International Electronic Journal of Algebra
Volume 5 (2009) 121-134

ON THE MAXIMAL CARDINALITY OF CHAINS OF INTERMEDIATE RINGS

David E. Dobbs, Gabriel Picavet, Martine Picavet-L'Hermitte

Received: 12 August 2008; Revised: 3 December 2008
Communicated by Abdullah Harmancı

Abstract. All rings considered are commutative with 1 and all subrings are unital. If $R \subseteq T$ are rings such that T is a finitely generated R-module, R is not a total quotient ring and $(R : T) = 0$, then there exists a denumerable chain of R-subalgebras of T. The rings having only finite chains of subrings are shown to be the same as the recently classified rings having only finitely many subrings.

Mathematics Subject Classification (2000): 13B99, 13B21; Secondary 13A15, 13G05
Keywords: Commutative ring, ring extension, subalgebra, chain, cardinality, determinant, FIP property, FSP property, integrality, greatest common divisor, pullback, singly generated ring, integral domain, total quotient ring

1. Introduction

All rings considered below are commutative with $1 \neq 0$; all ring extensions, subrings and subalgebras are unital. For us, a *chain* will mean a collection of certain types of sets that are pairwise comparable with respect to inclusion. Consider a ring extension $R \subset T$. Our interest here is in the possible cardinality of chains of R-subalgebras of T, i.e., of rings lying between R and T. In case T is finitely generated as an R-module, Theorem 2.1 presents a sufficient condition for there to exist a denumerable chain of (pairwise distinct) R-subalgebras of T. In another vein, Sections 3 and 4 culminate with a pair of theorems whose effect is to characterize the rings R such that each chain of subrings of R is finite. We next comment on the pedigree of these results and the organization of Sections 2–4.

The main motivation for Section 2 is the following recent result of the first-named author [5, Theorem 2.1]: if $R \subset T$ are (commutative integral) domains with corresponding quotient fields $K \subset L$ and $R \neq K$, then there exists a denumerable chain of R-subalgebras of T. (As usual, $\subset$ denotes proper inclusion.) The above "denumerable" conclusion is best possible, as it was shown in [5, Remark 2.2 (a)]

that the maximal order of any quadratic algebraic number field has only denumerably many subrings. A partial generalization of [5, Theorem 2.1] to rings with nontrivial zero-divisors was given in [5, Proposition 2.3] and is addressed further in Remark 2.3 below. After a number of reductions, the proof of [5, Theorem 2.1] reduced to the case where $T = R[\alpha]$ for some element α integral over R and, thus, to a case where T was a certain type of finitely generated R-module. In this spirit, Theorem 2.1 shows that if $R \subseteq T$ are rings (not necessarily domains) such that T is a finitely generated R-module, R is not a total quotient ring and the conductor $(R : T) := \{t \in T \mid tT \subseteq R\}$ is 0, then there exists a denumerable chain of R-subalgebras of T. Corollary 2.2 gives a reformulation of Theorem 2.1 in which the hypothesis of a vanishing conductor is absent. Remark 2.3 shows that Theorem 2.1 (even when buttressed by Corollary 2.2) neither implies, nor is implied by, [5, Theorem 2.1] (even when buttressed by [5, Proposition 2.3]).

Given a ring extension $R \subseteq T$, one may consider the property that each chain of R-subalgebras of T is finite. This property was considered for certain domains (R and) T in [2] and was characterized in [11, Theorem 2.14] in case R is a domain with quotient field T. In Sections 3 and 4, we consider this property in case R is the prime (sub)ring of T (without requiring that these rings be domains). The following definitions will facilitate matters.

Let $A \subseteq B$ be a ring extension, and let R be a ring with prime subring F. As in [1], we say that the ring extension $A \subseteq B$ *has* FIP (for the "finitely many intermediate rings property") if there are only finitely many rings C such that $A \subseteq C \subseteq B$. As in [8], we say that R *has* FSP (for the "finitely many subrings property") if $F \subseteq R$ has FIP, i.e., if R has only finitely many (unital) subrings. By analogy, we next introduce two additional definitions. We say that $A \subseteq B$ *has* FCP (for the "finite chains property") if each chain of A-subalgebras of B is finite. Also, we say that R *has* FCP if $F \subseteq R$ has FCP, i.e., if each chain of (unital) subrings of R is finite. We trust that the above definitions will not lead to any ambiguity, as it should always be clear whether "FSP" is being considered for an extension of rings or for an individual ring.

It is clear that if a ring extension $A \subseteq B$ has FIP, then $A \subseteq B$ has FCP. Consequently, if a ring R has FSP, then R has FCP. The main result of Sections 3 and 4 is that the converse is true: see Theorems 4.8 and 4.9. This effectively determines the rings that have FCP, as the rings that have FSP have been determined earlier, by combining [8, Theorem 3.20] with [7, Theorem 3.12]. This combining of results was necessary, as the determination of the rings having FSP was first accomplished

in case R is a singly generated ring. The same pattern occurs in determining the rings with FSP in Section 4, with Theorem 4.8 handling the classification for singly generated rings and Theorem 4.9 reducing matters to the singly generated case. Just as the earlier study of FSP was able to proceed more generally with the aid of some FIP-theoretic results for extensions whose base rings need not be prime rings, our work that culminates with a classification of certain rings in Theorems 4.8 and 4.9 proceeds with the help of more general studies of the ring extensions that have FSP. For the sake of clarity, that work on ring extensions is isolated in Section 3.

2. A sufficient condition for an infinite chain of subalgebras

We begin with the following companion for [5, Theorem 2.1].

Theorem 2.1. *Let $R \subseteq T$ be a ring extension such that T is finitely generated as an R-module. Suppose also that some nonunit of R is a non-zero-divisor of R and that $(R : T) = 0$. Then there exists a denumerable chain of R-subalgebras of T.*

Proof. Let x be a nonunit of R which is a non-zero-divisor of R, and let $\{t_1, \ldots, t_n\}$ be a finite generating set of T as an R-module. Without loss of generality, $t_1 = 1$. For each positive integer k, set $E_k := R + x^k T$. Then $\mathcal{C} := \{E_k\}$ is a descending chain of R-subalgebras of T, i.e., of subrings of T that contain R. It is enough to prove that $\mathcal{C}$ does not terminate.

Suppose, on the contrary, that $E_p = E_{p+1}$ for some positive integer p. For each integer $i \geq 2$, we have $x^p t_i \in E_p = E_{p+1}$, so that $x^p t_i = a_i + \sum_{j=2}^{n} x^{p+1} a_{ij} t_j$, for some $a_i, a_{ij} \in R$. Then $t_2, \ldots, t_n$ are solutions of the following linear system (S) of $n-1$ equations in the $n-1$ unknowns y_j:

$$\sum_{j=2}^{n} (x^p \delta_{ij} - x^{p+1} a_{ij}) y_j = a_i, \quad i = 2, \ldots, n,$$

where δ_{ij} denotes the Kronecker delta.

Let D be the determinant of the coefficient matrix M of the linear system (S), and let D_j be the determinant of the matrix obtained by replacing the entries of the $(j-1)$th column of M with the corresponding entries from the right-hand sides of the equations in the system (S). Of course, $D, D_j \in R$ for all j. Now, by Cramer's Rule, $Dt_j = D_j \in R$ for each $j \geq 2$. But $Dt_1 = D \cdot 1 = D \in R$ as well. Thus, $DT = D \sum_{i=1}^{n} Rt_i \subseteq R$; i.e., $D \in (R : T) = 0$.

Let A be the $(n-1) \times (n-1)$ matrix obtained from the entries a_{ij} (where $i, j = 2, \ldots, n$). Let I denote the $(n-1) \times (n-1)$ identity matrix. By factoring x from each row of M and then expanding the determinant, we see that $D =$

$x^{p(n-1)} \det(I - xA)$. As the hypotheses ensure that $n > 1$ and we have seen that $D = 0$, the hypothesis that x is a non-zero-divisor in R implies that $\det(I - xA) = 0$. Note that $\det(I - xA) = 1 + xr$ for some $r \in R$, and so $1 + xr = 0$. As x is a nonunit of R, we have found the desired contradiction. □

Although the hypothesis in Theorem 2.1 that "some nonunit of R is a non-zero-divisor of R" is easy to use, it may be of interest to note that this hypothesis is equivalent to "R is not a total quotient ring".

We next give a reformulation/generalization of Theorem 2.1.

Corollary 2.2. *Let $R \subseteq T$ be a ring extension such that $T = S + (R : T)$ for some R-subalgebra S of T such that S is finitely generated as an R-module. Suppose also that some nonunit of $R/(R : T)$ is a non-zero-divisor of $R/(R : T)$. Then there exists a denumerable chain of R-subalgebras of T.*

Proof. Consider the ring extension $A := R/(R : T) \subseteq T/(R : T) =: B$. Since $(R : T) = (R : S)$, we have that $B = S/(R : S)$ is finitely generated as an A-module. Since $(A : B) = 0$, Theorem 2.1 yields a denumerable chain of A-subalgebras of B. The assertion then follows via a standard homomorphism theorem. □

The hypothesis in Corollary 2.2 that "$T = S + (R : T)$ for some R-subalgebra S of T such that S is finitely generated as an R-module" is easily seen to be equivalent to "$T/(R : T)$ is finitely generated as an $R/(R : T)$-module". In view of the pullback description of $R = T \times_{T/(R:T)} R/(R : T)$, the above argument involving "a standard homomorphism theorem" really establishes the following result. If $R \subseteq T$ are rings with a common ideal I, then the maximal cardinality of a chain of R-subalgebras of T is the same as the maximal cardinality of a chain of $R/(R : T)$-subalgebras of $T/(R : T)$. Similar reasoning has occurred earlier (cf. [6, Proposition II.4]) and will occur again (cf. Proposition 3.2).

Remark 2.3. (a) Although Corollary 2.2 followed easily from Theorem 2.1 by factoring out the conductor, it should be noted that Corollary 2.2 is stronger than Theorem 2.1. To see this, let X be an analytic indeterminate over the field $\mathbb{Q}(i)$ of Gaussian numbers. Note that it follows from Corollary 2.2 that if we take $R := \mathbb{Z} + X\mathbb{Q}(i)[[X]] \subset \mathbb{Z}[i] + X\mathbb{Q}(i)[[X]] =: T$, then there is a denumerable chain of R-algebras of T. Indeed, by the above comments, one need only verify that there is a denumerable chain of rings between $R/(R : T) \cong \mathbb{Z}$ and $T/(R : T) \cong \mathbb{Z}[i]$, and this, in turn, is a consequence of [5, Theorem 2.1]. However, this conclusion cannot be drawn from Theorem 2.1 since $(R : T) = X\mathbb{Q}(i)[[X]] \neq 0$.

(b) Let $R := \mathbb{Z}$ and take T to be the ring of algebraic integers. Then [5, Theorem 2.1] yields that there is a denumerable chain of R-algebras of T. However, this conclusion cannot be drawn from Theorem 2.1 (or from Corollary 2.2) since T is not a finitely generated R-module. For a non-integral example to which [5, Theorem 2.1] applies (but which, of course, cannot be inferred from Theorem 2.1 or Corollary 2.2), consider $R := \mathbb{Z} \subset \mathbb{Z}[i]_{(1-i)\mathbb{Z}[i]} =: T$.

(c) It is easy to see that if $R \subset T$ are domains to which Theorem 2.1 can be applied, then [5, Theorem 2.1] also applies to $R \subset T$. However, Theorem 2.1 *does* have applications which are not consequences of [5]. To fabricate an example (necessarily involving nontrivial zero-divisors), we first recall the following statement of [5, Proposition 2.3]. Let $R \subset T$ be an integral ring extension such that no non-zero-divisor of R becomes a zero-divisor of T, the corresponding total quotient rings $K \subset L$ are distinct, $T \cap K = R \neq K$, (R, M) is quasilocal, and M contains a non-zero-divisor of R; then there is a denumerable chain of R-subalgebras of T. Now, let E be any singly generated ring of characteristic 0 which is finitely generated as a module over $\mathbb{Z}$, is not a domain, and satisfies $(\mathbb{Z} : E) = 0$. By [7, Theorem 3.12], E does not satisfy FSP; i.e., E has infinitely many subrings. More is true, for Theorem 2.1 implies that there is a denumerable chain of rings between $\mathbb{Z}$ and E. However, this conclusion cannot be drawn from [5] (i.e., from [5, Proposition 2.3]) since the base ring $\mathbb{Z}$ is not quasilocal. Finally, if one seeks to illustrate the same phenomenon for a ring extension whose base ring is not a domain, it suffices to consider $\mathbb{Z} \times \mathbb{Z} \subset E \times E$.

(d) One upshot of (b) and (c) is that the results of this section neither imply, nor are implied by, the results in [5]. It seems appropriate to end this section by pointing out, as in [5, Remark 2.2 (a)], that *all* these results do need the hypothesis that the base ring R is not a total quotient ring, the point being that a finite-dimensional field extension cannot have an infinite chain of intermediate rings (fields).

3. Some properties of the ring extensions that have FCP

This section collects some results on ring extensions having FCP. Most of this work will be applied in Section 4 in the characterization of the rings that have FCP. We begin with some facts about subalgebras and rings of fractions.

Proposition 3.1. *Let $R \subseteq T$ be a ring extension. Then:*

(a) If the ring extension $R \subseteq T$ has FCP, then $R \subseteq A$ has FCP and $A \subseteq T$ has FCP for all R-subalgebras A of T.

(b) If $R \subseteq T$ has FCP, then $R_S \subseteq T_S$ has FCP for all multiplicatively closed

subsets S of R.

(c) If, for each maximal ideal M of R, the ring extension $R_M \subseteq T_M := T_{R\setminus M}$ has FCP and $R_M = T_M$ canonically for all but finitely many M, then $R \subseteq T$ satisfies FCP.

Proof. (a) It is clear.

(b) The assertion is an easy consequence of the following fact, which was shown in the proof of [1, Corollary 2.3(a)]. The assignment $E \mapsto E \cap T$ gives an order-preserving injection from the set of R_S-subalgebras of T_S to the set of R-subalgebras of T.

(c) Let M range over the set of maximal ideals of R. We will use the following facts, which were established in the proof of [7, Lemma 3.7]. Consider the canonical ring homomorphism $i : T \to \prod T_M$. Then i is an injection and, if D is any R-subalgebra of T, then $D = i^{-1}(i(D))$ and $i(D) = i(T) \cap \prod D_M$.

Let $\mathcal{C} = \{D_j\}_{j\in J}$ be any chain of R-subalgebras of T. For each M, it follows from (b) that the induced chain $\mathcal{C}_M := \{(D_j)_M\}_{j\in J}$ of R_M-subalgebras of T_M is finite. By hypothesis, there are only finitely many maximal ideals N of R such that $R_N \neq T_N$; denote these finitely many N by $M_1, \ldots, M_r$. Thus, if $M \notin \{M_1, \ldots, M_r\}$ and $j \in J$, we have that $R_M \subseteq (D_j)_M \subseteq T_M = R_M$, so that $\mathcal{C}_M$ is the singleton set $\{R_M\}$. For each $k = 1, \ldots, r$, there exists a finite subchain

$$D_{(1_{M_k})} \subseteq \cdots \subseteq D_{(s_{M_k})}$$

of $\mathcal{C}$ such that $\mathcal{C}_{M_k} = \{(D_{(t)})_{M_k} \mid t = 1_{M_k}, \ldots, s_{M_k}\}$. Therefore (as M runs though all the maximal ideals of R), the set $\{\prod D_M \mid D \in \mathcal{C}\}$ is finite and so, by the facts recalled above from [7], the set of all possible $i^{-1}(i(T) \cap \prod D_M) = D \in \mathcal{C}$ is finite, as required. □

In the spirit of the comments preceding Remark 2.3, we turn next to a fact about pullbacks.

Proposition 3.2. *Let $R \subseteq T$ be a ring extension and I a common ideal of R and T. Then $R \subseteq T$ has FCP if and only if $R/I \subseteq T/I$ has FCP.*

Proof. Applying [6, Lemma II.3] to the pullback $R = T \times_{T/I} R/I$, we have an order-preserving and order-reflecting bijection between the set of all R-subalgebras of T and the set of all R/I-subalgebras of T/I. The assertion now follows easily. □

We next collect some basic facts about algebra-finiteness and algebraicity.

Proposition 3.3. *Let R be a ring with prime ring F and let T be a ring extension of R. Then:*

(a) If $R \subseteq T$ has FIP, then $R \subseteq T$ has FCP.

(b) If R has FSP, then R has FCP.

(c) If $R \subseteq T$ has FCP, then there is a finite subset $\{t_1, \ldots, t_n\}$ of T such that $T = R[t_1, \ldots, t_n]$, $R \subseteq R[t_i]$ has FCP for each $i = 1, \ldots, n$, and each t_i is algebraic over R.

(d) If R has FCP, then there is a finite subset $\{t_1, \ldots, t_n\}$ of R such that $R = F[t_1, \ldots, t_n]$, $F[t_i]$ has FCP for each $i = 1, \ldots, n$, and each t_i is algebraic over F.

Proof. (a) and (b) are clear (and were already noted in the Introduction).

(c) By the proof of [1, Proposition 2.2], we see that if T were not algebra-finite over R, then there would be a(n infinite) strictly ascending chain of R-subalgebras of T, contrary to the hypothesis that $R \subseteq T$ has FCP. Thus, $T = R[t_1, \ldots, t_n]$ for some finite subset $\{t_1, \ldots, t_n\}$ of T. By Proposition 3.1 (a), each $R \subseteq R[t_i]$ has FCP. Finally, each t_i must be algebraic over R, for if some t_i were transcendental over R, we could build the (infinite) strictly descending chain $\{R[t_i^{2^k}]\}_k$ of subrings of $R[t_i]$, contrary to the hypothesis that $R \subseteq T$ has FCP.

(d) Apply (c) with $(F, R) := (R, T)$. □

We show next that the algebraicity conclusion established in Proposition 3.3 (c) can be improved upon.

Proposition 3.4. *Let $R \subseteq T$ be a ring extension that has FCP. Then each $\alpha \in T$ is the root of a polynomial in $R[X]$ with a unit coefficient.*

Proof. Consider the descending chain of rings

$$R[\alpha] \supseteq R[\alpha^2] \supseteq \ \ldots \ \supseteq R[\alpha^{2^k}] \supseteq R[\alpha^{2^{k+1}}] \supseteq \ \ldots .$$

Since $R \subseteq T$ has FCP, $R[\alpha^{2^n}] = R[\alpha^{2^{n+1}}]$ for some positive integer n. In particular, $\alpha^{2^n} \in R[\alpha^{2^{n+1}}]$, from which the assertion is evident. □

Proposition 3.5. *Let R be a finite ring and let T be a ring extension of R. Then $R \subseteq T$ has FCP if and only if T is a finite ring.*

Proof. The "if" assertion is clear. Conversely, suppose that $R \subseteq T$ has FCP. We will show that T is finite by adapting the proof of [1, Proposition 3.4 (c)]. Since R has Krull dimension 0, combining Proposition 3.4 with [1, Proposition 3.4 (a)] shows that T is integral over R. In conjunction with the algebra-finiteness that was established in Proposition 3.3 (c), this implies that T is finitely generated as an R-module. Since R is finite, T must also be finite, as desired. □

We close the section with a technical result that is of some interest.

Proposition 3.6. *Let R be a residually finite ring, and let $R \subseteq T$ be a ring extension which is not integral. Suppose also that $T = R[t]$ for some element t and that $at = 0$ for some nonzero element $a \in R$. Then the ring extension $R \subseteq R[t]$ does not have FCP.*

Proof. We modify the proof of [7, Proposition 3.1]. Note that a is an element of the conductor $I := (R : T)$, and so $I \neq \{0\}$. Moreover, a is a nonunit of R and, indeed, $I \neq R$ since $T \neq R$ by the non-integrality assumption. By the "residually finite" hypothesis, R/I is a finite ring; it is nonzero since $I \neq R$. Moreover, we have $T/I = (R/I)[\bar{t}\,]$, where $\bar{t} := t + I \in T/I$. Since t is not integral over R, it follows easily that $\bar{t}$ is not integral over R/I. Thus, T/I cannot be finitely generated as an (R/I)-module. In particular, T/I is not a finite ring. Thus, by Proposition 3.5, the ring extension $R/I \subseteq T/I$ does not have FCP. Therefore, by Proposition 3.2, neither does $R \subseteq T$. □

4. Characterization of the rings that have FCP

Let R be a ring with prime ring F. With an eye toward eventually using Proposition 3.3 (d) as part of a characterization of the rings that have FCP, we begin by characterizing the singly generated rings of the form $F[t]$ which have FCP. To that end, we will adapt the approach that was used in [7] to study the singly generated rings which have FSP. The case of positive characteristic will be dispatched in Proposition 4.1. As usual, if n is a positive integer, we will write $\mathbb{Z}_n$ instead of $\mathbb{Z}/n\mathbb{Z}$; and we will let $\mathrm{char}(A)$ denote the characteristic of a ring A.

Proposition 4.1. *Let R be a ring R of positive characteristic. Then R has FCP if and only if R is a finite ring.*

Proof. The "if" assertion is trivial. Conversely, suppose that R has FCP. We will show that R is finite. Without loss of generality, $R \neq 0$. Let $n := \mathrm{char}(R)$. Then the prime ring of R is $F \cong \mathbb{Z}_n$, which is finite. As R has FCP, the ring extension $F \subseteq R$ has FCP, and so it follows from Proposition 3.5 that R is finite. □

We turn next to the case of characteristic 0, beginning with the case of domains. As usual, by an *overring* of a domain D, we mean any D-subalgebra of the quotient field of D.

Proposition 4.2. *Let R be a domain of characteristic 0. Then R has FCP if and only if $R \cong \mathbb{Z}_a$ for some positive integer a.*

Proof. If $R \cong \mathbb{Z}_a$, then R has FSP by [6, Proposition V.3], and so the assertion follows from Proposition 3.3 (b). Conversely, assume that R has FCP. Pick a (necessarily finite) maximal chain $\mathbb{Z} = R_0 \subset R_1 \subset \cdots \subset R_m = R$ of subrings of R. Each R_i, being a subring of R, must be a domain; and, by the maximality of the above chain, $R_i \subset R_{i+1}$ is a minimal ring extension, for $i = 0, \ldots, m-1$. Using the properties of minimal ring extensions for domains given in [12, Proposition 3.9] (cf. also [9, Theorem 2.7] and [13, page 1738]), we see that each R_{i+1} is isomorphic to an overring of R_i. Thus, R is isomorphic to an overring of $\mathbb{Z}$. Hence, by [6, Lemma V.2], $R \cong \mathbb{Z}_S$, where S is some saturated multiplicatively closed set which is generated by a uniquely determined subset S' of the set $\mathcal{P}$ of (positive) prime numbers. But the order-preserving bijection between the set of subsets of $\mathcal{P}$ and the set of overrings of $\mathbb{Z}$ [6, Lemma V.2] shows that S' is finite (for, otherwise, one could build an infinite strictly ascending chain of subrings of R, contrary to the assumption that R has FCP). Hence, by the proof of [6, Lemma V.3], $R \cong \mathbb{Z}_a$ where a is the product of the elements of S'. □

We turn next to the case of non-domains. This breaks naturally into three subcases.

Proposition 4.3. *Let R be a ring extension of $\mathbb{Z}$ which is module-finite over $\mathbb{Z}$ but is not a domain. Then R has FCP if and only if $(\mathbb{Z} : R) \neq 0$.*

Proof. By [6, Theorem V.4], $(\mathbb{Z} : R) \neq 0$ if and only if R has FSP. In view of Proposition 3.3 (b), it remains only to show that if R has FCP, then $(\mathbb{Z} : R) \neq 0$. As some (in fact, every nonzero) nonunit of $\mathbb{Z}$ is a non-zero-divisor of $\mathbb{Z}$, the assertion follows from Theorem 2.1. (An alternate proof of this assertion can be found by suitably modifying the last four paragraphs of the FIP-theoretic proof of [6, Proposition V.4].) □

Proposition 4.4. *Let t be an element of some ring extension of $\mathbb{Z}$ such that t is algebraic over $\mathbb{Z}$ but not integral over $\mathbb{Z}$. Suppose also that $\mathbb{Z}[t]$ is not a domain. If the algebraicity polynomial of least degree for t over $\mathbb{Z}$ has degree at least 2, then $\mathbb{Z} \subseteq \mathbb{Z}[t]$ does not have FCP.*

Proof. We will mimic the proof of [6, Corollary V.5]. Consider $R := \mathbb{Z}[t]$ and $I := (\mathbb{Z} : R)$. Assume first that $I \neq 0$. Then $\mathbb{Z}/I$ is a finite ring and $R/I = (\mathbb{Z}/I)[\bar{t}]$, where $\bar{t} := t + I \in T/I$. Moreover, $\bar{t}$ is not integral over $\mathbb{Z}/I$ since t is not integral over $\mathbb{Z}$. Thus R/I is not a finite ring, and so Proposition 4.1 shows that $\mathbb{Z}/I \subseteq R/I$ does not have FCP. Therefore, by Proposition 3.2, $\mathbb{Z} \subseteq R$ does not have FCP.

In the remaining case, where $I = 0$, we can again modify the proof from [6, Corollary V.5], by replacing [6, Theorem V.4] with Proposition 4.3 and [6, Proposition V.3] with Proposition 4.2. In this way, we find a nonzero integer b such that the ring extension $\mathbb{Z} \subseteq \mathbb{Z}[bt]$ does not have FCP. Thus, by Proposition 3.1 (a), R does not have FCP, to complete the proof. □

The last subcase for non-domains concerns a ring extension $\mathbb{Z} \subset \mathbb{Z}[t]$ such that t is algebraic but not integral over $\mathbb{Z}$, with $at = b$, for some nonzero integers a, b and such that $\mathbb{Z}[t]$ is not a domain. For Propositions 4.5–4.7, we impose the following **riding hypotheses and notation** introduced in [7] (just prior to [7, Lemma 3.2]): $\mathbb{Z} \subseteq R := \mathbb{Z}[t]$ is a non-integral ring extension; the element t satisfies $at = b$, where $a \geq 2$ is minimal; $b \geq 1$; the greatest common divisor of a and b is $d := (a, b)$; $\alpha := \frac{a}{d}$; $\beta := \frac{b}{d}$; and $\varphi : \mathbb{Z}[X] \to R$ is the ring homomorphism sending X to t.

Proposition 4.5. *If $d := (a, b) = 1$, then $R := \mathbb{Z}[t]$ has FCP and R is a domain.*

Proof. By [7, Theorem 3.4], R has FSP and R is a domain. The "FCP" conclusion follows from Proposition 3.3 (b). □

Proposition 4.6. *If $d := (a, b) > 1$ and αt is not integral over $\mathbb{Z}$, then $R := \mathbb{Z}[t]$ does not have FCP.*

Proof. By Proposition 3.1 (a), it is enough to show that the ring $S := \mathbb{Z}[\alpha t]$ does not have FCP. Consider the conductor $I := (\mathbb{Z} : S)$. By the proof of [7, Proposition 3.5], we get that $d \in I$, and so $\mathbb{Z}/I$ is a finite nonzero ring. Moreover, S/I cannot be finitely generated as a $(\mathbb{Z}/I)$-module, and so S/I is not a finite ring. Hence, by Proposition 4.1, S/I does not have FCP; i.e., the ring extension $\mathbb{Z}/I \subseteq S/I$ does not have FCP. Therefore, by Proposition 3.2, $\mathbb{Z} \subseteq S$ does not have FCP; i.e., S does not have FCP. □

We can now provide the last key step.

Proposition 4.7. *In addition to the riding hypotheses and notation, assume also that αt is integral over $\mathbb{Z}$. Then $R := \mathbb{Z}[t]$ has FCP if and only if there does not exist a prime number p such that* $\ker(\varphi) \subseteq p\mathbb{Z}[X]$.

Proof. Assume first that there does not exist a prime number p such that $\ker(\varphi) \subseteq p\mathbb{Z}[X]$. By [7, Theorem 3.8], R has FSP. Thus, R has FCP by Proposition 3.3 (b).

Conversely, assume that R has FCP. Observe that $\{\mathbb{Z}[t^{2^n}] \mid n = 1, 2, \dots\}$ is a descending chain of subrings of R. As R has FCP, this chain must terminate. Thus, there exist positive integers $k < m$ such that $\mathbb{Z}[t^{2^k}] = \mathbb{Z}[t^{2^m}]$. As $t^{2^k} \in \mathbb{Z}[t^{2^m}]$, we

can write $t^{2^k} = \sum_{i=0}^{n} d_i(t^{2^m})^i$, where each $d_i \in \mathbb{Z}$ (and n is a non-negative integer). Hence

$$0 = d_0 - t^{2^k} + d_1 t^{2^m} + d_2 t^{2\cdot 2^m} + \cdots + d_n t^{n\cdot 2^m},$$

and so $h := d_0 - X^{2^k} + d_1 X^{2^m} + d_2 X^{2\cdot 2^m} + \cdots + d_n X^{n\cdot 2^m} \in \ker(\varphi)$. Since h visibly has a unit coefficient, there can be no prime number p such that $\ker(\varphi) \subseteq p\mathbb{Z}[X]$. □

We proceed to give our two main results. Taken together, they serve to characterize the rings that have FCP. We begin with the characterization for singly generated rings. Recall that we define a ring to be *singly generated* if it is a (necessarily commutative unital) ring generated by some set of the form $\{0, 1, s\}$.

Theorem 4.8. *Let R be a singly generated ring. Then the following conditions are equivalent:*

(1) R has FCP.

(2) R has FSP.

(3) One of the following four conditions holds:

(a) R is a finite ring;

(b) $R \cong \mathbb{Z}_a$ for some positive integer a;

(c) R is a module-finite ring extension of $\mathbb{Z}$ which is not a domain and the conductor $(\mathbb{Z} : R)$ is nonzero;

(d) $R = \mathbb{Z}[t] \supset \mathbb{Z}$ is not integral over $\mathbb{Z}$, R is not a domain, there exist integers $a, b \geq 2$ such that $at = b$, and the greatest common divisor $d := (a, b)$ of the minimal such a and the corresponding b satisfies the following conditions: $d > 1$, $\frac{a}{(a,b)}t$ is integral over $\mathbb{Z}$, and there does not exist a prime number p such that $\ker(\varphi) \subseteq p\mathbb{Z}[X]$, where φ is the ring homomorphism $\mathbb{Z}[X] \to R$ sending X to t.

Proof. The equivalence (2) ⇔ (3) is a restatement of [7, Theorem 3.12]; and Proposition 3.3 (b) gives (2) ⇒ (1). It remains only to prove that (1) ⇒ (3).

Assume that R has FCP. If $\mathrm{char}(R) > 0$, then Proposition 4.1 gives (3)(a). If R is a domain of characteristic 0, then Proposition 4.2 gives (3)(b). If R is not a domain, is of characteristic 0 and is integral over $\mathbb{Z}$, then R is a module-finite ring extension of $\mathbb{Z}$ (since R is integral over $\mathbb{Z}$ and singly generated), and so Proposition 4.3 gives (3)(c). The last case arises when R is not a domain, is of characteristic 0 and is not integral over $\mathbb{Z}$. By hypothesis, $R = \mathbb{Z}[t]$ for some element t, and by Proposition 3.4, t must be algebraic over $\mathbb{Z}$. Then Propositions 4.4, 4.5, 4.6 and 4.7 combine to give (3)(d). □

We can now reduce matters to the singly generated case (which was handled in Theorem 4.8) and, in particular, show that the FCP and FSP properties of rings are equivalent.

Theorem 4.9. *Let R be a ring with prime ring F. Then the following conditions are equivalent:*

(1) R has FCP;

(2) R has FSP;

(3) R is a finite-type F-algebra and whenever $\{t_1, \ldots, t_n\}$ is a finite set such that $R = F[t_1, \ldots, t_n]$, then $F[t_i]$ has FSP for each i;

(4) R is a finite-type F-algebra and whenever $\{t_1, \ldots, t_n\}$ is a finite set such that $R = F[t_1, \ldots, t_n]$, then $F[t_i]$ has FCP for each i;

(5) Either (a) R is a finite-type ring extension of $\mathbb{Z}$ and whenever $\{t_1, \ldots, t_n\}$ is a finite set such that $R = \mathbb{Z}[t_1, \ldots, t_n]$, then $\mathbb{Z}[t_i]$ has FCP for each i or (b) R is finite.

(6) Either (λ) R is a ring extension of $\mathbb{Z}$ such that there exists a finite set $\{t_1, \ldots, t_n\}$ for which $R = \mathbb{Z}[t_1, \ldots, t_n]$ and $\mathbb{Z}[t_i]$ has FCP for each i or (μ) R is finite.

Proof. (1) $\Rightarrow$ (4) Rework the proof of Proposition 3.3 (d).

(4) $\Leftrightarrow$ (3) Apply Theorem 4.8.

(3) $\Leftrightarrow$ (2) This equivalence is part of [8, Theorem 3.20].

(2) $\Rightarrow$ (1) Apply Proposition 3.3 (b).

Since we have seen that (1) $\Leftrightarrow$ (2), the equivalence of (5) and (6) with the other conditions now follows from the corresponding equivalences that were established for the FSP property in [8, Theorem 3.20]. □

In closing, we answer a question that may arise because of the phrase "maximal cardinality" that appears in the title of this work. If a ring R is such that each chain of subrings of R is finite, must there be a finite upper bound on the cardinality of all such chains? The answer is in the affirmative, for that is precisely the content of the implication (1) $\Rightarrow$ (2) in Theorem 4.9. One such upper bound is the cardinality of the set of subrings of R. This is the least upper bound in case the subrings of R are linearly ordered by inclusion, a situation which has been studied in [3], [4], [10].

References

[1] D. D. Anderson, D. E. Dobbs and B. Mullins, *The primitive element theorem for commutative algebras*, Houston J. Math., 25 (1999), 603–623. Corrigendum, Houston J. Math., 28 (2002), 217–219.

[2] A. Ayache and A. Jaballah, *Residually algebraic pairs of rings*, Math. Zeit., 225 (1997), 49–65.

[3] E. Curtin, *Infinite rings whose subrings are nested*, Proc. Roy. Irish Acad. Sect. A, 94 (1994), 59–66.

[4] E. Curtin, *Finite rings whose subrings are nested*, Proc. Roy. Irish Acad. Sect. A, 94 (1994), 67–75.

[5] D. E. Dobbs, *Extensions of integral domains with infinite chains of intermediate rings*, Comm. Algebra, to appear.

[6] D. E. Dobbs, B. Mullins, G. Picavet and M. Picavet-L'Hermitte, *On the FIP property for extensions of commutative rings*, Comm. Algebra, 33 (2005), 3091–3119.

[7] D. E. Dobbs, B. Mullins and M. Picavet-L'Hermitte, *The singly generated unital rings with only finitely many unital subrings*, Comm. Algebra, 36 (2008), 2638–2653.

[8] D. E. Dobbs, G. Picavet and M. Picavet-L'Hermitte, *A characterization of the commutative unital rings with only finitely many unital subrings*, J. Algebra Appl., to appear.

[9] D. E. Dobbs and J. Shapiro, *A classification of the minimal ring extensions of an integral domain*, J. Algebra, 305 (2006), 185–193.

[10] M. S. Gilbert, Extensions of commutative rings with linearly ordered intermediate rings, Ph. D. dissertation, University of Tennessee, Knoxville, TN, 1996.

[11] R. Gilmer, *Some finiteness conditions on the set of overrings of an integral domain*, Proc. Amer. Math. Soc., 131 (2003), 2337–2346.

[12] G. Picavet and M. Picavet-L'Hermitte, About minimal morphisms, Multiplicative Ideal Theory in Commutative Algebra, Springer-Verlag, New York (2006), 369–386.

[13] J. Sato, T. Sugatani and K. I. Yoshida, *On minimal overrings of a Noetherian domain*, Comm. Algebra, 20 (1992), 1735–1746.

David E. Dobbs
Department of Mathematics,
University of Tennessee,
Knoxville, TN 37996-1300, U.S.A.
e-mail: dobbs@math.utk.edu

Gabriel Picavet and Martine Picavet-L'Hermitte
Laboratoire de Mathématiques Pures
Université Blaise Pascal
63177 Aubière Cedex, France
e-mails: Gabriel.Picavet@math.univ-bpclermont.fr
Martine.Picavet@math.univ-bpclermont.fr