Gulf Journal of Mathematics
Vol 10, Issue 1 (2021) 69-94

CHARACTERIZING FINITE BOOLEAN RINGS BY USING FINITE CHAINS OF SUBRINGS

DAVID E. DOBBS[1] AND NOÔMEN JARBOUI[2,3*]

Abstract. Let R be a nonzero associative ring with identity. It is proved that R is a finite Boolean ring if (and only if) 1 is the only unit of R and there exists a finite maximal chain $\mathcal{C}$ each of whose n steps is a proper unital ring extension, $R_0 := \mathbb{F}_2 \subset \ldots \subset R_n = R$, going from $\mathbb{F}_2$ to R. If these equivalent conditions hold and R has exactly n maximal ideals, then any such $\mathcal{C}$ has length $n-1$ and the number of unital subrings of R is B_n, the n^{th} Bell number. It is also proved that if R has characteristic p for some prime number p, then R is isomorphic to a finite direct product of copies of $\mathbb{F}_p$ if (and only if) for some integer $m \geq 0$, R has exactly $m+1$ maximal ideals and there exists a finite maximal chain of proper unital ring extensions, $\mathcal{R}_0 := \mathbb{F}_p \subset \ldots \subset \mathcal{R}_m = R$, going from $\mathbb{F}_p$ to R, such that $\mathcal{R}_{m-1}$ is a commutative ring and R is a unital $\mathcal{R}_{m-1}$-algebra. Additional characterizations, applications, examples and remarks are given.

1. Introduction

The first goal of this work is to generalize some recent results from [19] to a noncommutative setting and thereby deepen our understanding of finite Boolean rings. Accomplishing the first goal will involve extending the context for the FIP, FCP and FMC concepts to noncommutative ring extensions. Our second goal is to, insofar as possible, extend the methods that gave our main result on finite Boolean rings and thereby use finite maximal chains of rings to obtain characterizations of several classes of rings of arbitrary prime characteristic p, such as the finite direct products of copies of $\mathbb{F}_p$. Since a minimal ring extension of a commutative ring can be noncommutative, the accomplishment of the second goal will require the introduction of a variant of the FMC property that permits the use of methods that have been fruitful for commutative ring extensions.

The next paragraph announces some conventions and notation. After that, four paragraphs provide some relevant background, then one paragraph states the results from [19] that we are generalizing, then one paragraph gives details about our first main result (Theorem 2.2) and explains some ways in which it generalizes the above-mentioned results from [19], and then two paragraphs describe our results for arbitrary prime characteristic p, including a catenarian conclusion

Date: Received: Jan 12, 2021; Accepted: Mar 6, 2021.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 13B99; Secondary 13A15, 16U60, 16B99.

Key words and phrases. Associative ring, Boolean ring, unit, unital ring extension, FMC, minimal ring extension.

(Corollary 2.10 (b)) that strengthens an inequality that had been observed in [19] in the Boolean context.

All rings considered below are assumed to be associative and unital. All inclusions of rings, all subrings and all ring extensions are assumed to be unital; and all algebras (over commutative rings) are considered to be unital (though not necessarily commutative). If R is a ring, then $\mathrm{Max}(R)$ denotes the set of maximal ideals of R and $\mathrm{U}(R)$ denotes the set of units of R. Also, if $\mathfrak{S}$ is a set, then $\mathcal{P}(\mathfrak{S})$ denotes the power set of $\mathfrak{S}$ and $|\mathfrak{S}|$ denotes the cardinal number of $\mathfrak{S}$. As usual, for each positive integer n, B_n denotes the n^{th} *Bell number*, that is, the number of partitions of the set $\{1, \ldots, n\}$; and $\subset$ denotes proper inclusion.

It is convenient to recall next that a ring extension $A \subset B$ is called a *minimal ring extension* if there does not exist a ring C such that $A \subset C \subset B$. The definition of this concept in [16] stipulated that the rings A and B are commutative, but this concept has been extended and studied for arbitrary (that is, possibly noncommutative) rings in recent years, in papers such as [15], [2] and [8].

Next, we extend the context for some concepts that have been widely studied for ring extensions involving commutative rings. Let $R \subseteq S$ be (possibly noncommutative) rings. We say that $R \subseteq S$ *satisfies* FIP if $|[R, S]| < \infty$. Also, we say that $R \subseteq S$ *satisfies* FCP if every chain in $[R, S]$ is finite; and we say that $R \subseteq S$ *satisfies* FMC if there exists a finite maximal chain, $R = R_0 \subset \ldots \subset R_n = S$, in $[R, S]$ going from R to S. (Note that in any such chain, each step $R_{i-1} \subset R_i$ is a minimal ring extension.) For ring extensions in which the top ring is (and hence both rings are) commutative, the FIP property and the FCP property were each characterized in [12], but we are not aware of any characterizations of either of those properties for ring extensions involving arbitrary (that is, possibly noncommutative) rings. For arbitrary ring extensions, it is clear that FIP $\Rightarrow$ FCP $\Rightarrow$ FMC, but neither of these implications has a valid converse. The classical example of a ring extension that satisfies FCP but not FIP is $\mathbb{F}_p[X^p, Y^p] \subset \mathbb{F}_p[X, Y]$, where p is any prime number and X, Y are commuting, algebraically independent indeterminates over $\mathbb{F}_p$. An example showing that FMC $\not\Rightarrow$ FCP was given in [4, Example 6.4]. (The latter example is striking. It features a quasi-local (commutative) integral domain R of Krull dimension 2 and an overring S of R (contained in the quotient field of R) such that there exists a maximal chain in $[R, S]$ that has length 2 and goes from R to S (so $R \subset S$ satisfies FMC) although $R \subset S$ does not satisfy FCP. In a sense, this example is best-possible, because the existence of a maximal chain of rings of length 1 going from A to B is equivalent to $A \subset B$ being a minimal ring extension, and of course, any minimal ring extension satisfies FCP.)

Recall that a ring R is called a *Boolean ring* if $r^2 = r$ for all $r \in R$. It is well known (and easy to see) that any Boolean ring is commutative and, if it is nonzero, has characteristic 2. The only integral domain that is a Boolean ring is $\mathbb{Z}/2\mathbb{Z}$ (that is, $\mathbb{F}_2$); and a direct product $\prod_{i \in I} R_i$ is a Boolean ring if and only if R_i is a Boolean ring for each $i \in I$. In particular, any direct product of finitely many copies of $\mathbb{F}_2$ is a finite Boolean ring. The converse is well known. Indeed, one can use the Chinese Remainder Theorem to show that if R is a Boolean ring with $|\mathrm{Max}(R)| = n < \infty$, then R is isomorphic to the direct product of n copies

of $\mathbb{F}_2$: cf. the proof of (4) $\Rightarrow$ (2) in [9, Corollary 2.5]. Thus, a finite commutative ring R is a Boolean ring if and only if R is isomorphic to a direct product of finitely many copies of $\mathbb{F}_2$. Consequently, any finite Boolean ring R satisfies $|R| = 2^n$ for some non-negative integer n. The following is another classical way to characterize these rings: a ring R such that $|R| = 2^n < \infty$ is a (finite) Boolean ring if and only if R is isomorphic to $\mathcal{P}(\{1, \ldots, n\})$. (The ring structure on $\mathcal{P}(\mathfrak{S})$ for any set $\mathfrak{S}$ will be reviewed two paragraphs below.) A proof of this classical characterization of finite Boolean rings can be found in [24, Theorem 3.20] as an application of subdirect sums. Remark 2.3 (g) will give a direct, straightforward way to connect the above two classical characterizations of the finite Boolean rings.

It is easy to see that if R is a Boolean ring, then $\mathrm{U}(R) = \{1\}$. Recently, in [9], the authors initiated the study of (possibly noncommutative) rings R such that $\mathrm{U}(R) = \{1\}$. Any nonzero ring R with this property must have characteristic 2. Such a ring need not be commutative, as the free $\mathbb{F}_2$-algebra on any set has this property [9, Theorem 2.1]. Some evident examples of commutative rings with this property are provided by [9, Theorem 2.13 (a)], namely, the polynomial rings over $\mathbb{F}_2$ in any (possibly infinite) set of commuting, algebraically independent indeterminates. The "$\mathrm{U}(R) = \{1\}$" concept has been used to characterize Boolean rings using a criterion that does not explicitly posit commutativity. Indeed, a ring R is Boolean if and only if $\mathrm{U}(R) = \{1\}$ and R is a von Neumann regular ring [9, Corollary 2.10]. In the same vein, [9, Corollary 2.5] included the following characterizations. If R is a ring, then: R is a finite Boolean ring $\Leftrightarrow$ $\mathrm{U}(R) = \{1\}$ and R is a left- (or right- or both) Artinian ring $\Leftrightarrow$ $\mathrm{U}(R) = \{1\}$ and R is a semisimple ring.

In contrast to the setting of the preceding paragraph, [19] studied rings R that are exquisitely commutative, specifically, rings of the form $R = \mathcal{P}(\mathfrak{S})$ for some (usually nonempty, often finite) set $\mathfrak{S}$. As is well known (and easy to see), $\mathcal{P}(\mathfrak{S})$ is a Boolean ring, with symmetric difference playing the role of addition and intersection playing the role of multiplication, so that $\mathfrak{S}$ is the multiplicative identity element of $\mathcal{P}(\mathfrak{S})$. If $|\mathfrak{S}| \geq 2$, we will identify $\{\emptyset, \mathfrak{S}\}$ with $\mathbb{F}_2$, so that $\mathbb{F}_2 \subseteq \mathcal{P}(\mathfrak{S})$. We next discuss the first of the results from [19] that we are generalizing here. Apart from a topologically formulated equivalent condition that we will mention later, [19, Theorem 2.3] can be stated as follows. Let $\mathfrak{S}$ be a nonempty set and $R := \mathcal{P}(\mathfrak{S})$. Then R is a finite Boolean ring $\Leftrightarrow$ $\mathbb{F}_2 \subseteq R$ satisfies FIP $\Leftrightarrow$ $\mathbb{F}_2 \subseteq R$ satisfies FCP; and if these equivalent conditions hold and $n := |\mathfrak{S}| \geq 2$, then $|[\mathbb{F}_2, R]| = \mathrm{B}_n$. Next, we discuss the second of the results from [19] that we are generalizing here. One can state [19, Theorem 2.5] as follows. If $\mathfrak{S}$ is a finite set with $2 \leq n := |\mathfrak{S}|$ and $R := \mathcal{P}(\mathfrak{S})$, then the maximal length of a (finite maximal) chain in $[\mathbb{F}_2, R]$ is $n - 1$. One should note that the methods in [19] are largely topological and the main contribution in [19] is the "topologically formulated equivalent condition" that we promised to mention. That remaining part of [19, Theorem 2.3] can be stated as follows: if $\mathfrak{S}$ is a nonempty set and $R := \mathcal{P}(\mathfrak{S})$, then R is a finite Boolean ring if and only if the elements of $[\mathbb{F}_2, R]$ are the topologies on $\mathfrak{S}$ in which every open set is closed.

We next describe what is established in our first main result (Theorem 2.2) and indicate two of the ways that, in our opinion, it improves the above-mentioned results from [19]. (Remark 2.4 (a) indicates six such ways.) Theorem 2.2 (a) states that if R is a nonzero ring, then: R is a finite Boolean ring $\Leftrightarrow$ $\mathrm{U}(R) = \{1\}$ and $\mathbb{F}_2 \subseteq R$ satisfies FIP $\Leftrightarrow$ $\mathrm{U}(R) = \{1\}$ and $\mathbb{F}_2 \subseteq R$ satisfies FCP $\Leftrightarrow$ $\mathrm{U}(R) = \{1\}$ and $\mathbb{F}_2 \subseteq R$ satisfies FMC. Perhaps the most important way that this improves [19, Theorem 2.3] is the (possibly unexpected) involvement of the FMC property in an equivalent condition that gives a significant deepening of our understanding of conditions on finite chains of ring extensions. The most significant part of Theorem 2.2 (b) states that if R is a finite nonzero Boolean ring with $n := |\mathrm{Max}(R)|$, then each finite maximal chain of rings in $[\mathbb{F}_2, R]$ going from $\mathbb{F}_2$ to R has length $n-1$ and $[\mathbb{F}_2, R]| = \mathrm{B}_n$. Perhaps the most important way that this improves the nontopological portion of [19, Theorem 2.5] that was stated above is that Theorem 2.2 (b) establishes a kind of caternarian behavior for the poset $[\mathbb{F}_2, R]$ inasmuch as *every* finite maximal chain is shown to have length $n-1$ (whereas [19, Theorem 2.5] left open the question of whether some finite maximal chain could have length less than $n-1$).

The first part of the paper closes with a far-ranging eight-part remark that includes additional comments about the concepts discussed to that point and, in Remark 2.4 (f), a suggestion for a possible direction for future research.

The second half of the paper begins with Example 2.5, which presents an example of a chain of minimal ring extensions $B_0 \subset B_1 \subset B_2$ such that B_0 and B_1 are commutative, B_2 is noncommutative, and $|B_2|$ is minimal with these properties. While the data in Example 2.5 has been considered earlier (for instance, in [20]), the minimality of $|B_2|$ seems to be new. In Example 2.5, B_2 is neither a B_1-algebra nor a nontrivial direct product. The latter aspect means that one cannot study such data by using some methods that have been fruitful in dealing with finite chains of commutative ring extensions, such as those summarized in [7, Lemma 2.2]. To avail ourselves of those methods here, we introduce the "Adjusted FMC" condition (in short, AFMC) that restricts attention to the finite maximal increasing chain of rings with the property that their last step $B_{m-1} \subset B_m$ is such that B_m is a B_{m-1}-algebra. Although it is easy to see that AFMC implies that B_m is commutative (cf. Theorem 2.7 (a)), having access to the AFMC conditions allows us to characterize some classes of rings in settings that are ostensibly noncommutative. For any prime number p, these include the finite fields of characteristic p (Corollary 2.8), the finite commutative semisimple rings of characteristic p (Corollary 2.9) and rings isomorphic to finite direct products of F_p (Corollary 2.10). These results are obtained by repeated use of ([7, Lemma 2.2], of course, and) Theorem 2.7 (c), which is our main technical result that studies the AFMC property by bringing to bear the inert/decomposed/ramified trichotomy (in the sense of [10]) for the minimal ring extensions whose rings are commutative.

We view our second main result, Corollary 2.10, as being the natural counterpart of Theorem 2.2 when considering finite rings of arbitrary prime characteristic p. As p need not be 2, one needs a replacement for the "$\mathrm{U}(R) = \{1\}$" condition that had appeared in the characterizations of finite Boolean rings in Theorem

2.2 (a). This replacement is accomplished in a number of ways in the characterizations that are given in Corollary 2.10 (a); and, of course, AFMC plays a role in each of those characterizations that is analogous to the role that FMC played in Theorem 2.2 (a). Most pleasantly, our approach allows the proof of Theorem 2.2 (b) to carry over, *mutatis mutandis*, to prove Corollary 2.10 (b). For any prime number p, the upshot is that if R is isomorphic to a direct product of n ($< \infty$) copies of $\mathbb{F}_p$, then the poset $[\mathbb{F}_p, R]$ exhibits the following kind of catenarian behavior: *every* finite maximal chain has length $n - 1$. Thus, Corollary 2.10 (b) generalizes Theorem 2.2 (b) (which is the case $p = 2$), which was itself a generalization of an inequality in [19, Theorem 2.5]. Moreover, Corollary 2.11 gives a result that seems to be new even in the finite Boolean case ($p = 2$): for any prime number p, if R is a ring of the kind characterized in Corollary 2.10 (a) and n is any positive integer, the properties "$|\mathrm{Max}(R)| = n$" and "$|[\mathbb{F}_p, R]| = B_n$" are equivalent. However, as Example 2.11 shows, it is easy to see, for any prime number p, that those two properties are logically independent in the universe of finite commutative rings of characteristic p. Needless to say, this overview has not specified the fine tuning of the AFMC concept ("m-AFMC chain" property) that is deeply involved in the statements and proofs of the above-mentioned results in the second half of this paper.

We wish to express our thanks to Gabriel Picavet and Martine Picavet-L'Hermitte for a stimulating correspondence in regard to Example 2.5.

A final comment about notation: as usual, X will denote an indeterminate over the ambient ring(s).

2. Results

For several decades, different schools of thought have assigned differing meanings to the term "ring" and to associated terms such as 'subring" and "ring extension." Our usage here was stipulated in the first and second sentences of the third paragraph of the Introduction. In order to clearly cite and use some deep material that has been developed by the "other" school of thought, we devote the next paragraph to some definitions that will be put to work in Lemma 2.1.

As usual, an *rng* is a "ring possibly without 1," that is, a structure satisfying all the axioms of a (unital) ring except possibly the axiom requiring the existence of a multiplicative identity. Thus, a ring R is same as an rng that has a multiplicative identity. At times, it will be convenient to denote the multiplicative identity of a ring R by 1_R. Also, we will say that A is a *subrng* of B (or that $A \subseteq B$ is an *rng extension*, or that B is an *rng extension* of A) if A and B are rngs such that $A \subseteq B$ and the operations of addition and multiplication on A are induced by the corresponding operations on B. Finally, if $A \subset C$ is an rng extension, we say that $A \subset C$ is a *minimal rng extension* (or that A is a *maximal subrng* of C) if A and C are the only rngs B such that both $A \subseteq B$ and $B \subseteq C$ are rng extensions.

Lemma 2.1. *(a) Let A, B, C be such that A is a subrng of B, B is a subrng of C, and A is a subring of C. Then both $A \subseteq B$ and $B \subseteq C$ are (unital) ring extensions.*

(*b*) *If $A \subset C$ is a minimal ring extension, then A is a maximal subrng of C.*

(*c*) (*Cf. Laffey* [22]*, Klein* [21]) *If $R \subset S$ is a minimal ring extension and R is finite, then S is finite.*

(*d*) *Let R be a nonzero ring of characteristic $n > 0$ and view $\mathbb{Z}/n\mathbb{Z} \subseteq R$ as usual. Then R is finite if and only if $\mathbb{Z}/n\mathbb{Z} \subseteq R$ satisfies* FMC.

Proof. (a) It suffices to prove that B is a ring such that 1_B equals both 1_A and 1_C. As $A \subseteq C$ is a ring extension, $1 := 1_A = 1_C$. Since the multiplication on B is induced by the multiplication on C and $1 = 1_C = 1_A \in A \subseteq B$, we have that 1 acts like a multiplicative identity element of B. Thus, B is a ring with $1_B = 1 = 1_C = 1_A$.

(b) We will prove that if B is an rng such that both $A \subseteq B$ and $B \subseteq C$ are rng extensions, then B is either A or C. Therefore, since $A \subset C$ is a minimal ring extension, it suffices to prove that both $A \subseteq B$ and $B \subseteq C$ are ring extensions. This, in turn, follows from (a).

(c) In view of (b), it may appear, at first glance, that the assertion in (c) is the same as a deep result that was proven independently by Laffey and Klein (in [22] and [21], respectively). However, the items called "rings" (resp., "ring extensions;" resp., "maximal subrings") in [22] and [21] are actually rngs (resp., rng extensions; resp., maximal subrngs). This can be discerned in [22, line 9, page 286] where one considers the possibility that a certain proper ideal (arising from a result of Lewin [23, Lemma 1]) may be a "subring" of a given "ring." While [23, Lemma 1] also plays a role in the proof in [21], Klein explicitly states [21, page 1389] that the larger "ring" in a "ring extension" is not assumed to contain a multiplicative identity element. Accordingly, before applying the result of Laffey and Klein, we must reformulate it by using our terminological conventions. The result of Laffey and Kline can be restated as follows: if C is a maximal subrng of D and C is finite, then D is finite. Combining this fact with (b) immediately establishes (c).

(d) The "only if" assertion is intuitively clear (since the finiteness of R ensures that the poset $[\mathbb{Z}/n\mathbb{Z}, R]$ satisfies both the descending chain condition and the ascending chain condition). For the sake of completeness, we next give the details of a formal proof of it. Assume that R is finite. We induct on $|R|$ (restricting attention to rings having the fixed characteristic n). For the induction basis, $R = \mathbb{Z}/n\mathbb{Z}$, and the assertion is clear in this case. Hence, without loss of generality, $|R| > n$ and we turn to the induction step. Since any strictly increasing chain $\{R_i\}$ of subrings of R leads to a strictly increasing sequence $\{|R_i|\}$ of positive integers bounded above by $|R| < \infty$, it follows that R has a maximal subring. (This conclusion could also be obtained by arguing that, since R is a finitely generated module over the Noetherian ring $T := \mathbb{Z}/n\mathbb{Z}$, R is a Noetherian T-module, and so the existence of a maximal subring of R follows by applying the maximum condition to the set of proper subrings of R.) Choose a maximal subring A of R. As $A \subset R$ is a minimal ring extension, $|A| < |R|$. Hence, by the (strong) induction hypothesis, there exists a finite maximal chain $\mathcal{C}$ of rings going from $\mathbb{Z}/n\mathbb{Z}$ to A. Then $\mathcal{C} \cup \{R\}$ is a finite maximal chain of rings going from $\mathbb{Z}/n\mathbb{Z}$ to R, and so $\mathbb{Z}/n\mathbb{Z} \subseteq R$ satisfies FMC. This proves the "only if" assertion.

Next, assume that the "if" assertion fails. Choose a counterexample R with a finite maximal chain $\mathcal{C}$,

$$\mathbb{Z}/n\mathbb{Z} = R_0 \subset \ldots \subset R_k = R,$$

of rings going from $\mathbb{Z}/n\mathbb{Z}$ to R such that k, the length of $\mathcal{C}$, is minimal (among chains going from $\mathbb{Z}/n\mathbb{Z}$ to counterexamples to the "if" assertion). As R is a counterexample, R is infinite. Thus $k \geq 1$. Since $\mathcal{C}\backslash\{R_k\}$ is a finite maximal chain (of length $k-1$) going from $\mathbb{Z}/n\mathbb{Z}$ to R_{k-1}, the minimality of k ensures that R_{k-1} is not a counterexample; that is, R_{k-1} is finite. Then, since $R_{k-1} \subset R_k$ is a minimal ring extension, it follows from (c) that R is finite, the desired contradiction, thus completing the proof. □

We next present our first main result. Using the above material and a result from [9], we will quickly prove a new characterization of finite Boolean rings in Theorem 2.2 (a). As mentioned in the Introduction (and as will be explained in detail in Remark 2.4 (x)), Theorem 2.2 improves upon [19, Theorems 2.3 and 2.5] in a number of ways. To condense notation, we will write $\mathbb{F}_2$ instead of $\mathbb{Z}/2\mathbb{Z}$ in Theorem 2.2, with similar notational economies later.

Theorem 2.2. *Let R be a nonzero ring. Then:*

(a) The following conditions are equivalent:

(1) $\mathrm{U}(R) = \{1\}$ *and* $\mathbb{F}_2 \subseteq R$ *satisfies* FIP*;*

(2) $\mathrm{U}(R) = \{1\}$ *and* $\mathbb{F}_2 \subseteq R$ *satisfies* FCP*;*

(3) $\mathrm{U}(R) = \{1\}$ *and* $\mathbb{F}_2 \subseteq R$ *satisfies* FMC*;*

(4) $\mathrm{U}(R) = \{1\}$ *and there exists at least one finite maximal chain,* $\mathbb{F}_2 = \mathcal{D}_0 \subset \ldots \subset \mathcal{D}_m = R$*, in* $[\mathbb{F}_2, R]$*;*

(5) R is a finite Boolean ring.

(b) If the equivalent conditions in (a) hold and $n := |\mathrm{Max}(R)|$*, then any finite maximal chain as in (4) has length* $m = n - 1$ *and the number of subrings of R is* B_n*, the* n^{th} *Bell number.*

Proof. (a) It is clear that (5) ⇒ (1); and (3) ⇔ (4) by the definition of the FMC property. Moreover, (1) ⇒ (2) ⇒ (3) trivially, since FIP ⇒ FCP ⇒ FMC. Therefore, it will suffice to prove that (3) ⇒ (5).

Assume (3). Then, by Lemma 2.1 (d), R is finite. According to [9, Corollary 2.5], a ring is a finite Boolean ring if (and only if) it is finite and has only one unit. Hence, R is a (finite) Boolean ring, as desired.

(b) It will be convenient, for each integer $e \geq 1$, to let T^e denote the direct product of e copies of $\mathbb{F}_2$. Assume (4). We claim that R is isomorphic (as a ring) to T^{m+1}. Without loss of generality, $m \geq 1$. By hypothesis, there exists a finite maximal chain of rings $\mathbb{F}_2 = \mathcal{D}_0 \subset \mathcal{D}_1 \subset \cdots \subset \mathcal{D}_m = R$. We will prove, by induction on k (for $1 \leq k \leq m$), that each $\mathcal{D}_k$ is isomorphic as a $\mathcal{D}_{k-1}$-algebra to $\mathbb{F}_2 \times \mathcal{D}_{k-1}$ (and hence isomorphic as a ring to T^{k+1}). We turn next to the case $k = 1$.

Since it is a subring of the Boolean ring R, $\mathcal{D}_1$ must be commutative. Therefore, by a fundamental classification result of Ferrand-Olivier [16, Lemme 1.2], there are only three possibilities for the structure of $\mathcal{D}_1$ as an $\mathbb{F}_2$-algebra. Two of these three possibilities are ruled out because $\mathrm{U}(\mathcal{D}_1) = \{1\}$. So, up to isomorphism as

an $\mathbb{F}_2$-algebra, $\mathcal{D}_1$ must be the remaining possibility, which is T^2. Replacing $\mathcal{D}_1$ with T^2 has the effect, for all $i = 2, \ldots, m$, of replacing $\mathcal{D}_i$ with $\mathcal{D}_i \otimes_{\mathcal{D}_1} T^2$, which is isomorphic as a $\mathcal{D}_1$-algebra to $\mathcal{D}_i$. One must make this kind of replacement and theoretical observation at each stage of this inductive/iterative proof, noting that it does not affect the conclusion that the ring at hand has the claimed description up to isomorphism. This proves the above claim in case $k = 1$.

Next, for the induction step, we can assume that $2 \leq k < m$ and we have arranged that $\mathcal{D}_k$ is T^{k+1}. Since $\mathcal{D}_k \subset \mathcal{D}_{k+1}$ is a minimal ring extension, [7, Lemma 2.2] shows that for some (uniquely determined) index i such that $1 \leq i \leq k+1$, $\mathcal{D}_{k+1}$ is $\mathcal{D}_k$-algebra isomorphic to

$$(\prod_{j=1}^{i-1} \mathbb{F}_2) \times E \times (\prod_{j=i+1}^{k+1} \mathbb{F}_2),$$

where $\mathbb{F}_2 \subset E$ is a minimal ring extension (and, as usual, an empty direct product is the zero ring and can be ignored). Necessarily, $\mathrm{U}(E) = \{1\}$. Hence, by the above argument (while analyzing $\mathcal{D}_1$) that used [16, Lemme 1.2], E is $\mathbb{F}_2$-algebra isomorphic to T^2. Therefore, $\mathcal{D}_{k+1}$ is $\mathcal{D}_k$-algebra isomorphic to the direct product of $(k+1)+1 = k+2$ copies of $\mathbb{F}_2$; that is, $\mathcal{D}_{k+1} \cong T^{k+2}$ as $\mathcal{D}_k$-algebras. Using tensor products to adjust $\mathcal{D}_{k+1}, \ldots, , \mathcal{D}_m$ (but only up to isomorphism), we thus complete a proof of the induction step. This completes the inductive/iterative proof of the above claim that $R = \mathcal{D}_m \cong T^{m+1}$.

In view of the above claim (together with the well known description of the prime spectrum of a finite direct product of commutative rings and the fact that $\mathbb{F}_2$ has exactly one prime ideal), we see that R has exactly $m+1$ maximal ideals; that is, $n := |\mathrm{Max}(R)| = m+1$. Equivalently, $m = n-1$. As n depends only on (the ring isomorphism class of) R, the above proof shows that this conclusion applies to the length of *any* finite maximal chain of rings going from $\mathbb{F}_2$ to R.

It remains only to prove that $|[\mathbb{F}_2, R]| = \mathrm{B}_n$. As $n = m+1$, what was shown above provides a ring isomorphism $f : R \to T^n$. Necessarily, f is an $\mathbb{F}_2$-algebra isomorphism, and so by a standard homomorphism theorem, $|[\mathbb{F}_2, R]| = |[\mathbb{F}_2, T^n]|$. If $n = 1$, then $T = \mathbb{F}_2$, whence $|[\mathbb{F}_2, R]| = 1$. Since it follows easily from the definition of the Bell numbers that $\mathrm{B}_1 = 1$, this completes the proof of the assertion in case $n = 1$. Thus, we may suppose henceforth that $n \geq 2$. Then, since $\mathbb{F}_2$ is a field, [13, Proposition 4.15 (c)] ensures that $|[\mathbb{F}_2, T^n]| = \mathrm{B}_n$. The proof is complete. □

It is natural to ask to what extent Theorem 2.2 can be generalized if one omits the hypotheses that a given ring R has characteristic 2 or satisfies the condition "$\mathrm{U}(R) = \{1\}$". A first, positive step toward answering such questions is given in Proposition 2.3. One interesting consequence of Proposition 2.3 is that any minimal (ring) extension of a finite prime ring is a finite commutative ring.

Beginning with Proposition 2.3, we assume familiarity with the partitioning of the integral minimal ring extensions involving commutative rings into three classes: inert, decomposed, and ramified. A convenient source for that trichotomy is [26, Theorem 3.3]. It may be summarized as follows. Let $A \subset B$ be commutative rings forming an integral ring extension, with conductor $M := (A : B)$, and

put $K := A/M$. If $A \subset B$ is also a minimal ring extension, then $M \in \mathrm{Max}(A)$ (so that K is a field) and exactly one of the following three assertions holds: B/M is a minimal field extension of K (in which case, $A \subset B$ is said to be *inert*), B/M is K-algebra isomorphic to $K \times K$ (in which case, $A \subset B$ is said to be *decomposed*), B/M is K-algebra isomorphic to $K[X]/(X^2)$ (in which case, $A \subset B$ is said to be *ramified*).

Proposition 2.3. *Let R be a nonzero ring of characteristic $k > 0$, put $A := \mathbb{Z}/k\mathbb{Z}$, and view $A \subseteq R$ as usual. Then:*

(a) If $A \subset R$ is a minimal ring extension, then R is a finite commutative ring that is integral over A.

(b) Let the prime-power decomposition of k be $k = \prod_{i=1}^{s} q_i^{\alpha_i}$, where $q_1, \ldots, q_s$ are pairwise distinct prime numbers and each $\alpha_i \geq 1$. Using the Chinese Remainder Theorem, identify A with $\prod_{i=1}^{s} \mathbb{Z}/q_i^{\alpha_i}\mathbb{Z}$. Then $A \subset R$ is a minimal ring extension if and only if there exists a (necessarily unique) index j such that R is isomorphic to

$$(\prod_{i=1}^{j-1} \mathbb{Z}/q_i^{\alpha_i}\mathbb{Z}) \times B_j \times (\prod_{i=j+1}^{s} \mathbb{Z}/q_i^{\alpha_i}\mathbb{Z}),$$

where $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \subset B_j$ is a minimal ring extension. Assume henceforth that these equivalent conditions hold. Then $A \subset R$ is the same kind of minimal ring extension (that is, ramified, decomposed, or inert) as $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \subset B_j$. If $\alpha_j = 1$, then up to isomorphism, the number of ramified (resp., decomposed; resp., inert) candidates for B_j is 1, namely, $\mathbb{F}_{q_j}[X]/(X^2)$ (resp., 1, namely, $\mathbb{F}_{q_j} \times \mathbb{F}_{q_j}$; resp., $\aleph_0$, corresponding to the finite field extensions of prime vector-space dimension over $\mathbb{F}_{q_j}$ in some fixed algebraic closure of $\mathbb{F}_{q_j}$). If $\alpha_j \geq 2$, then up to isomorphism, the number of ramified candidates for B_j is finite and at least 2 (as small as 2 in some examples and larger than 2 in other examples). If $\alpha_j \geq 2$, then up to isomorphism, there is a unique decomposed candidate for B_j, namely, $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \times \mathbb{F}_{q_j}$, and there are no inert candidates for B_j.

Proof. (a) Pick $r \in R \setminus A$. Since A is generated as a cyclic additive group by $\{1\}$, A is contained in the center of R. It follows that the elements in the subring of R generated by $A \cup \{r\}$ are just the sums of powers of r (with 0 being the empty sum). As these elements clearly commute with each other, it follows that this subring is commutative. However, since $A \subset R$ is a minimal ring extension, this subring must be R. Thus, R is commutative. While the finiteness of R is a consequence of Lemma 2.1 (c), it should be noted that the special case of Lemma 2.1 (c) in which all the relevant rings are commutative can be proved without appealing to [22] or [21], by a simple application of [5, Proposition 7]. Indeed, [5, Proposition 7] ensures that the minimal ring extension $A \subset R$ is integral; and, whenever we have an integral minimal ring extension $D \subset E$ with D finite and E commutative, then E is algebra-finite over D, hence module-finite over D, hence finite.

(b) By (a), we can apply the relatively large amount that is known about commutative minimal ring extensions. The characterization of when $A \subset R$ is a minimal ring extension (in terms of the existence of a (necessarily unique) index

j and an associated minimal ring extension $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \subset B_j$ with certain behavior) follows from [7, Lemma 2.2], as does the assertion that $A \subset R$ is the same kind of minimal ring extension as $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \subset B_j$. In case $\alpha_j = 1$, the assertions about the candidates for B_j follow from [16, Lemme 1.2] (with support from the classical Galois theory of finite fields to explain why there are denumerably many isomorphism classes that have inert representatives). Suppose henceforth that $\alpha_j \geq 2$. Then $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z}$ is a special principal ideal ring (SPIR), but not a field. Hence, the assertions about the decomposed or inert candidates for B_j follow from [5, Propositions 10 and 8]. Finally (if $\alpha_j \geq 2$), the "finite and at least 2" assertion about the ramified candidates for B_j follows from [7, Theorem 3.4 (f)], while the "as small as 2" and "larger than 2" assertions follow from parts (e) and (f), respectively, of [5, Proposition 12]. The proof is complete. □

Despite the positive nature of Proposition 2.3 (which was able to use the theory of commutative ring extensions to detail the structure of the minimal ring extensions of any finite prime ring), the project of extending FMC-related themes from Theorem 2.2 in the absence of the "$\mathrm{U}(R) = \{1\}$" condition will hit a noncommutative roadblock in Example 2.5. Circumventing that roadblock will require a tweaking of the FMC property. That will ultimately lead to the desired analogues of Theorem 2.2 in Corollaries 2.10 and 2.11, which will be preceded by the fundamental Theorem 2.7 and other applications in Corollaries 2.8 and 2.9. (The above results will be followed by Example 2.12, one of whose purposes is to provide some perspective to the role of Corollaries 2.10 and 2.11 in the overall theory of the rings of prime characteristic.) Before addressing the new variant of the FMC property that will be required for our journey, we give a far-ranging remark that collects eight comments about the above material.

Remark 2.4. (a) In the next two paragraphs, we offer our opinion about the ways in which Theorem 2.2 improves upon [19, Theorems 2.3 and 2.5]. First, recall that a significant part of [19, Theorem 2.3] can be stated as follows. Let $\mathfrak{S}$ be a nonempty set and $R := \mathcal{P}(\mathfrak{S})$. Then R is a finite Boolean ring $\Leftrightarrow \mathbb{F}_2 \subseteq R$ satisfies FIP $\Leftrightarrow \mathbb{F}_2 \subseteq R$ satisfies FCP; and if these equivalent conditions hold and $n := |\mathfrak{S}| \geq 2$, then $|[\mathbb{F}_2, R]| = \mathrm{B}_n$. Next, recall that [19, Theorem 2.5] can be stated as follows. If $\mathfrak{S}$ is a finite set with $2 \leq n := |\mathfrak{S}|$ and $R := \mathcal{P}(\mathfrak{S})$, then the maximal length of a (finite maximal) chain in $[\mathbb{F}_2, R]$ is $n - 1$.

We believe that the characterization of finite Boolean rings in Theorem 2.2 (a) improves [19, Theorem 2.3] in the following four ways. First, Theorem 2.2 is predicated more generally is that it does not assume that R takes the form $\mathcal{P}(\mathfrak{S})$ for some set $\mathfrak{S}$ (after all, some infinite Boolean rings are not isomorphic to a ring having that form). Second, another way that Theorem 2.2 is predicated more generally is that the condition "$\mathrm{U}(R) = \{1\}$" does not imply that R is commutative. Third, and perhaps most importantly, the (possibly unexpected) involvement of the FMC property in one of the equivalent conditions in Theorem 2.2 (a) gives a significant deepening of our understanding of the chain conditions, as we recalled above that FMC $\not\Rightarrow$ FCP. Fourth, the involvement of the "$\mathrm{U}(R) = \{1\}$" property in the statement of Theorem 2.2 allows us to view Theorem 2.2 (a) as a companion for results (such as the above-mentioned [9, Corollaries 2.10

and 2.5]) that characterize Boolean rings using conditions that avoid the explicit assumption of commutativity.

Recall that Theorem 2.2 (b) states that if R is a finite nonzero Boolean ring with $n := |\mathrm{Max}(R)|$, then each finite maximal chain of rings in $[\mathbb{F}_2, R]$ going from $\mathbb{F}_2$ to R has length $n-1$ and $|[\mathbb{F}_2, R]| = \mathrm{B}_n$. This improves the nontopological portion of [19, Theorem 2.5] that was stated above in the following two ways. First, and more importantly, Theorem 2.2 (b) establishes a kind of catenarian behavior for the poset $[\mathbb{F}_2, R]$ inasmuch as *every* finite maximal chain is shown to have length $n-1$ (whereas [19, Theorem 2.5] left open the question of whether some finite maximal chain could have length less than $n-1$). Second, as a final minor point, Theorem 2.2 (b) also handles the easy case $n = 1$ which was not addressed in [19, Theorem 2.5].

(b) In characterizing finite Boolean rings, one cannot delete either of the components of condition (4) in Theorem 2.2 (a). Indeed, on the one hand, if one deletes the requirement that $\mathrm{U}(R) = \{1\}$, then taking $R := \mathbb{F}_2[X]/(X^2)$ gives an example of a ring of characteristic 2 such that there exists a (finite) maximal chain of rings of length 1 going from $\mathbb{F}_2$ to R (since $\mathbb{F}_2 \subset R$ is a minimal ring extension) although R is not Boolean. On the other hand, if R is a ring of characteristic 2 such that $\mathrm{U}(R) = \{1\}$, there need not exist a finite maximal chain of rings going from $\mathbb{F}_2$ to R: consider, for instance, $R := \mathbb{F}_2[X]$.

(c) Consider the first step $R_0 = \mathbb{F}_2 \subset R_1$ of a chain satisfying condition (4) in the statement of Theorem 2.2 (a). Then (by using both parts of Theorem 2.2), R_1 is a finite Boolean ring with $|\mathrm{Max}(R_1)| = 2$. In fact, R_1 is isomorphic (as an $\mathbb{F}_2$-algebra, equivalently, as a ring) to $\mathbb{F}_2 \times \mathbb{F}_2$. More generally, if p is any prime number and R is a ring of characteristic p with no nonzero nilpotent elements such that $|\mathrm{Max}(R)| > 1$ and $\mathbb{F}_p \subset R$ is a minimal ring extension, then R is isomorphic (as an $\mathbb{F}_p$-algebra, equivalently, as a ring) to $\mathbb{F}_p \times \mathbb{F}_p$.

For a proof, note first that R is a commutative ring, by Proposition 2.3 (a). Therefore, since $\mathbb{F}_p$ is a field, it follows from [16, Lemme 1.2] that R is isomorphic to either $\mathbb{F}_p \times \mathbb{F}_p$ or $\mathbb{F}_p[X]/(X^2)$ or a minimal field extension of $\mathbb{F}_p$. The second (resp., third) of these possibilities can be rejected because $X + (X^2)$ is a nonzero nilpotent element of $\mathbb{F}_p[X]/(X^2)$ (resp., because R has more than one maximal ideal), and so the assertion follows by the process of elimination.

(d) A special role for $\mathbb{F}_2 \times \mathbb{F}_2$ was identified in (c). This ring also played a striking role in the above proof of Theorem 2.2 (b) (where it was denoted by T^2). In fact, this ring has played a couple of important roles in the theory of rings R satisfying $\mathrm{U}(R) = \{1\}$. For instance, it was shown in [9, Proposition 2.20 (c)] that $\mathbb{F}_2 \times \mathbb{F}_2$ is, up to isomorphism, the only (possibly noncommutative) ring R such that $\mathrm{U}(R) = \{1\}$ and R is a minimal ring extension of its prime subring. Another role for $\mathbb{F}_2 \times \mathbb{F}_2$ in that theory was identified in [9, Theorem 2.21 (c)]. We will identify quite a different kind of role for this ring in (g) below.

(e) For any nonzero finite Boolean ring R, the first conclusion in Theorem 2.2 (b) asserts that the poset $[\mathbb{F}_2, R]$ exhibits a kind of catenarity. One should not expect that kind of behavior in general, even when all the relevant rings are commutative and all the relevant ring extensions satisfy FMC. Examples illustrating this were given in [14, Propositions 6.9 and 7.4]. For instance, in [14,

Proposition 7.4], one finds an example of minimal ring extensions $A \subset C$ and $C \subset D$ (that are, respectively, inert and ramified) and a ring $B \in [A, D]$ such that $A \subset B$ is a (ramified) minimal ring extension and each maximal chain of rings going from B to D is finite but consists of several (at least one) ramified steps followed by an inert step.

(f) Let R be a nonzero ring, with prime subring A. If R is finite (and hence has positive characteristic), then $A \subseteq R$ certainly satisfies FIP. (So, according to Theorem 2.2, the finite Boolean rings can be characterized within that class by the property of having only one unit.) In fact, according to [10, Proposition V.1], if R is commutative and of positive characteristic, then $A \subseteq R$ satisfies FIP if and only if R is finite. Building on this result and other work in [10], it was shown in [11, Theorem 2.1] that the class of commutative rings R that are singly generated (in the sense that R can be generated as a ring by a set of the form $\{0, 1, r\}$) and are such that $A \subseteq R$ satisfies FIP can be partitioned into four mutually disjoint sets (one of which consists of the class of finite singly generated commutative rings). Most of the contribution of [11] was to elucidate the fourth of these sets, for which the analysis became quite delicate. As [11, Remark 2.2 (a)] explained, one consequence of [11, Theorem 2.1] is that $\mathbb{Z} \subset \mathbb{Z}[X]/(4X-2, 2X^2-X)$ satisfies FIP, while $\mathbb{Z} \subset \mathbb{Z}[X]/(4X-2)$ does not satisfy FIP. We suggest that it would be interesting to characterize all the (not necessarily commutative) rings R, with prime subring A, such that $A \subseteq R$ satisfies FIP.

(g) Once again, let R be a nonzero ring with prime subring A. By Theorem 2.2, if there exists a finite maximal chain of rings going from A to R, then R is a finite Boolean ring if and only if $A = \mathbb{F}_2$ and $\mathrm{U}(R) = \{1\}$. Of course, Zorn's Lemma ensures the existence of some (possibly infinite) maximal chain in $[A, R]$ with minimum element A and maximum element R. Typically, any such maximal chain is a proper subset of $[A, R]$. So, it seems natural to ask if matters become more tractable if one assumes that $A \subseteq R$ is an example of what has (for extensions involving commutative rings) been called a λ-extension (also known as a "chained extension"), that is, a ring extension $A \subseteq R$ such that $[A, R]$ is linearly ordered by inclusion. Let us agree to extend that terminology for ring extensions involving arbitrary rings. The results of studying this condition for maximal chains of length 2 are extensive and somewhat complicated: cf. [6, Corollaries 2.21 and 3.6]. However, thanks to the second conclusion in Theorem 2.2 (b), we can characterize the relevant finite Boolean rings very succinctly, as follows. Let R be a nonzero (possibly noncommutative) ring R such that $\mathbb{F}_2 \subseteq R$ is a λ-extension. Then: $\mathrm{U}(R) = \{1\}$ and there exists a finite maximal chain, $\mathbb{F}_2 = R_0 \subset \ldots \subset R_m = R$, in $[\mathbb{F}_2, R] \Leftrightarrow R$ is a finite Boolean ring $\Leftrightarrow R$ is isomorphic to either $\mathbb{F}_2$ or $\mathbb{F}_2 \times \mathbb{F}_2$.

For a proof, Theorem 2.2 and the first paragraph of (c) combine to reduce our task to showing the following: $\mathrm{U}(R) = \{1\}$ and $[\mathbb{F}_2, R] = \{R_i \mid 0 \leq i \leq m\}$ being a finite linearly ordered set implies that $m \leq 1$. Recall that R is isomorphic to the direct product of n copies of $\mathbb{F}_2$ and, by Theorem 2.2 (b), the prevailing hypothesis implies that $m = n - 1$ and $m + 1 = |[\mathbb{F}_2, R]| = \mathrm{B}_n$. Hence $n = \mathrm{B}_n$. However, it is easy to see from the definition of the Bell numbers that $\mathrm{B}_k > k$ for all $k \geq 3$. Therefore $n \leq 2$, and so $m \leq 1$, thus completing the proof.

(h) In view of the motivating comments in the Introduction, we wish to close this remark with the following self-contained proof that for any positive integer n, if R_1 is the direct product of n copies of $\mathbb{Z}/2\mathbb{Z}$ and R_2 is the power set of $\{1, 2, \ldots, n\}$, then $R_1 \cong R_2$. As usual, write $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Consider the function $f : R_1 \to R_2$ sending a typical n-tuple $(c_1, ..., c_n)$ to the set $\{i \mid 1 \leq i \leq n$ and $c_i = 1\}$. We will prove that f is a ring isomorphism. Since f is clearly a bijection, it remains only to show that f is a ring homomorphism. It is easy to see that $f(1) = 1$ and that f preserves multiplication. Thus, we need only observe that $f(u + v) = f(u) + f(v)$ where $u = (a_1, ..., a_n)$ and $v = (b_1, ..., b_n)$. This can be done by the following calculation (with Δ denoting symmetric difference):

$$f(u) + f(v) = f(u)\Delta f(v) =$$
$$\{i \mid 1 \leq i \leq n \text{ and either } (a_i = 1 \text{ and } b_i \neq 1) \text{ or } (b_i = 1 \text{ and } a_i \neq 1)\} =$$
$$\{i \mid 1 \leq i \leq n \text{ and } a_i + b_i \neq 0\} =$$
$$\{i \mid 1 \leq i \leq n \text{ and } a_i + b_i = 1\} = f(u + v).$$

This completes Remark 2.4.

The first example that was mentioned in Remark 2.4 (b) featured a finite commutative ring (namely, $\mathbb{F}_2[X]/(X^2)$) that is a minimal ring extension of $\mathbb{F}_2$. Moreover, Proposition 2.3 (a) ensures that if $\mathbb{F}_2 \subset R$ is a minimal ring extension, then R is a finite commutative ring. However, there do exist minimal ring extensions $A \subset R$ with A commutative and R noncommutative, for instance $\mathbb{C} \subset \mathbb{H}$, as noted in [15, page 3482]. It is also possible for a finite maximal chain of rings to go from $\mathbb{F}_2$ to a finite noncommutative ring. Example 2.5 identifies a finite noncommutative ring R that is of minimal cardinality with respect to the property that there exists a finite maximal chain of rings going from some commutative ring A to R. In that example, $A = \mathbb{F}_2$. The upshot will be that there is no positive counterpart of Proposition 2.3 (a) for maximal finite chains of length $m \geq 2$, as Example 2.5 specifies how to build a finite chain of any given length $m \geq 2$, consisting of minimal ring extensions, going from $\mathbb{F}_2$ to a noncommutative ring.

Example 2.5. Consider any integer $m \geq 2$. Then there exists a finite maximal chain of finite rings, $B_0 = A \subset \ldots \subset B_m = B$, such that B_0 and B_1 are commutative and B_m is noncommutative. For an example of such data in which $|B|$ is the minimum possible, take $m = 2$ and $A = \mathbb{F}_2$, with B the ring $\mathrm{U}_2(\mathbb{F}_2)$ of upper triangular 2×2 matrices over $\mathbb{F}_2$. A maximal chain of rings $\mathbb{F}_2 \subset B_1 \subset B_2 := \mathrm{U}_2(\mathbb{F}_2)$ going from $\mathbb{F}_2$ to $\mathrm{U}_2(\mathbb{F}_2)$ can be built using $B_1 := \{0, I, C, I + C\}$, where I is the 2×2 identity matrix and C is the 2×2 matrix whose only nonzero entry is $c_{11} = 1$. (In particular, in this example, $B_{m-1} \subset B$ is a minimal ring extension, B_{m-1} is commutative, and B is noncommutative.) To construct an example for any $m > 2$, it suffices to prolong the above chain by inductively choosing B_{i+1} to be any minimal ring extension of B_i, for $i = 3, 4, \ldots, m - 1$.

Proof. For the case $m = 2$, take $B_0 := A := \mathbb{F}_2$, $B_1 := \{0, I, C, I + C\}$ and $B_2 := \mathrm{U}_2(\mathbb{F}_2)$. View $A \subset B_2$ by identifying $\alpha \in A$ with the scalar matrix αI. Since $C^2 = C$, one checks easily that $(I + C)^2 = I + C$ and $C(I + C) = 0 = (I + C)C$. It follows that B_1 is the internal direct product of the (unital) rings

$\{0, C\}$ and $\{0, I+C\}$. Thus, $B_1 \cong \mathbb{F}_2 \times \mathbb{F}_2$, and so B_1 is a commutative ring, with $|B_1| = 4$. Also, $B_0 \subset B_1$ and $B_1 \subset B_2$ are each minimal ring extensions since the corresponding (additive) group-theoretic indexes are each prime numbers. (Indeed, by Lagrange's Theorem, $[B_2^+ : B_1^+] = |B_2|/|B_1| = 8/4 = 2$; similarly, $[B_1^+ : B_0^+] = 2$.) Next, note that B_2 is noncommutative. (For instance, C does not commute with the matrix in B_2 whose only nonzero entries are in the $(1,1)$ and $(1,2)$ positions. It will be useful later to note that, since C is not in the center of B_2, the ring $B_2 = \mathrm{U}_2(\mathbb{F}_2)$ is not an algebra over B_1; and that $|\mathrm{U}(B_2)| = 2$.) For the case $m > 2$, the iterative procedure described in the final sentence of the statement of this theorem is appropriate because each nonzero ring has a minimal ring extension [15, Remark 2.5].

It remains to explain why $\mathrm{U}_2(\mathbb{F}_2)$ is of minimum cardinality with respect to the announced property. For this, we can ignore rings of prime cardinality, as any such ring is commutative. Also, it is well known that any ring of characteristic 2 and cardinality 4 must be commutative. (In fact, up to isomorphism, such a ring must be one of $\mathbb{F}_4$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_2[X]/(X^2)$.) Hence, by Lagrange's Theorem, one only needs to show that if $\mathcal{R}$ is a ring of characteristic 3 and cardinality 6, then $\mathcal{R}$ is commutative. With $D := \{0, 1, 2\} := \mathbb{F}_3 \subset \mathcal{R}$ and $e \in \mathcal{R} \setminus D$, we have $\mathcal{R} = \{0, 1, 2, e, 1+e, 2+e\}$, which clearly must be commutative. The proof is complete. □

The above ring extension $\mathbb{F}_2 \subset B := \mathrm{U}_2(\mathbb{F}_2)$ was studied in [20, Example 2.13] to emphasize that B is a noncommutative ring with exactly three maximal subrings that are commutative. That kind of situation was studied more generally in [20, Theorem 4.23], but the minimality property of $|B|$ that was established in Example 2.5 does not seem to have been noted elsewhere.

Parts (a) and (b) of the next remark present a couple of examples in which the various roles that had been played by the number 2 in Example 2.5 are played by an arbitrary prime number p. Parts (c) and (b) of Remark 2.6 give two other methods for constructing noncommutative minimal ring extensions. Because we intend to seek analogues of Theorem 2.2 in which the earlier role of 2 in Theorem 2.2 will be played by an arbitrary prime number, the remark closes by explaining why we will tweak one of the concepts that we have been using.

Remark 2.6. (a) Let p be a prime number, let $\mathrm{U}_2(\mathbb{F}_p)$ be the ring of upper triangular 2×2 matrices over $\mathbb{F}_p$, and let C be the element of $\mathrm{U}_2(\mathbb{F}_p)$ whose only nonzero entry is $c_{12} = 1$. One variant of Example 2.5 considers the chain $A := B_0 := \mathbb{F}_p \subset B_1 \subset B_2 := \mathrm{U}_2(\mathbb{F}_p)$, where $B_1 := A + AC$. Since $C^2 = 0$, it is easy to see that B_1 is a commutative ring. However, B_1 is not contained in the center of B_2 (that is, B_2 is not a B_1-algebra) since C does not commute with the element of B_2 whose only nonzero entry is 1 in the $(1,1)$ position. Both $B_0 \subset B_1$ and $B_1 \subset B_2$ are minimal ring extensions since the corresponding (additive) group-theoretic indexes are $|B_1|/|B_0| = p^2/p = p$ and $|B_2|/|B_1| = p^3/p^2 = p$. Therefore, as in the proof of Example 2.5, we can, for any integer $m \geq 3$, by applying [15, Remark 2.5] $m-1$ times, construct $\{B_i \mid 0 \leq i \leq m\}$, an increasing (finite) maximal chain of rings, of length m, going from $\mathbb{F}_p = B_0$ to some (noncommutative) ring B_m such that B_1 is commutative (and of cardinality p^2),

B_2 is noncommutative (and of cardinality p^3), and $B_1 \subset B_2$ is a minimal ring extension.

(b) Once again, let p be a prime number and let $m \geq 3$. Another variant of Example 2.5 (and of (a)), still with $A := B_0 := \mathbb{F}_p$, features $B := \mathrm{U}_p(\mathbb{F}_p)$, the ring of upper triangular $p \times p$ matrices over $\mathbb{F}_p$. In this example, $B_1 := A + AC$, where C is the element of $\mathrm{U}_p(\mathbb{F}_p)$ whose only nonzero entry is $c_{1p} = 1$. Once again, since $C^2 = 0$, we see that B_1 is a commutative ring. Also, B_1 is not contained in the center of B since C does not commute with the element of B whose only nonzero entry is 1 in the $(1,1)$ position. In addition, $B_0 \subset B_1$ is a minimal ring extension since its (additive) group-theoretic index is $|B_1|/|B_0| = p^2/p = p$. However (in contrast with the situation in (a)), there is no reason to believe that $B_1 \subset B$ is a minimal ring extension if $p > 2$, since its (additive) group-theoretic index is then $p^{(p^2+p-4)/2}$, which is not a prime number. Nevertheless, since B is finite, there exists an increasing finite maximal chain $\mathcal{C} = \{B_i \mid 0 \leq i \leq \mu\}$, of length $\mu \geq 3$ (possibly $\mu > m$), going from $\mathbb{F}_p$ to $B_\mu = B$. Hence, there exists j, with $2 \leq j \leq \mu$, such that B_{j-1} is commutative, B_j is noncommutative, and $B_{j-1} \subset B_j$ is a minimal ring extension. Of course, if $m > \mu$, one can apply [15, Remark 2.5] $m - \mu$ times to augment $\mathcal{C}$ to a finite maximal chain of length m.

(c) Example 2.5, together with its variants in (a) and (b), used matrices, with an emphasis on producing a minimal ring extension whose "bottom" ring is commutative and whose "top" ring is noncommutative. The example in (b) featured a "top" ring whose cardinality was not easily determined. (It was at most $p^{(p^2+p)/2}$.) If one does not mind a "top" ring that is "large," there is a quick way to produce examples of minimal ring extensions whose "bottom" and "top" ring are both "large." This method uses matrices, but not as in Example 2.5 or its variants in (a) and (b). Indeed, if $R \subset S$ is any minimal ring extension and $n \geq 2$, then $M_n(R) \subset M_n(S)$ is a minimal ring extension whose "bottom" ring is noncommutative and whose "top" ring has cardinality $|S|^{n^2}$. (As usual, $M_n(\Lambda)$ denotes the ring of all $n \times n$ matrices with entries in a ring Λ.) This result and its converse were proved in [2, Corollary].

(d) Another way to produce an example of noncommutative rings $\Lambda \subset \Gamma$ forming a minimal ring extension is the following. Let $A \subset B$ be any minimal ring extension and let R be any noncommutative ring. Put $\Lambda := R \times A$ and $\Gamma := R \times B$. Then Λ and Γ inherit noncommutativity from R. Moreover, one checks easily that if $\xi \in \Gamma \setminus \Lambda$, then the ring, say Ω, generated by $\Lambda \cup \{\xi\}$ is Γ. (In detail, since $R \times 0 \subseteq \Lambda \subseteq \Omega$, it suffices to show that $0 \times B \subseteq \Omega$. Write $\xi = (r, b)$, with $r \in R$ and $b \in B \setminus A$. Therefore, since the minimality of $A \subset B$ ensures that the ring generated by A and b is B, it suffices to prove that $(0, b) \in \Omega$ and $0 \times A \subseteq \Omega$. We have $(0, b) = (0, 1)\xi \in \Lambda\Omega \subseteq \Omega$. Finally, $0 \times A = (0, 1)\Lambda \subseteq \Lambda^2 = \Lambda \subseteq \Omega$.) Consequently, $\Lambda \subset \Gamma$ is a minimal ring extension.

Similarly, one can show that if R and S are rings and $\Lambda \subset \Gamma$ is a minimal ring extension, then $R \times \Lambda \times S \subset R \times \Gamma \times S$ is a minimal ring extension. This observation has been of enormous use in studying minimal ring extensions that involve (especially finite) commutative rings, because a commutative ring extension of a finite direct product of n nonzero rings is isomorphic to a direct product

of commutative ring extensions of the given n direct factors (cf. [7, Lemma 2.2]). Unfortunately, no such description of minimal ring extensions is possible for noncommutative rings. For instance, the ring $B_2 = \mathrm{U}_2(\mathbb{F}_2)$ in Example 2.5 is not expressible as a nontrivial direct product of rings, although it is a minimal ring extension of $B_1 = \{0, C\} \times \{0, I + C\}$ ($\cong \mathbb{F}_2 \times \mathbb{F}_2$). Significantly, B_2 is not a B_1-algebra. Because of such examples, we will next introduce a variant of the FMC property. That variant will require the "top" step in any relevant finite maximal chain to be an algebra. Upshots of using that variant will include a partial generalization of Theorem 2.2 to certain rings having arbitrary characteristic, as well as characterizations of some important classes of commutative rings. This completes the remark.

Our next main goal is to obtain a positive counterpart of Theorem 2.2 for finite maximal chains of arbitrary (finite) length without assuming the "$\mathrm{U}(R) = 1$" condition. To accomplish that goal, it will be necessary to modify some of the other ambient conditions. As we saw in the proof of Example 2.5 that the ring $\mathrm{U}_2(\mathbb{F}_2)$ has exactly two distinct units, it seems unlikely that it would be fruitful to replace "$\mathrm{U}(R) = 1$" with some sort of "smallness" condition on $\mathrm{U}(R)$. Instead, we will proceed by modifying the FMC property. A clue as to how that modification should be defined comes from the observation that was made in the proof of Example 2.5 that (the data in Example 2.5 are such that) B_2 is not a B_1-algebra. In other words, B_1 is not contained in the center of B_2.

This paragraph will introduce the modifications of the FMC concept that will (to some extent) allow us to generalize Theorem 2.2 to certain finite rings of arbitrary prime characteristic that need not satisfy the "$\mathrm{U}(R) = 1$" condition. These modifications will allow us to extend, to a noncommutative context, most of the conclusions of [7, Lemma 2.2], a result that has played key roles in the proofs of Theorem 2.2 and Proposition 2.3. As noted above, the following definitions are motivated by the fact that B_2 was not a B_1-algebra in Example 2.5. Let $A \subseteq B$ be rings. We will say that $A \subseteq B$ satisfies AFMC (for "Adjusted FMC") if there exists (in $[A, B]$) a finite maximal increasing chain of rings going from A to B whose last step $B_{m-1} \subset B$ is such that B is a B_{m-1}-algebra. If the number of steps in such a chain is relevant, we will say, for an integer $m \geq 0$, that $A \subseteq B$ satisfies m-AFMC if there exists a finite maximal chain (in $[A, B]$), $A = B_0 \subset \ldots \subset B_m = B$, such that B is a B_{m-1}-algebra, and we will call any such chain an m-AFMC *chain* (*going from A to B*). Some conclusions about these new concepts are clear. For instance, $A \subseteq B$ satisfies AFMC if and only if $A \subseteq B$ satisfies m-AFMC for some $m \geq 0$. Similarly, when one defines the m-FMC property in the obvious way, one has that $A \subseteq B$ satisfies FMC if and only if $A \subseteq B$ satisfies m-FMC for some $m \geq 0$. Of course, m-AFMC $\Rightarrow$ m-FMC, and so AFMC $\Rightarrow$ FMC. However, as Example 2.5 shows, FMC $\not\Rightarrow$ AFMC; in fact, 2-FMC $\not\Rightarrow$ AFMC.

A less trivial fact (which is central to the reason that we have introduced the AFMC property) is that if $A \subseteq B$ satisfies m-AFMC (for some m), then B is a commutative ring. (Here is a quick proof. By focusing on the last step in an m-AFMC chain going from A to B, it is enough to prove that if $A \subset B$ is a

minimal ring extension and B is an A-algebra (and A is commutative), then B is commutative. This, in turn, can be easily proved by adapting the first six sentences of the proof of Proposition 2.3 (a).) Though easy, this fact is useful. For instance, it shows that the AFMC property remedies a feature of the FMC property that was revealed by Example 2.5. Indeed, the data in Example 2.5 were such that $B_1 \subset B_2$ is a minimal ring extension (and hence satisfies 1-FMC) and B_1 is commutative but B_2 is noncommutative. In a sense, AFMC is the natural variant of FMC that should be studied by those who are (primarily but not exclusively) interested in commutative rings, as it is now clear that if $A \subseteq B$ are commutative rings, then $A \subseteq B$ satisfies m-AFMC (if and) only if $A \subseteq B$ satisfies m-FMC.

The next result is formulated in terms of finite rings because we wish to avoid discussing integrally closed minimal ring extensions here. Recall that if $A \subseteq B$ are finite commutative rings, then B is integral over A. (For a variety of proofs of this fact, see [17, Theorem 2.1], [25, Theorem XIII.1], [7, Proposition 2.1].)

Theorem 2.7. *Let R be a nonzero ring of characteristic $k > 0$ and view $\mathbb{Z}/k\mathbb{Z} \subseteq R$ as usual. Then:*

(a) If A is a subring of R such that $A \subseteq R$ satisfies m-AFMC for some $m \geq 0$, then R is a commutative ring.

(b) If A is a finite subring of R such that $A \subseteq R$ satisfies m-AFMC for some $m \geq 0$, then R is a finite commutative ring.

(c) Let the prime-power decomposition of k be $k = \prod_{j=1}^{s} q_j^{\alpha_j}$, where $q_1, \ldots, q_s$ are pairwise distinct prime numbers and each $\alpha_j \geq 1$. Using the Chinese Remainder Theorem, identify $A = \mathbb{Z}/k\mathbb{Z} = \prod_{j=1}^{s} \mathbb{Z}/q_j^{\alpha_j}\mathbb{Z} \subseteq R$. Suppose that $A \subseteq R$ satisfies m-AFMC, with $A = R_0 \subset \ldots \subset R_m = R$ an m-AFMC chain. (So, by (b), R is a finite commutative ring.) Then $|\mathrm{Max}(R)| \leq s + m$. If $0 \leq \nu \leq m$, then $|\mathrm{Max}(R)| = s + \nu$ if and only if exactly ν of the steps of the form $R_{i-1} \subset R_i$ are decomposed (minimal ring) extensions (and the other $m - \nu$ steps of the form $R_{i-1} \subset R_i$ are ramified or inert (minimal ring) extensions). In particular, $|\mathrm{Max}(R)| = s + m$ if and only if $R_{i-1} \subset R_i$ is a decomposed extension for all $i = 1, \ldots, m$. Also, R has no nonzero nilpotent elements if and only if $\alpha_1 = \cdots = \alpha_s = 1$ and each step ($R_{i-1} \subset R_i$ for $1 \leq i \leq m$) is either decomposed or inert.

Proof. (a) This assertion was proved in the above comments.

(b) By (a), we need only prove that R is finite. By induction on m, we may assume that $A \subset B$ is a minimal ring extension. Then an application of Proposition 2.3 (a) shows that R is finite.

(c) For each $j \in \{1, \ldots, s\}$, the ring $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z}$ has a unique prime ideal, hence a unique maximal ideal. Since A has been identified with the direct product of these s rings, $|\mathrm{Max}(R_0)| = |\mathrm{Max}(A)| = s$. Therefore, to prove the first of the four assertions in (c), namely that $|\mathrm{Max}(R)| \leq s + m$, it will be enough to show that if $0 \leq i \leq m - 1$, then

$$|\mathrm{Max}(R_i)| \leq |\mathrm{Max}(R_{i+1})| \leq |\mathrm{Max}(R_i)| + 1.$$

For each i, R_i is a finite (hence Artinian) commutative ring, and so a standard result (cf. [3, Theorem 8.7]) ensures that R_i is (apart from the ordering of the factors) uniquely expressible as an internal direct product of finite local (nonzero) rings $R_{i\lambda}$, where λ ranges over some finite index set Γ_i depending on i. It is evident that $|\mathrm{Max}(R_i)| = |\Gamma_i|$. Thus, to prove the above-displayed inequality, it is enough to show that when R_{i+1} is expressed as a direct product of (finite nonzero) local rings, the number of factors appearing in that direct product description is either the same as or one more than the number of factors appearing in the corresponding description of R_i as a direct product.

Since $R_i \subset R_{i+1}$ is a minimal ring extension involving commutative rings, it follows from [7, Lemma 2.2] that we can (up to isomorphism) compare those two descriptions. In fact, to pass from the direct product description of R_i to the corresponding description of R_{i+1}, one simply replaces one of the factors $R_{i\lambda}$ with a minimal ring extension of it, say E. As R_{i+1} is a finite commutative ring, $R_i \subset R_{i+1}$ is an integral extension, and it follows that $R_{i\lambda} \subset E$ is also an integral extension. Moreover, by [7, Lemma 2.2], $R_{i\lambda} \subset E$ is the same kind of minimal ring extension (that is, either inert, ramified or decomposed) as $R_i \subset R_{i+1}$. As $R_{i\lambda}$ has a unique maximal ideal, it is well known (cf. [10, Corollary II. 2]) that the number of maximal ideals of E is 1 (resp., 1; resp, 2) if $R_{i\lambda} \subset E$ is inert (resp., ramified; resp., decomposed). This completes the proof that $|\mathrm{Max}(R)| \leq s + m$.

We turn to the second assertion in (c), namely that if $0 \leq \nu \leq m$, then $|\mathrm{Max}(R)| = s + \nu$ if and only if exactly ν of the steps of the form $R_{i-1} \subset R_i$ are decomposed extensions. (The parenthetical part of that assertion will then follows by the process of elimination.) The above argument showed that the function f given by $f(i) := |\mathrm{Max}(R_i)|$ satisfies $f(0) = s$ and $f(i) \leq f(i+1) \leq f(i) + 1$ whenever $0 \leq i \leq m-1$; and that $f(i+1) = f(i) + 1$ if and only if the minimal ring extension $R_i \subset R_{i+1}$ is decomposed. Hence,

$$|\mathrm{Max}(R)| - s = |\mathrm{Max}(R)| - |\mathrm{Max}(A)| = \sum_{i=0}^{m-1} (|\mathrm{Max}(R_{i+1})| - |\mathrm{Max}(R_i)|)$$

is the number of steps $R_i \subset R_{i+1}$ that are decomposed. The assertion follows.

Since the "In particular" assertion in (c) is just the special case of the third assertion where $\nu = m$, we turn to the final assertion. Note that if R has no nonzero nilpotent elements, then the same is true of A and, *a fortiori*, also true of each $\mathbb{Z}/q_j^{\alpha_j}\mathbb{Z}$. Thus, without loss of generality, $\alpha_1 = \cdots = \alpha_s = 1$. Then $A = \prod_{j=1}^{s} \mathbb{F}_{q_j}$, a finite direct product of fields. Certainly, R_0 has no nonzero nilpotent elements. Thus, R has at least one nonzero nilpotent element if and only if there exists a necessarily unique index μ, $0 \leq \mu \leq m-1$, such that R_μ has no nonzero nilpotent elements and $R_{\mu+1}$ has a nonzero nilpotent element. Using the notation that was introduced above, we see, thanks to the Ferrand-Olivier classification [16, Lemme 1.2], that in each of the μ passages from R_0 to R_1, from R_1 to R_2, ..., and from $R_{\mu-1}$ to R_μ, what has happened (up to isomorphism, for $t = 0, \ldots, \mu - 1$) is the replacement of a field $R_{t\lambda}$ with a minimal ring extension of $R_{t\lambda}$ which is either a field or a direct product of two fields and that, in the passage from R_μ to $R_{\mu+1}$, some field $F := R_{\mu\lambda}$ has (up to isomorphism) been

replaced with $F[X]/(X^2)$. In other words, R has at least one nonzero nilpotent element if and only if there exists a necessarily unique index μ, $0 \leq \mu \leq m-1$, such that each of the first μ steps in the increasing m-AFMC chain going from A to R is either inert or decomposed and the step $R_\mu \subset R_{\mu+1}$ is ramified. This completes the proof. □

The next three corollaries use the m-AFMC property to give characterizations of some prominent kinds of finite commutative rings.

Corollary 2.8. *Let p be a prime number and let R be a (necessarily nonzero) ring of characteristic p. View $\mathbb{F}_p \subseteq R$ as usual. Then:*

(a) Let m be a non-negative integer. Then the following two conditions are equivalent:

(1) R is a (not necessarily commutative) integral domain and $\mathbb{F}_p \subseteq R$ satisfies m-AFMC*;*

(2) $R \cong \mathbb{F}_{p^{q_1 \cdot \cdots \cdot q_m}}$, for some finite list of prime numbers $q_1, \ldots, q_m$ (possibly with $q_i = q_j$ for some $i \neq j$).

(b) The following three conditions are equivalent:

(i) R is a (not necessarily commutative) integral domain and $\mathbb{F}_p \subseteq R$ satisfies FCP*;*

(ii) R is a (not necessarily commutative) integral domain and $\mathbb{F}_p \subseteq R$ satisfies AFMC*;*

(iii) R is a finite field.

Proof. (a) (1) ⇒ (2): Assume (1), with $\mathbb{F}_p = R_0 \subset \ldots \subset R_m = R$ an m-AFMC chain. By Theorem 2.7 (b), R is a finite commutative integral domain. Therefore, the same is true of each R_i. Hence, each R_i is a finite field. Also, if $1 \leq i \leq m$, the minimal ring extension $R_{i-1} \subset R_i$ is a minimal field extension, whose vector space dimension is necessarily (by the classical Galois theory of finite fields) a prime number, say q_i. Then for each i, $|R_i| = p^{q_1 \cdot \cdots \cdot q_i}$, and (2) follows.

(2) ⇒ (1): Assume (2). It follows easily from a standard homomorphism theorem that if A and B are rings of characteristic p such that $A \cong B$ and $\mathbb{F}_p \subseteq A$ satisfies m-AFMC, then $\mathbb{F}_p \subseteq B$ satisfies m-AFMC. Thus, without loss of generality, we can assume that $R = \mathbb{F}_{p^{q_1 \cdot \cdots \cdot q_m}}$. We need only prove that $\mathbb{F}_p \subseteq R$ satisfies m-AFMC. To do so, we need only produce an m-AFMC chain going from $\mathbb{F}_p$ to R. That, in turn, can be done as follows: whenever $1 \leq i \leq m$, define

$$R_i := \mathbb{F}_{p^{q_1 \cdot \cdots \cdot q_i}}.$$

Indeed, as we saw above whenever $1 \leq i \leq m$, $R_{i-1} \subset R_i$ is a q_i-dimensional vector space extension of (finite) fields, hence a minimal field extension, hence a minimal ring extension.

(b) (i) ⇒ (ii): Assume (i). As FCP ⇒ FMC, it follows from Lemma 2.1 (d) that R is finite and, for some non-negative integer m, there exists a finite maximal chain $\mathcal{C}$, of length m, of rings going from $\mathbb{F}_p$ to R. As R is a finite integral domain, it is a division ring. (For the sake of completeness, we include a familiar proof of this fact. It suffices to show that each nonzero element $r \in R$ has a left inverse u and right inverse v in R (for then $u = v$ and $r \in \mathrm{U}(R)$). The existence of u (resp., v) is a consequence of the Pigeonhole Principle, as right (resp., left)

multiplication by r is an injective, hence surjective, self map of R.) Therefore, by a celebrated theorem of Wedderburn, R is a (finite) field. In particular, R is commutative. Thus $\mathcal{C}$ is an m-AFMC chain, whence $\mathbb{F}_p \subseteq R$ satisfies AFMC.

(ii) $\Rightarrow$ (iii): Assume (ii). Then there exists a non-negative integer m such that $\mathbb{F}_p \subseteq R$ satisfies m-AFMC. Hence, (iii) follows from the implication (1) $\Rightarrow$ (2) that we proved in (a).

(iii) $\Rightarrow$ (i): It suffices to prove that if A is any nonzero ring of characteristic $k > 0$, then $\mathbb{Z}/k\mathbb{Z} \subseteq A$ satisfies FCP. While this is intuitively clear, we give a formal proof of it. Suppose that the assertion fails. Then there exists an infinite chain $\mathcal{C}$ in $[\mathbb{Z}/k\mathbb{Z}, A]$. We can write $\mathcal{C} = \{A_\lambda \mid \lambda \in \Lambda\}$ for some (infinite) index set Λ such that $A_\mu \neq A_\nu$ whenever $\mu \neq \nu$ in Λ. Then $\{|A_\lambda| \mid \lambda \in \Lambda\}$ is an infinite subset of the finite set $\{z \in \mathbb{Z} \mid 1 \leq z \leq 2^k\}$, the desired contradiction. □

The appearance of the FCP property in the statement of Corollary 2.8 (b) was made possible by the result of Wedderburn stating that every finite division ring is a field. This theorem of Wedderburn is widely regarded as the gateway to the study of commutativity results in associative ring theory (cf. [18, Chapter 3]), and [1] surveyed more than 20 proofs of it. However, Example 2.5 has revealed a fundamental inadequacy of FCP and we wish to avoid future asides considering commutativity issues as we move beyond the class of finite fields. Accordingly, the FCP property will not be mentioned in the next two corollaries.

Commutative semisimple rings can be characterized as the rings that are isomorphic to finite direct products of fields. This characterization can be deduced from the direct product structure theorem for Artinian rings [3, Theorem 8.7] that was used in the proof of Theorem 2.7 (c). (It can also be obtained as a corollary of Artin-Wedderburn theory.) In particular, a finite commutative ring is semisimple if and only if it is isomorphic to a finite direct product of finite fields. The next result gives some AFMC-theoretic characterizations of these rings. While all the steps in the m-AFMC chains appearing in the proof of Corollary 2.8 (a) were inert (minimal ring) extensions, one of equivalent conditions in Corollary 2.9 allows steps in the relevant m-AFMC chains to be either decomposed or inert.

Corollary 2.9. *Let p be a prime number and let R be a (necessarily nonzero) ring of characteristic p. View $\mathbb{F}_p \subseteq R$ as usual. Then the following conditions are equivalent:*

*(1) There exist a non-negative integer m_1 and an m_1-*AFMC *chain, $\mathbb{F}_p = R_0 \subset \ldots \subset R_{m_1} = R$, going from $\mathbb{F}_p$ to R, such that each step $R_{i-1} \subset R_i$ of that chain is either inert or decomposed;*

*(2) There exists a non-negative integer m_2 such that $\mathbb{F}_p \subseteq R$ satisfies m_2-*AFMC *and R has no nonzero nilpotent elements;*

(3) R is isomorphic to a finite direct product of finite fields (of characteristic p);

(4) R is a finite commutative semisimple ring.

Proof. As noted above, the equivalence of (3) and (4) is well known.

(1) $\Leftrightarrow$ (2): This equivalence holds (and one can take $m_1 = m_2$), by the fourth assertion in Theorem 2.7 (c).

(1) $\Rightarrow$ (3): Assume (1). Next, observe that a minimal field extension of a finite field is a finite field. Therefore, as in the proof of Theorem 2.7 (c), we see that each R_i is a finite commutative ring that can be (apart from the ordering of the factors) uniquely expressed as an internal direct product of finite local (nonzero) rings $R_{i\lambda}$ (where λ ranges over some finite index set Γ_i depending on i); and in each of the m passages from R_0 to R_1, from R_1 to R_2, ..., and from R_{m-1} to R_m, what has happened (up to isomorphism, for $t = 0, \ldots, m-1$) is the replacement of a finite field $R_{t\lambda}$ with a minimal ring extension of $R_{t\lambda}$ which is either a finite field or a direct product of two finite fields. Therefore, for each $i = 0, \ldots, , m$, R_i is a finite direct product of (finitely many but) at least $i + 1$ finite fields. In particular, this is true of $R_{m_1} = R$.

(3) $\Rightarrow$ (1): Assume (3). By the second sentence in the proof that (2) $\Rightarrow$ (1) in the proof of Corollary 2.8, we can assume that $R = \prod_{j=1}^{d} K_j$, where each K_j is a finite field and $d \geq 1$. For each integer $e \geq 1$, it will be convenient to let T^e denote the direct product of e copies of $\mathbb{F}_p$. We use [16, Lemme 1.2] and [7, Lemme 2.2] to begin building the required m_1-AFMC chain with $d - 1$ decomposed steps,

$$R_0 = \mathbb{F}_p \subset R_1 := T^2 \subset \ldots \subset R_{d-1} := T^d.$$

Next, consider the field K_1. As it is a finite field of characteristic p, $K_1 \cong \mathbb{F}_{p^{f_1}}$ for some integer $f_1 \geq 1$. Without loss of generality, $K_1 = \mathbb{F}_{p^{f_1}}$. Let $q_1 \cdot \cdots \cdot q_{\mu_1}$ be the factorization of f_1 as a (possibly empty) product of finitely many prime numbers $q_1, \ldots, q_{\mu_1}$ (possibly with $q_i = q_j$ for some $i \neq j$). As in the proof of the implication (2) $\Rightarrow$ (1) in Corollary 2.8 (a), there is an μ_1-AFMC chain, say $\mathcal{C}_1$, going from $\mathbb{F}_p$ to K_1 such that each step of $\mathcal{C}_1$ is an inert (field) extension of finite fields. Similarly, for each $j = 2, \ldots, d$, there exists an AFMC chain, say $\mathcal{C}_j$, going from $\mathbb{F}_p$ to K_j such that each step of $\mathcal{C}_j$ is an inert (field) extension of finite fields.

Next, augment the above-displayed chain with a chain of length μ_1, whose i^{th} member is obtained by replacing the *first* direct factor (equal to $\mathbb{F}_p$) of T^d with the i^{th} member of $\mathcal{C}_1$. By [7, Lemma 2.2], each of the newly added μ_1 steps inherits (from the corresponding step of $\mathcal{C}_1$) the property of being an inert extension. Next, augment the chain that has been built thus far with a chain whose i^{th} member is obtained by replacing what had been the *second* direct factor (equal to $\mathbb{F}_p$) of T^d with the i^{th} member of $\mathcal{C}_2$. As before, [7, Lemma 2.2] ensures that each of the newly added steps of the augmented chain is inert. Iterate the process, ending with an augmentation with a chain whose i^{th} member is obtained by replacing what had been the d^{th} direct factor (equal to $\mathbb{F}_p$) of T^d with the i^{th} member of $\mathcal{C}_d$. As before, each newly added step is inert, by [7, Lemma 2.2]. The upshot is a finite maximal chain of rings, say $\mathcal{C}$, going from $\mathbb{F}_p$ to $\prod_{j=1}^{d} K_j = R$, whose first $d - 1$ steps are decomposed and whose subsequent steps are all inert. Hence, $\mathcal{C}$ is an AFMC chain of the kind required in (1). The proof is complete. □

The proof of the implication (3) $\Rightarrow$ (1) in Corollary 2.9 gave an algorithm that constructed a suitable m-AFMC chain by placing all its decomposed steps at the beginning of the chain and then followed those with all the inert steps. However, for "most" finite commutative semisimple rings R, there is "usually" more than

one suitable m-AFMC chain. For instance, if $R := \mathbb{F}_{p^2} \times \mathbb{F}_p \times \mathbb{F}_{p^2}$, the following 4-AFMC chain going from $R_0 = \mathbb{F}_p$ to $R_4 = R$ alternates its decomposed steps and its inert steps:

$$R_0 \subset R_0 \times R_0 \subset \mathbb{F}_{p^2} \times R_0 \subset \mathbb{F}_{p^2} \times R_0 \times R_0 \subset R.$$

Recall that a ring R is a finite Boolean ring if and only if R is isomorphic to a finite direct product of copies of $\mathbb{F}_2$. From that point of view, Corollary 2.10 can be seen as our second main result. It extends themes from the "finite Boolean ring" context of Theorem 2.2 (a) to finite rings of prime characteristic without an assumption having the flavor of "$\mathrm{U}(R) = \{1\}$." Perhaps more importantly, Corollary 2.10 (b) generalizes, to the context of arbitrary prime characteristic, the "catenarian" conclusion about length in Theorem 2.2 (b) (which had itself generalized an inequality in the "finite Boolean ring" context in [19, Theorem 2.5]). Recall from Remark 2.4 (e) that one should not expect that kind of catenarian behavior in general.

Corollary 2.10. *Let R be a nonzero ring of prime characteristic $p > 0$ and view $\mathbb{F}_p \subseteq R$ as usual. Then:*

(a) The following three conditions are equivalent:

(1) $\mathbb{F}_p \subseteq R$ satisfies m-AFMC, with an m-AFMC chain $\mathbb{F}_p = R_0 \subset \ldots \subset R_m = R$, each of whose steps $R_{i-1} \subset R_i$ is decomposed;

(2) $\mathbb{F}_p \subseteq R$ satisfies m-AFMC and $|\mathrm{Max}(R)| = m + 1$;

(3) R is isomorphic (as a ring, equivalently, as a vector space over $\mathbb{F}_p$) to a direct product of finitely many copies of $\mathbb{F}_p$.

(b) If the equivalent conditions in (a) hold and $n := |\mathrm{Max}(R)|$, then any finite maximal chain going from $\mathbb{F}_p$ to R (that is, any FMC *chain going from $\mathbb{F}_p$ to R; equivalently, any* AFMC *chain going from $\mathbb{F}_p$ to R) has length $m = n - 1$ and the number of subrings of R is B_n, the n^{th} Bell number.*

Proof. (a) (1) $\Leftrightarrow$ (2): This equivalence follows at once from the third assertion in Theorem 2.7 (c).

(1) $\Rightarrow$ (3): Assume (1). It now suffices to rework the proof of the implication (1) $\Rightarrow$ (3) in the proof of Corollary 2.9. First, using [7, Lemma 2.2] and [16, Lemme 1.2], change the phrase "either a finite field or a direct product of two finite fields" in that proof to "a direct product of two copies of $\mathbb{F}_p$." Then the argument allows us to conclude that R is isomorphic to a direct product of $m+1$ copies of $\mathbb{F}_p$.

(3) $\Rightarrow$ (1): Assume (3). We need only the first paragraph of the proof of the implication (1) $\Rightarrow$ (3) in the proof of Corollary 2.9. It suffices to rework that paragraph by changing the phrase "to begin building" to "to build."

(b) The parenthetical "equivalently" assertion holds because all the relevant rings are commutative. Next, it will be convenient, for each integer $e \geq 1$, to let T^e denote a direct product of e copies of $\mathbb{F}_p$. By (1), pick an m-AFMC chain going from $\mathbb{F}_p$ to R, each of whose steps is decomposed. Then, by combining [7, Lemma 2.2] and [16, Lemme 1.2], we can conclude that $R \cong T^{m+1}$.

We claim that each step in any maximal chain of rings going from $\mathbb{F}_p$ to R must be decomposed. This claim follows because of the essentially unique way

that a nonzero finite commutative ring can be expressed as a direct product of local rings (cf. [3, Theorem 8.7]). Indeed, if some step $R_{i-1} \subset R_i$ in such a chain were either inert or ramified, it would follow from [7, Lemma 2.2] and [16, Lemme 1.2] that some local direct factor of R would properly contain $\mathbb{F}_p$, which would contradict the above-mentioned uniqueness since $R \cong T^{m+1}$.

Now that the claim has been established, we can be brief. Apart from changing "$\mathbb{F}_2$" to "$\mathbb{F}_p$" ten times, the final two paragraphs of the proof of Theorem 2.2 (b) carry over *verbatim*, thus completing the proof. □

Next, by reworking some of the above material, we obtain some remarkable equivalences. As was the case in Corollary 2.10 (b), the m-AFMC and m-FMC properties are equivalent in the context of Corollary 2.11.

Corollary 2.11. *Let p be a prime number and let m be a non-negative integer. Let R be a nonzero ring satisfying the equivalent conditions in Corollary 2.10 (a). (In other words, let R be a ring that is isomorphic to a nonempty finite direct product of copies of $\mathbb{F}_p$.) Then the following three conditions are equivalent:*

(1) $\mathbb{F}_p \subseteq R$ satisfies m-FMC;

(2) $|\mathrm{Max}(R)| = m + 1$;

(3) $|[\mathbb{F}_p, R]| = B_{m+1}$.

Proof. By hypothesis, R is isomorphic to a direct product of d copies of $\mathbb{F}_p$, for some integer $d \geq 1$. Note that d is uniquely determined by R. (This can be seen via the uniqueness result [3, Theorem 8.7] or, more simply, by considering the dimension of R as a vector space over $\mathbb{F}_p$.) Let e be a non-negative integer such that $\mathbb{F}_p \subseteq R$ satisfies e-FMC. Define $f := |\mathrm{Max}(R)|$ and $g := |[\mathbb{F}_p, R]|$. By the proof of the implication (1) $\Rightarrow$ (3) in the proof of Corollary 2.10, we get $d = e + 1$, and so $e = d - 1$. Next, it is clear that $f = d$. Next, by Corollary 2.10 (b), $g = B_f$, and so $g = B_d$. It follows that g uniquely determines d (since B_n is a strictly increasing function of n). We will next prove the asserted equivalences by reformulating (1), (2) and (3) in terms of d.

We have that (1) holds if and only if $m = (e =)\ d - 1$. Also, (2) holds if and only if $m+1 = (f =)\ d$, that is, if and only if $m = d-1$. Finally, (3) $\Leftrightarrow B_{m+1} = g$ $(= B_d) \Leftrightarrow m + 1 = d \Leftrightarrow m = d - 1$. The proof is complete. □

In contrast to the behavior in Corollary 2.11, the next result presents an example that highlights a way in which the rings that are isomorphic to a finite direct product of copies of $\mathbb{F}_p$ are very special within the universe of finite commutative rings of prime characteristic p.

Example 2.12. Let p be a prime number. Then, with m denoting a non-negative integer, the following three properties are logically independent for finite commutative rings of characteristic p:

(i) $\mathbb{F}_p \subseteq R$ satisfies m-FMC;

(ii) $|\mathrm{Max}(R)| = m + 1$;

(iii) $|[\mathbb{F}_p, R]| = B_{m+1}$.

In other words, for finite commutative rings of characteristic p, none of the three properties (i), (ii), (iii) implies either of the other two properties.

Proof. We do not need six sets of data to prove the assertion. Indeed, each of the required six non-implications can be seen by taking $R := \mathbb{F}_{p^{16}}$, the finite field of cardinality p^{16}. (The interested reader is invited to construct more esoteric examples.) Indeed, for this R, we have $[\mathbb{F}_p, R] = \{\mathbb{F}_{p^j} \mid j \in \{1, 2, 4, 8, 16\}\}$. Hence, $|[\mathbb{F}_p, R]| = 5 = B_3 = B_{2+1}$. Moreover, since B_n is a strictly increasing function of n, it follows that 2 is the only value of m such that $|[\mathbb{F}_p, R]| = B_{m+1}$. Next, since R is a field, $|\mathrm{Max}(R)| = 1$, and so 0 is the only value of m such that $|\mathrm{Max}(R)| = m + 1$. Finally, since $[\mathbb{F}_p, R]$ is linearly ordered by inclusion (in this example), it is clear that $\mathbb{F}_p \subseteq R$ satisfies 4-FMC. Therefore, it remains only to show that $\mathbb{F}_p \subseteq R$ satisfies neither 0-FMC nor 2-FMC.

Of course, $\mathbb{F}_p \subseteq R$ does not satisfy 0-FMC, since $\mathbb{F}_p \subset R$. To complete the proof, we will show that if $\mathbb{F}_p \subseteq R$ satisfies m-FMC, then $m \neq 2$. Let $\mathbb{F}_p = R_0 \subset \ldots \subset R_m = R$ be an m-FMC chain going from $\mathbb{F}_p$ to R. Because of the essentially unique way that a nonzero finite commutative ring can be expressed as a direct product of local rings (cf. [3, Theorem 8.7]), it follows from the proof of Theorem 2.7 that each step $R_{i-1} \subset R_i$ must be an inert (minimal ring) extension. (Indeed, otherwise, it follows from [7, Lemma 2.2] and [16, Lemme 1.2] that the first step that is either decomposed or ramified would place a nonzero zero-divisor into R_m, contradicting the fact that R is a domain.) Consequently, each step $R_{i-1} \subset R_i$ is a minimal field extension, whose vector space dimension is necessarily a prime number, say q_i. If $m = 2$, then

$$p^{16} = |\mathbb{F}_{p^{16}}| = |R_1|^{q_2} = (|R_0|^{q_1})^{q_2} = p^{q_1 q_2},$$

whence $16 = q_1 q_2$, a contradiction (thanks to the uniqueness part of the Fundamental Theorem of Arithmetic). The proof is complete. □

Part (a) of our closing remark provides a generalization, to arbitrary prime characteristic, of another result that we gave earlier in characteristic 2. Remark 2.13 (b) is in the spirit of Remark 2.4 (b). Finally, Remark 2.13 (c) is in the spirit of the adage that all analogies between really different things break down at some point.

Remark 2.13. (a) By using Corollary 2.10, we can adapt the reasoning in Remark 2.4 (g) to prove the following result. Let p be a prime number. Let R be a nonzero (possibly noncommutative) ring R such that $\mathbb{F}_p \subseteq R$ is a λ-extension. Then there exists an AFMC chain, going from $\mathbb{F}_p$ to R, each of whose steps is a decomposed (minimal ring) extension if and only if R is isomorphic to either $\mathbb{F}_p$ or $\mathbb{F}_p \times \mathbb{F}_p$.

(b) One cannot delete either of the components of condition (2) in Corollary 2.10. Indeed, on the one hand, if one deletes the requirement that $\mathbb{F}_p \subseteq R$ satisfies m-AFMC, then taking $R := \mathbb{F}_p(X)$ (or $\mathbb{F}_p[X]/(X^2)$) gives a ring R that satisfies $|\mathrm{Max}(R)| = m + 1$ (for $m := 0$) but is not isomorphic to a direct product of finitely many copies of $\mathbb{F}_p$. On the other hand, if one deletes the requirement that $|\mathrm{Max}(R)| = m + 1$, then taking $R := \mathbb{F}_{p^2}$ gives a ring R such that $\mathbb{F}_p \subseteq R$ satisfies m-AFMC with $m := 1$, but is not isomorphic to a direct product of finitely many copies of $\mathbb{F}_p$.

(c) In closing, we address the fact that we chose the ring R in Example 2.12 to be a field. One knows from Corollary 2.11 that no ring illustrating the conclusion

of Example 2.12 could satisfy the equivalent conditions in Corollary 2.10 (a). In particular, no such ring could be a Boolean ring. Recall from [9, Corollary 2.10] that a (not necessarily commutative) ring A is a Boolean ring if and only if A is a von Neumann regular ring such that $\mathrm{U}(A) = \{1\}$. As Example 2.12 asserted, *i.a.*, the existence of certain rings R of prime characteristic $p > 2$, we could not choose an R such that $\mathrm{U}(R) = \{1\}$. Accordingly, we decided to choose R as a suitable von Neumann regular ring. Recall that a commutative ring R is a von Neumann regular ring if and only if R_M is a field for each $M \in \mathrm{Max}(R)$. In particular, a (quasi-)local commutative ring is von Neumann regular if and only if it is a field. That is why we decided to choose R to be the smallest field of characteristic p that illustrates all the assertions in Example 2.12, namely, $\mathbb{F}_{p^{16}}$. In case the given characteristic in Example 2.12 is $p = 2$, then the ring (field) R that we chose does have characteristic 2. Since the prescription of suitable rings R in Example 2.12 needed to be appropriate in any prime characteristic p, we believe that our choice of R pushed the analogy as far as possible and, in case $p = 2$, came "close" to satisfying the "$\mathrm{U}(A) = \{1\}$" condition.

References

1. M. Adam and B. J. Mutschler, *On Wedderburn's Theorem about finite division algebras*, unpublished manuscript, 2003.
2. N. Al-Kuleab and N. Jarboui, *A note on intermediate matrix rings*, Far East Journal Math. Edu. **17** (4) (2018), 227-229.
3. M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, MA, 1969.
4. P. J. Cahen, D. E. Dobbs and T. G. Lucas, *Finitely valuative domains*, J. Algebra Appl. **11** (6) (2012), 1250112, 39 pages; DOI: 10.1142/S0219498812501125.
5. D. E. Dobbs, *On the commutative rings with at most two proper subrings*, Int. J. Math. Math. Sci., volume 2016, Article ID 6912360, 13 pages, 2016. doi:10.1155/2016/6912360.
6. D. E. Dobbs, *Certain towers of ramified minimal ring extensions of commutative rings*, Comm. Algebra **46** (8) (2018), 3461-3495; DOI: 10.1080/00927872.2017.1412446.
7. D. E. Dobbs, *A minimal ring extension of a large finite local prime ring is probably ramified*, J. Algebra Appl. **19** (1) (2020), 2050015 (27 pages); DOI: 10.1142/S0219498820500152.
8. D. E. Dobbs and N. Jarboui, *Normal pairs of noncommutative rings*, Ric. Mat. **69** (1) (2020), 95-109; DOI: 10.1007/s11587-019-00450-2.
9. D. E. Dobbs and N. Jarboui, *Associative rings in which 1 is the only unit*, Pales. J. Math. **9** (2) (2020), 604-619.
10. D. E. Dobbs, B. Mullins, G. Picavet and M. Picavet-L'Hermitte, *On the FIP property for extensions of commutative rings*, Comm. Algebra **33** (9) (2005), 3091-3119.
11. 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.
12. D. E. Dobbs, G. Picavet and M. Picavet-L'Hermitte, *Characterizing the ring extensions that satisfy FIP or FCP*, J. Algebra **371** (2012), 391-429.
13. D. E. Dobbs, G. Picavet and M. Picavet-L'Hermitte, *Transfer results for the FIP and FCP properties of ring extensions*, Comm. Algebra **43** (2015), 1279-1316.
14. D. E. Dobbs, G. Picavet, M. Picavet-L'Hermitte and J. Shapiro, *On intersections and composites of minimal ring extensions*, JP J. Algebra, Number Theory and Appl. **26** (2) (2012), 103-158.
15. T. J. Dorsey and Z. Mesyan, *On minimal extensions of rings*, Comm. Algebra **37** (2009), 3463-3486.

16. D. Ferrand and J.-P. Olivier, *Homomorphismes minimaux d'anneaux*, J. Algebra **16** (1970), 461-471.
17. G. L. Ganske, Finite local rings, Ph. D. dissertation, Univ. of Oklahoma, Norman, OK, 1971.
18. I. N. Herstein, Noncommutative Rings, Math. Assn. America, Carus Monographs **15**, distributed by John Wiley and Sons, Inc., New York, 1968.
19. A. Jaballah and N. Jarboui, *From topologies of a set to subrings of its power set*, Bull. Aust. Math. Soc. **102** (1) (2020), 15-20.
20. O. A. S. Karamzadeh and N. Nazari, *On maximal commutative subrings of non-commutative rings*, Comm. Algebra **46** (12) (2018), 5083-5115.
21. A. A. Klein, *The finiteness of a ring with a finite maximal subring*, Comm. Algebra **21** (4) (1993), 1389-1392.
22. T. J. Laffey, *A finiteness theorem for rings*, Proc. Roy. Irish Acad. Sect. A **92** (2) (1992), 285-288.
23. J. Lewin, *Subrings of finite index in finitely generated rings*, J. Algebra **5** (1967), 84-88.
24. N. H. McCoy, The Theory of Rings, Macmillan, New York, 1964.
25. B. R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.
26. G. Picavet and M. Picavet-L'Hermitte, About minimal morphisms, pp. 369–386, In: Multiplicative Ideal Theory in Commutative Algebra (eds. J. W. Brewer, S. Glaz, W. Heinzer and B. Olberding), Springer-Verlag, New York, 2006.

[1] Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320
Email address: ddobbs1@utk.edu

[2] Department of Mathematics, College of Science, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia
Email address: njarboui@kfu.edu.sa

[3] Department of Mathematics, Faculty of Sciences, University of Sfax, P.O. Box 1171, Route Soukra, 3038 Sfax, Tunisia
Email address: noomenjarboui@yahoo.fr