by virtue of being finitely generated and residually finite ([5], p. 415).

PROPOSITION 3. *Let A be a commutative ring, and let G be a finitely generated and residually finite group. Then $R = AG$ is A-algebra-Hopfian.*

Proof. Assume $f : R \to R$ is an onto homomorphism of A-algebras, and let r in R be such that $f(r) = 0$. Let A' be as in Lemma 3. Then $R' = A'G$.

By Theorems 1 and 2, R' is A'-residually finite and, therefore, residually finite as a ring. Hence, since R' is finitely generated, it is ring-Hopfian. Since f restricted to R' is onto, we have $r = 0$.

Following the terminology of [2], we shall say that a group G is locally indicable if every finitely generated subgroup of G admits a nontrivial homomorphism to the group of integers $\mathbb{Z}$. In [2] it is shown that if G is a locally indicable group, and A is a ring without any divisors of zero, then any unit of AG is of the form $\mathbf{a}g$, where $\mathbf{a}$ is a unit in A and g is an element of G. It is then easy to show the result below.

PROPOSITION 4. *Let G be a locally indicable and Hopfian group. Let A be a ring with* 1. *Then the group algebra AG is A-algebra-Hopfian in either of the cases*: (i) *A has no divisors of zero or* (ii) *A is commutative and has no nilpotent elements.*

Proof. Let f be an A-algebra homomorphism of AG onto AG. Suppose that A has no zero divisors. Then using the theorem of Higman quoted above, we have that for each g in $G, f(g) = a(g)f'(g)$, where $a(g)$ is a unit of A and $f'(g)$ is an element of G. The mapping f' determines a group homomorphism of G to G, and because f is A-linear and onto, it follows that f' is an epimorphism. Thus, f' is an isomorphism since G is Hopfian, and it is clear then that f must be an isomorphism as well.

If A is commutative, then for each prime ideal P of A we have that $(R/P)G$ is R/P-algebra-Hopfian. If an element $a_1g_1 + \cdots + a_ng_n$ of AG is in the kernel of an endomorphism of AG to itself, it follows that each a_i is in every prime ideal of R and is, therefore, nilpotent. This completes the proof.

Remark. It is clear that if AG has no units other than those of the form $\mathbf{a}g$, then AG is A-algebra-Hopfian.

We turn to one example of a co-Hopfian algebra, i.e., an algebra that admits no proper one-one endomorphisms.

PROPOSITION 6. *Let R be a commutative ring with* 1 *and let G be a finite abelian group of order n. Assume that n is a unit in R. Then RG is co-Hopfian as an R-algebra.*

Proof. It follows from [7], Theorem 1.1 that RG is a separable R-algebra, i.e., that RG is projective as an (RG, RG)-bimodule. If a separable R-algebra T has no proper idempotents and is a projective R-module of finite type, then it admits only finitely many R-algebra endomorphisms ([3], Lemma 1.3). A homomorphic image of a separable R-algebra is separable, so by decomposing RG into a finite direct sum of R-algebras each without proper idempotents, we can show that RG admits only a finite set of R-algebra endomorphisms. It follows at once that such an endomorphism is one-one if, and only if, it is onto.

Remark. The proof above can be used to show that for a cocycle f in the group cohomology group H^2 (G, Units (R)), the crossed product RG_f is co-Hopfian.

Note added in proof. We have recently become aware of a result of Trevor Evans (*J. London Math. Soc.* (2), 1 (1969), 399–403) which together with Theorem 1 implies that the word problem is solvable for finitely generated commutative rings.

Acknowledgment

We thank I. Hughes for helpful conversations.

References

1. O. Goldman, Hilbert rings and the Hilbert Nullstellensatz. *Math. Z.* **54** (1951), 136–140.
2. G. Higman, The units of group-rings. *Proc. London Math. Soc.* **46** (1940), 231–248.
3. G. J. Janusz, Separable algebras over commutative rings. *Trans. Amer. Math. Soc.* **122** (1966), 461–479.
4. J. Lewin, Subrings of finite index in finitely generated rings. *J. of Algebra* **5** (1967) 84–88.
5. W. Magnus, A. Karrass, and D. Solitar, Combinatorial group theory. Interscience (John Wiley), New York, 1966.
6. W. V. Vasconcelos, On local and stable cancellation. *An. da Acad. Brasileira de, Ciências* **37** (1965), 389–393.
7. S. Williamson, Crossed products and hereditary orders. *Nagoya Math. J.* **23** (1963), 103–120.
8. O. Zarisky and P. Samuel, Commutative algebra. Van Nostrand, New York, 1958.