Journal of Pure and Applied Algebra 8 (1976) 97–104

ON FINITELY ACCESSIBLE AND FINITELY OBSERVABLE RINGS

Eduardo D. SONTAG*
Center for Mathematical System Theory, Department of Mathematics, Univ. of Florida, Gainesville, Fla. 32611, U.S.A.

Communicated by S. Eilenberg
Received 4 August 1975

Two classes of rings which occur in linear system theory are introduced and compared. Characterizations of one of them are given in terms of integral extensions and a Cayley–Hamilton type matrix condition.

Introduction

Two classes of rings (not necessarily commutative) which appear naturally in generalizing the theory of linear dynamical systems are studied in this paper. For motivation the reader is referred to Sontag [4]. The exposition is mathematically self-contained.

From a system-theoretic standpoint the interesting questions concern algebraic properties of the first family ("FA" rings, for which all the usual properties of the commutative case extend), and especially its relation with the second family ("FO" rings) and the left–right analog of the latter (related to questions of duality).

The problems mentioned above are approached by first characterizing FA rings by a Cayley–Hamilton type condition and by conditions involving integral extensions. A comparison is made in the case of no zero-divisors with Ore domains. The relation between both classes is given by Theorem 3.2 and the counterexample in section 4. The treatment is elementary throughout; in particular, in section 3 a matrix-theoretical approach is used where more general functors $\mathrm{Hom}_R(.,M)$ than $M = R$ would perhaps be also suitable.

1. Finitely accessible rings

All rings will be associative with identity, homomorphisms preserving the latter. Unless otherwise stated, "module" will stand for (unitary) left module, and in general all one-sided notions will be left-notions, the right analogues having the corre-

* This research was supported in part by US Army Research Grant DA-ARO-D-31-124-72-G114 through the Center for Mathematical System Theory, University of Florida, Gainesville, Fla. 32611, U.S.A.

sponding prefix. Maps are written on the right for (left) modules and on the left for right modules.

The following notations are used:

${}^nR$, free (left) module on n generators (row vectors);

R^n, right module of column vectors;

R_n, $n \times n$ matrix ring.

No distinction is made between End $({}^nR)$ and R_n, expressing maps in the standard basis $\{e_i\}$. If R is a subring of the ring S, then S is *finite* over R when it is finitely generated as an R-module.

We single out two definitions of integral extensions of the many possible generalizations of the commutative case; many others are known.

1.1. Definition. Let S be a ring and R a subring of S. An element y of S is called (left) *integral* over R provided it satisfies an equation $y^n + a_{n-1}y^{n-1} + ... + a_0 = 0$ with $a_0, ..., a_{n-1}$ in R. If every element of S is integral over R, we say that S is (left) *integral* over R.

1.2. Definition. Let R, S be as above. An element y of S is called (left) *A-integral* provided that there exist $c_1, ..., c_n$, where each c_i commutes with all elements of R, such that $M = Rc_1 + ... + Rc_n$ contains an element which is not a zero divisor and satisfies $My \subseteq M$. S is *A-integral* over R if every element of S is.

An even more restrictive definition is sometimes necessary [1], where also $1 \in M$ is required; this could be substituted for Definition 1.2 in what follows without changing any statements.

1.3. Theorem. *Let R be a ring. The following are equivalent:*

(a) *Every finite extension of R is integral.*

(b) *For every n and any T in* R_n, *there exist an integer k and* $a_0, ..., a_{k-1}$ *in R with*

$$T^k = \sum_{i=0}^{k-1} a_i T^i.$$

(c) *For any n, let* $M = {}^nR$ *and* $g = e_1$. *Then, for all F in* End (M), *there exist an integer k and* $a_0, ..., a_{k-1}$ *in R such that*

$$gF^k = \sum_{i=0}^{k-1} a_i gF^i .$$

(d) *The same conclusion as in* (c) *holds for any finitely generated R-module M and every g in M.*

(e) *Let M be a finitely generated R-module and* $g_1, ..., g_m$ *elements of M. For any F in* End (M) *there exist an integer k and* $a_0, ..., a_{k-1}$ *in R such that* $g_jF^k = \sum_{i<k} a_i g_j F^i$ *for all* $j = 1, ..., m$.

(f) *For every pair of finitely generated projective modules M, N, for all F in* End (M) *and all G in* Hom (N, M) *there exists an integer k with*

$$\sum_{i=0}^{k} \operatorname{Im} GF^i = \sum_{i=0}^{k+1} \operatorname{Im} GF^i .$$

(g) *Every A-integral extension of R is integral over R.*

Proof. We shall prove (a) ⇒ (b) ⇒ (c) ⇒ (d) ⇒ (a), (d) ⇒ (e) ⇒ (g) ⇒ (b), and (e) ⇒ (f) ⇒ (c).

(a) ⇒ (b). Immediate from the fact that R_n is a finite extension of R, when every r in R is identified with the corresponding diagonal matrix.

(b) ⇒ (c). Obvious because e_1 commutes with every element of R.

(c) ⇒ (d). Assume that M is finitely generated. Then, for some n, there exists a surjective R-module homomorphism φ: ${}^nR \to M$ such that $e_1\varphi = g$. Define $\hat{F}$: ${}^nR \to {}^nR$ such that $\varphi F = \hat{F}\varphi$. An equation for $(\hat{F}, e_1)$ is mapped by φ into the corresponding equation for (F, g).

(d) ⇒ (a). Assume that S is a finite extension of R. For y in S, consider the R-endomorphism F of S given by $s \mapsto sy$, and apply (d) with $g = 1$.

(d) ⇒ (e). Consider R^n as a bimodule. Then $\hat{M} := R^n \otimes_R M$ is a finitely generated R-module. Define

$$g := \sum_{i=1}^{n} e_i \otimes g_i$$

in $\hat{M}$, and $\hat{F} := 1_{R^m} \otimes F$ in End $(\hat{M})$. An equation for $(\hat{F}, g)$ gives a common equation for all (F, g_i).

(e) ⇒ (g). Assume that R, S, M and y are as in (1.2), and $m = \Sigma l_j c_j$ is not a zero divisor, with all l_j in R. Consider the endomorphism $z \mapsto zy$ of M. It follows from (e) that there exist $a_0, \ldots, a_n = 1$ in R with $\Sigma_i a_i c_j y^i = 0$ for all j. By hypothesis, $a_i c_j = c_j a_i$ for all i, j. Denote by t the element $\Sigma a_i y^i$. Then,

$$mt = \Big(\sum_{j=1}^{k} l_j c_j\Big)\Big(\sum_{i=1}^{n} a_i y^i\Big) = \sum_{j=1}^{k} l_j\Big(\sum_{i=1}^{n} a_i c_j y^i\Big) = 0 .$$

Since m is not a zero divisor, it follows that $t = 0$. Hence y is integral.

(g) ⇒ (b). Define $M := R_n$. Observe that $M = \Sigma_{i,j} RE_{ij}$ where E_{ij} is the matrix having as its only non-zero entry the identity in the (i, j)th position. It follows that R_n is an A-integral extension of R, so by (g) it is integral.

(e) ⇒ (f). Assume that $g_1, \ldots, g_m$ generate the image of G. It follows that there exists a k such that the finite set of all $g_j F^i$ with $i < k$ generates $\Sigma_{i \geqslant 0} \operatorname{Im} GF^i$.

(f) ⇒ (c). Trivial. □

1.4. Definition. A ring satisfying the conditions in Theorem 1.3 is called a *finitely accessible* ring, or simply an FA ring.

The terminology is motivated from condition (f), which appears naturally in system theory. It is clear from (f) that the concept is Morita invariant, i.e. it holds simultaneously for rings with equivalent categories of (left) modules. It is also obvious that all left Noetherian and all commutative rings are FA rings. Using methods of automata theory, this class of rings can be also characterized as those whose polynomial rings admit a localization by their respective multiplicative subsets of monic polynomials [4, Theorem 3.6].

We recall [2, p. 6] that a ring R is *weakly n-finite* iff ^nR is not isomorphic to a proper direct summand of itself or, equivalently, iff every surjective endomorphism of ^nR is an automorphism, or iff for A, B in R_n the relation $AB = I$ implies $BA = I$. R is *weakly finite* iff it is weakly n-finite for every n. It is not difficult to prove, using condition (f), that every FA ring is weakly finite. This necessary condition is not very sharp, but is enough to provide many counterexamples.

2. A comparison with the Ore condition

Recall that a (left) *Ore domain* is an integral domain in which any two non-zero elements a, b satisfy $Ra \cap Rb \neq 0$.

The statement (1.3a) provides an interesting connection with Ore domains. We first prove:

2.1. Proposition. *Assume R has no zero divisors. Then R is a (left) Ore domain iff for each integer n, each T in R_n, and g in ^nR, there exist an integer m and $a_0, \ldots, a_m$ in R, $a_m \neq 0$, with $\Sigma a_i g T^i = 0$.*

Proof. Suppose a, b are nonzero elements of R. If the property is true for $n = 1$, $g = a$, $T = b$, then there are $a_0, \ldots, a_m$ with $\Sigma a_i a b^i = 0$. If $a_k \neq 0$, $k < m$ smallest such, cancelling b^k the relation becomes

$$\left(-\sum_{i=k}^{m-1} a_{i+1} a b^{i-k}\right) b = a_k a ,$$

so $Ra \cap Rb \neq 0$.

Conversely, if K is the field of left fractions of R, ^nK has finite length as a K-module. Given g and T, over K we have a relation $gT^n = \Sigma_{i<n} k_i g T^i$, where each $k_i = b_i^{-1} a_i$ with a_i, b_i in R. We may assume all b_i are equal [2, Exercise 0.5.2], say to b, so

$$bgT^n = \Sigma a_i g T^i ,$$

and there is a dependence in R, in fact with $m = n$. □

By a proof similar to that of Theorem 1.3 and defining (left) algebraic extensions in the corresponding way, one has:

2.2. Proposition. *Suppose R has no zero divisors. Then R is an Ore domain iff every finite extension of R is algebraic.* □

Given a ring R and α a ring endomorphism of R, denote by $R[z;\alpha]$ the *skew polynomial ring* consisting of all finite sums $\Sigma a_i z^i$ with a_i in R, coefficientwise addition and equality, and product given by the distributive extension of $z \cdot a := (a\alpha)z$. The *right* skew polynomial ring is defined similarly. If α is an automorphism both concepts coincide. If R is an integral domain and α is injective, the degree satisfies all usual properties and $R[z;\alpha]$ is also a domain; if, further, R is a (left) Ore domain, $R[z;\alpha]$ is also an Ore ring [2, p. 36].

Consider now an arbitrary commutative integral domain D and $A := D[\{x_i, i \in \mathbf{Z}\}]$. Let α be the ring automorphism of A which sends x_i to x_{i+1} for all i. Then $R := A[z;\alpha]$ is both a left and right Ore domain. We claim that it is not FA. Assume on the contrary that there are $y_0, \ldots, y_{n-1}$ in R with $x_0 z^n = \Sigma y_i x_0 z^i$. Each y_i is a polynomial $y_i = \ldots + a_i z^{n-i} + \ldots$ with a_i in A for all i, and the dots standing for the terms in z^k, $k \neq n-i$. So we have

$$x_0 z^n = \sum_{i=0}^{n-1} (\ldots + a_i z^{n-i} + \ldots) x_0 z^i = \ldots + \sum_{i=0}^{n-1} a_i (x_0 \alpha^{n-i}) z^n + \ldots .$$

Equating coefficients in z^n we have

$$x_0 = \sum_{i=0}^{n-1} a_i (x_0 \alpha^{n-i}) = \sum_{i=0}^{n-1} a_i x_{n-i} .$$

We get a contradiction, proving the claim. We have then proved somewhat more than:

2.3. Proposition. *The class of FA rings with no zero divisors is properly included in the class of (left) Ore domains.*

Since every Ore domain is weakly finite, the same example also proves that not every weakly finite ring is an FA ring.

3. Finitely observable rings and relations between both classes

The following notion is in a sense dual to that of FA rings, when the latter are characterized using (1.3f).

3.1. Definition. R is a *finitely observable* ring, or simply an FO ring, provided that for any pair of finitely generated projective modules M, N and for all $F \in \operatorname{End}(M)$,

$H \in \mathrm{Hom}\,(M, N)$, there exists an integer k with

$$\bigcap_{i=0}^{k} \ker F^i H = \bigcap_{i=0}^{k-1} \ker F^i H .$$

The terminology is again motivated by system theory, where the notion of observability is dual to that of accessibility. It is then of interest to investigate whether any of the properties implies the other, either for the same ring or for its opposite. The positive implications are given by the following result.

3.2. Theorem. *Let R be an FA ring. Then R^{op} is an FO ring. If, moreover, R has no zero divisors, then R is an FO ring.*

Proof. We first remark that it is enough to check definition 3.1 for a free module of finite rank M and $N = R$; the equivalence with 3.1 follows easily once that N is embedded in some ${}^nR$ and a free presentation is chosen for M.

Assume given T in R_n and h in R. Since R is an FA ring, it follows from (1.3d) (with the transposed matrices $g := h'$, $F := T'$) that there exist an integer k and $a_0, \ldots, a_{k-1}$ in R such that

$$h'(T')^k = \sum_{i=0}^{k-1} a_i h'(T')^i .$$

It follows that

$$\bigcap_{i=0}^{k-1} \ker T^i h = \bigcap_{i=0}^{k} \ker T^i h ,$$

where the powers of T and the products are now taken over the opposite ring. Hence R^{op} is an FO ring, by the above remarks.

If R is also an integral domain, it follows from Proposition 2.3 that it is a (left) Ore ring. Therefore it is embeddable in a division ring, and the latter is obviously an FO ring. Hence the last part of the theorem will be proved once that the FO property is shown to be hereditary. Indeed, assume that R is a subring of the ring S, T is in R_n, and h is in R. The same matrices induce morphisms T_S, h_S of the S-modules ${}^nS$, S. For all i, $\ker T^i h = (\ker T_S^i h_S) \cap {}^nR$. Using again the remark at the beginning of the proof, R is an FO ring whenever S is. □

It is again not difficult to prove that all FO rings are weakly finite, hence counterexamples are easily available. However, the class is still very broad, due to the fact that it is hereditary. For instance, the free associative ring on two generators, $R := \mathbf{Z}\langle x_1, x_2\rangle$, is not an Ore domain, hence by Proposition 2.3 it cannot be an FA ring. But being embeddable in a division ring, both R and R^{op} are FO rings. Therefore, the statements

R is FO *implies R is* FA

R is FO *implies* R^{op} *is* FA

are both false, even in the case of rings with no zero divisors.

4. A counterexample

We have proved in Theorem 3.2 that for domains the FA condition is weaker than the FO condition. We now produce a counterexample to the corresponding statement for arbitrary rings. The same construction serves to give negative answers to many other questions.

Let S be an arbitrary but fixed (left) Noetherian domain. Consider the ring C of all infinite matrices (a_{ij}) with rows and columns indexed by $\mathbf{N}$ and such that each column has only a finite number of nonzero entries. Denote by A the subset of matrices with finitely many nonzero entries. For each n, let $A_n \subseteq A$ consist of those matrices satisfying also $a_{ij} = 0$ for $j > n$. Denote by b the matrix given by $a_{ij} = 1$ iff $i = j + 1$ and 0 otherwise. Denote by s_j the matrix whose only nonzero entry is $a_{1j} = 1$.

Identify $s \in S$ with $s \cdot I$, thereby including S in C. Denote by D the smallest subring of C containing S and b. All elements of S commute with b. Therefore $D \simeq S[X]$ and D is Noetherian. In particular, D is an FA ring; being embeddable in a field, D is also an FO ring. Let B_n be $A_n + D$ (the set of all sums), and $B := A + D = (\bigcup A_n) + D = \bigcup(A_n + D) = \bigcup B_n$.

Observe now that A_n is a left ideal in C and that $A_n b \subseteq A_{n-1} \subseteq A_n$. So $A_n D \subseteq A_n$. Hence if $a_i + d_i \in B_n$, $i = 1, 2$, with $a_i \in A_n$, $d_i \in D$, their product $(a_1 a_2 + d_1 a_2 + a_1 d_2) + d_1 d_2 \in B_n$. Each B_n is then a subring of C. The union being directed, B is also a subring. Since $b^i s_j$ is the matrix whose only nonzero entry is 1 in the $(i+1, j)$th position, it follows that A_n is the D-submodule of C generated by $s_1, \ldots, s_n$. So B_n is generated as a D-module by $I, s_1, \ldots, s_n$. It is easy to check that these generators are in fact left linearly independent. So B_n is a finite extension of D, freely generated as a D-module.

The class of FA rings is easily shown to be closed under finite extensions. The class of FO rings, on the other hand, is closed under extensions $R \subseteq S$ where the overring S is *free* as an R-module. We conclude that each B_n is both an FA and an FO ring.

The class of FA rings is also closed under direct limits (this can be proved easily from (1.3b)). Since $B = \varinjlim B_n$, it follows that *B is an FA ring.*

Now consider B as a left B-module and b, s_1 as endomorphisms (by right translation). Observe that $s_n b^i = s_{n-i}$ if $0 \leq i < n$ and 0 otherwise. Observe that $s_1^2 = s_1$, $s_j s_1 = 0$ for $j \neq 1$. We have then $s_n b^i s_1 = s_1$ if $i = n - 1$ and 0 otherwise. Define

$F := b$, $H := s_1$. Then s_n is in ker F^iH for $i = 0, \ldots, n-2$ but not in ker $F^{n-1}H$. Hence *B is not an FO ring.* Therefore the two classes are not comparable.

Along with Theorem 3.2, this proves that neither the FA nor the FO conditions are left–right symmetric. In the case of FA rings, a much stronger statement holds: there exists a ring R which is a right Euclidean ring and which is not an FA ring. Indeed, define $R := S[z; \alpha]$, where S is $k(x)$, k a commutative field, and $\alpha: x \mapsto x^2$.

Both classes are closed under finite products, but $R := B^{\omega}$, $g := (s_1, s_2, s_3, \ldots)$ and $T := (b, b, b, \ldots)$ show that the class of FA rings is not closed under countable products. A similar counterexample holds for FO rings, when $R := \Pi\{B_i, i \in \mathbf{N}\}$, T as before and $h := (s_1, s_1, s_1, \ldots)$.

Now let D be an arbitrary nonprincipal ultrafilter over $\mathbf{N}$, R_1 the corresponding ultrapower of B and R_2 the ultraproduct of the B_i, $i = 1, 2, \ldots$. A reasoning as above shows that R_1 is not an FA ring and R_2 is not an FO ring. This proves that neither of both classes defined in this paper is *axiomatic* [3, p. 256], i.e. they cannot be defined in first order logic.

References

[1] T.W. Atterton, Definitions of integral elements and quotient rings over noncommutative rings with identity, J. Austral. Math. Soc. 13 (1972) 433–466.

[2] P.M. Cohn, Free Rings and Their Relations (Academic Press, 1971).

[3] G. Grätzer, Universal Algebra (Van Nostrand, 1968).

[4] E. Sontag, On linear systems and noncommutative rings, Math. Syst. Theory 10 (1976) 327–344.