Gulf Journal of Mathematics
Vol 12, Issue 2 (2022) 1-30

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v12i2.677

ON MINIMAL RING EXTENSIONS OF FINITE RINGS

DAVID E. DOBBS[1*]

Abstract. Two conditions, (i) and (ii), are defined, that may hold for a given (unital) ring extension $R \subset S$ of (unital, associative, not necessarily commutative) finite rings. It is shown that if S is commutative, "either (i) or (ii)" is necessary and sufficient for $R \subset S$ to be a minimal ring extension; and for such extensions, (i) and (ii) are logically independent. For extensions with S (finite and) noncommutative, "either (i) or (ii)" is neither necessary nor sufficient for $R \subset S$ to be a minimal ring extension; and for such minimal ring extensions, (i) and (ii) are logically independent. Let $R \subset S_j$ be minimal ring extensions with S_j (finite and) commutative (for $j = 1, 2$) and R local. Then: S_1 and S_2 are the same type (ramified, decomposed or inert) of minimal extension of $R \Leftrightarrow |Z(S_1)| = |Z(S_2)| \Leftrightarrow |U(S_1)| = |U(S_2)|$.

1. Introduction

All rings considered below are assumed to be associative and unital, but not necessarily commutative. 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 Λ is a ring, $\mathrm{Max}(\Lambda)$ denotes the set of all maximal (two-sided) ideals of Λ; $U(\Lambda)$ denotes the set of units (with both a left inverse and right inverse) of Λ; and if Λ is nonzero and commutative, $Z(\Lambda)$ denotes the set of zero-divisors of Λ. As usual, $|\mathcal{S}|$ denotes the cardinal number of a set $\mathcal{S}$; $\mathbb{F}_j$ denotes the finite field with cardinality j; $\subset$ denotes proper inclusion; and X denotes an indeterminate over the ambient ring(s). For rings $R \subseteq S$, $[R, S]$ denotes the set of intermediate rings, that is $\{T \mid T \text{ is a ring and } R \subseteq T \subseteq S\}$; and, following [18], we say that $R \subset S$ is a *minimal ring extension* if $|[R, S]| = 2$; that is, if $R \subset S$ and there does not exists a ring T such that $R \subset T \subset S$. The definition of a minimal ring extension in [18] stipulated that the rings R and S are commutative, but this concept has been extended and studied for arbitrary (that is, possibly noncommutative) rings in recent years, in papers such as [17] and [1].

As the title indicates, our interest here is in minimal ring extensions $R \subset S$ where R and S are finite rings. Actually, the finiteness of S follows from the other

Date: Received: Aug 11, 2021; Accepted: Dec 5, 2021.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 13B99, 16B99; Secondary 13M99, 13B21, 16P10, 12E20.

Key words and phrases. Minimal ring extension, finite ring, zero-divisor, integrality, Dorroh extension.

conditions. (This fact was recently proven in [11, Lemma 2.1 (c)] as a consequence of a deep noncommutative result on rng extensions, due independently to Klein [24] and Laffey [26].) The first result in Section 2 characterizes when commutative finite rings $R \subset S$ form a minimal ring extension. That characterization is "if and only if either (i) or (ii)," where (i) and (ii) are two conditions that may hold for any ring extension of arbitrary (that is, not necessarily commutative) finite rings. The definitions of (i) and (ii) take advantage of the finiteness of R and S by considering the number $d := \log_{|R/M|}(|S/M|)$ where M is a maximal ideal of R that is also an ideal of S. (The summary of information about commutative minimal ring extensions that is given in the next paragraph will explain why the existence of such $M \in \mathrm{Max}(R)$ is to be be expected, at least when $R \subset S$ is a minimal ring extension of commutative rings.) To be brief here (a longer summary will follow the next paragraph), most of Section 2 studies the extent to which minimal ring extensions $R \subset S$ satisfy (i) and/or (ii) when R (hence S) is finite but not necessarily commutative; and Section 3 develops other finite numbers (besides d), especially $|Z(S)|$ and $|U(S)|$, to see what sort of information they can provide about a minimal ring extension $R \subset S$ when R is commutative, local and finite.

This paragraph provides a focused summary of some of what is known about minimal ring extensions $R \subset S$ when S is commutative. We will ignore the topic of integrally closed minimal ring extensions because of the well known fact that if $R \subset S$ are finite commutative rings, then S is integral over R (cf. [27, Theorem XIII.1], [9, Proposition 2.1]). It follows from the above comments that every commutative minimal ring extension of a finite (commutative) ring must be finite (cf. also [7, Proposition 7]). The first classification result on minimal ring extensions was due to Ferrand-Olivier [18, Lemme 1.2]: if k is a field, then a nonzero commutative k-algebra B is a minimal ring extension of k (when we view $k \subseteq B$ via the injective structural map $k \to B$) if and only if B is k-algebra isomorphic to (exactly one of) $k[X]/(X^2)$, $k \times k$ or a minimal field extension of k. Now let $R \subset S$ be an integral ring extension with S commutative, and consider its conductor $M := (R : S)$ $(:= \{s \in S \mid sS \subseteq R\})$. A standard ring homomorphism theorem shows that $R \subset S$ is a minimal ring extension if and only if $R/M \subset S/MS$ $(= S/M)$ is a minimal ring extension. Thus (cf. also [18, Lemme 1.2 and Proposition 4.1], [13, Lemma II.3], [28]), for commutative rings $R \subset S$, the above-mentioned classification result of Ferrand-Olivier leads to the following trichotomy: $R \subset S$ is a (an integral) minimal ring extension if and only if M $(:= (R : S)) \in \mathrm{Max}(R)$ and (exactly) one of the following three conditions holds: $R \subset S$ is said to be respectively *ramified*, *decomposed*, or *inert* if S/MS $(= S/M)$ is isomorphic, as an algebra over the field $k := R/M$, to $k[X]/(X^2)$, $k \times k$, or a minimal field extension of k.

The characterization in Theorem 2.1 of minimal ring extensions $R \subset S$, where R is finite and S is commutative, uses descriptions of R and S as finite direct products of local rings. Requiring such descriptions is not a limitation when considering only finite commutative rings (cf. [2, Theorem 8.7]), but such a requirement would be too restrictive to accommodate a broad array of noncommutative ring

extensions. So, prior to the statement of Lemma 2.4, we reformulate conditions (i) and (ii) (which had appeared in the statement of Theorem 2.1) so that their new definitions are not connected to any supposed direct product descriptions of R and S. (For finite commutative rings $R \subset S$, these reformulations have no effect if R is local, while if R is not local, these reformulations have an insignificant effect, in view of [9, Lemma 2.2].) For commutative rings, Theorem 2.1 (together with the comments immediately following its proof) shows that that (i) and (ii) are logically independent (regardless of whether one considers their original versions or their reformulated versions). With the new formulations, the properties (i) and (ii) become meaningful for all ring extensions involving arbitrary (that is, possibly noncommutative) rings. From that point onward in Section 2 (aside from a few general observations), all rings are assumed to be finite but not necessarily commutative.

When venturing into a noncommutative setting, it seems reasonable (in view of [18, Théorème 2.2] and Theorem 2.1) to first consider the reformulated conditions (i) and (ii) in the context of ring extensions $R \subset S$ such that R is (finite,) commutative and local and S is (finite and) noncommutative. For that context, we find: in Corollary 2.5 that $R \subset S$ satisfying (ii) is a sufficient condition for $R \subset S$ being a minimal ring extension; in Example 2.6, by using a construction of George Bergman, a minimal ring extension satisfying both (i) and (ii) and another minimal ring extension satisfying (i) but not (ii); and in Example 2.7, by "twisting" multiplication with the help of an automorphism of $\mathbb{F}_4$, a minimal ring extension satisfying (ii) but not (i). Bridging toward a "wholly noncommutative" context, Remark 2.8 (d) shows that the much studied minimal ring extension $R \subset S$ from [11, Example 2.5], where R is a finite commutative ring with exactly two maximal ideals and S is a (finite) noncommutative ring, satisfies neither (i) nor (ii).

For the context of ring extensions $R \subset S$ with R noncommutative (and S finite), we find: in Example 2.9 (in the spirit of Example 2.6), by using a matricial result of Al-Kuleab and Jarboui [1], a minimal ring extension satisfying both (i) and (ii) and another minimal ring extension satisfying (i) but not (ii); in Example 2.10 (in the spirit of Example 2.8 (d)), by using upper triangular matrices, a minimal ring extension satisfying neither (i) nor (ii); and in Example 2.11 (in the spirit of Example 2.7), by using Dorroh extensions (in the sense of [17]), a minimal ring extension satisfying (ii) but not (i). Section 2 also contains a number of other analogous examples and a variety of remarks.

Returning to a "wholly commutative" (and "wholly finite") context, Section 3 examines the information conveyed by $|Z(R)|$ and $|Z(S)|$ (and, to a lesser extent, by $|U(R)|$ and $|U(S)|$) when (finite) commutative rings $R \subset S$ form a minimal ring extension. To simplify formulas, we also assume there that (R, M) is local. (In view of [9, Lemma 2.2 (b)], this assumption does not impose a significant reduction of generality.) As is well known, the "local" hypothesis implies that $|R| = p^\lambda$ for some prime number p and some integer $\lambda \geq 1$. For the context where $R \subset S$ is a minimal ring extension of finite commutative rings, the basic formulas for $|Z(R)|$ and $|Z(S)|$ can be found in Lemmas 3.1 and 3.5. While it is clear that $|Z(R)| = |Z(S)|$ if $R \subset S$ is inert, we show in Theorem 3.2

that if $R \subset S$ is either ramified or decomposed, then $|Z(S)| \geq p|Z(R)|$, with equality if and only if $R \subset S$ is ramified with $R/M \cong \mathrm{F}_p$. Also noteworthy (in Corollary 3.7) is the fact that, given two minimal ring extensions $R \subset S$ and $R \subset T$ (with both S and T finite and commutative and R local), one has the following: $R \subset S$ and $R \subset T$ are the same type (that is, ramified, decomposed or inert) of minimal ring extension $\Leftrightarrow |Z(S)| = |Z(T)| \Leftrightarrow |U(S)| = |U(T)|$. (For specific relevant inequalities, see Corollary 3.6 (c), (d).) Moreover, for a commutative minimal ring extension $(R, M) \subset S$, Corollary 3.9 establishes that $|Z(S/M)|/|Z(R/M)| = |Z(S)|/|Z(R)|$, with Corollary 3.10 giving the analogous result where the units operator $U(-)$ replaces the zero-divisor operator $Z(-)$.

Moving beyond the context of minimal ring extensions, Corollary 3.3 (b) gives the following application of Theorem 3.2. Let $(R, M) \subset (S, N)$ be (distinct) finite commutative local rings. Let (the positive integer) $\mathcal{L}$ be the maximal length of a (finite) chain of rings going from R to S. Then there exists an integer k with the following property. For any maximal chain of rings $\mathcal{C} : R = R_0 \subset \ldots \subset R_L = S$, of length L, going from R to S, we have $0 \leq k \leq L \leq \mathcal{L}$ and $|Z(S)| \geq p^{L-k}|Z(R)|$; moreover, under the stated conditions, $|Z(S)| = p^{L-k}|Z(R)|$ if and only if both of the following conditions hold: (1) the $L-k$ ramified steps in $\mathcal{C}$ are the initial $L-k$ steps as the chain $\mathcal{C}$ moves "upward" from R to S (so that the k inert steps in $\mathcal{C}$ are the final k steps as the chain $\mathcal{C}$ "approaches" and "reaches" S), and (2) if $k \neq L$, then $R/M \cong \mathbb{F}_p$. Furthermore, k is the number of prime factors (counting repeated factors with repetition) in the factorization of the integer $\dim_{R/M}(S/N)$ as a product of prime numbers.

As explained above, part of this article is intended to study rings that are not necessarily commutative in the spirit of some of the chain-theoretic work in [11]. We would hope that some readers of this journal would be especially interested in examining whether the code-theoretic work on certain finite commutative rings in [4] and/or the graph-theoretic work that had applications to certain finite commutative rings in [30] could also be extended to contexts involving some noncommutative rings.

Any unexplained material is standard, as in [2] and [22].

2. The characterization and some analogues

We begin with a characterization of the commutative minimal ring extensions of a finite commutative ring.

Theorem 2.1. *Let $R \subset S$ be (distinct) finite commutative rings. Then the following is a necessary and sufficient condition for $R \subset S$ to be a minimal ring extension: there exist rings $R_1 \subset S_1$ and a (possibly zero) ring B such that R is ring-isomorphic to $R_1 \times B$, S is R-algebra isomorphic to $S_1 \times B$, (R_1, M) is (quasi-)local, and the quantities $K := R_1/M$, $A := S_1/MS_1$, and $d := \dim_K(A)$ [equivalently, $d := \log_{|K|}(|A|)$] are such that*
either (i) $M \in \mathrm{Max}(S_1)$ and d is a prime number
or (ii) M is an ideal of S_1 and $d = 2$.

Moreover, if $R \subset S$ is a minimal ring extension, then: if $R \subset S$ is either ramified or decomposed, then (ii) holds and (i) does not hold; if $R \subset S$ is inert, then (i) holds; and if $R \subset S$ is inert, then (ii) holds if and only if $d = 2$.

Furthermore, if $R \subset S$ is a minimal ring extension (necessarily satisfying (i) and /or (ii)) then, once R and S have been identified with $R_1 \times B$ and $S_1 \times B$, respectively, as above, the above-mentioned ideal M (which is also mentioned in (i) and (ii)) is uniquely determined by the fact that the crucial maximal ideal of $R \subset S$ is $M \times B$.

Proof. As R and S are each finite commutative rings, they are each expressible as (essentially uniquely determined) finite direct products of (finite quasi-) local rings (cf. [2, Theorem 8.7]). In fact, by [9, Lemma 2.2 (b)], we can, without loss of generality, fix descriptions of R as $R_1 \times \cdots \times R_n$ and of S as $S_1 \times \cdots \times S_n$ for some local rings (R_i, M_i) and rings S_i such that $R_i \subseteq S_i$ for all $i = 1, \ldots, n$. It is clear that $R_j \subset S_j$ for at least one index j; and that a necessary condition for $R \subset S$ to be a minimal ring extension is that there cannot exist more than one such j. Thus, by relabeling if necessary, we can assume, without loss of generality, that $j = 1$, and then put $B := \prod_{i=2}^{n} R_i$ (with an empty direct product of rings being viewed as the zero ring, as usual), so that $R = R_1 \times B$ and $S = S_1 \times B$. By [9, Lemma 2.2 (b)], $R \subset S$ is a minimal ring extension if and only if $R_1 \subset S_1$ is a minimal ring extension. Put $M := M_1$, the unique maximal ideal of R_1.

Recall that $R \subset S$ is an integral ring extension (since S is a finite commutative ring). Suppose that $R \subset S$ is a minimal ring extension. Thus, it must be either ramified, decomposed or inert. By [9, Lemma 2.2 (b)], $R_1 \subset S_1$ is the same kind of minimal ring extension as $R \subset S$. Since R_1 is quasi-local, the crucial maximal ideal of $R_1 \subset S_1$ must be M, and so $M = (R_1 : S_1)$ by [18, Théorème 2.2]. It follows that M is an ideal of S_1, and so $A = S_1/M$. Suppose first that $R \subset S$ is either ramified or decomposed. Then A is K-algebra isomorphic to either $K[X]/(X^2)$ or $K \times K$, whence $|A| = |K|^2$ and $d = 2$, so that condition (ii) is satisfied. Suppose next that $R \subset S$ is inert; equivalently that $R_1 \subset S_1$ is inert. Then $M \in \mathrm{Max}(S_1)$ and $K \subset A$ is a minimal field extension. Hence, by the classical Galois Theory of finite fields, d is a prime number, and so condition (i) is satisfied.

We next prove that conditions (i) and (ii) are each sufficient to prove that $R \subset S$ (equivalently, that $R_1 \subset S_1$) is a minimal ring extension. Note that (i) and (ii) each imply that M is an ideal of S_1, whence $A = S_1/M$. Therefore, by a standard homomorphism theorem (cf. [13, Lemma II.3]), it will suffice to prove that $R_1/M = K \subset A = S_1/M$ is a minimal ring extension (for then $R_1 \subset S$ is a minimal ring extension, and hence so is $R \subset S$). If (i) holds, then A is a field, and then the sufficiency of (i) holds because of the standard fact (cf. [21, Exercise 1 (b), page 20]) that if $F \subset L$ are fields such that $\dim_F(L)$ is a prime number, then $F \subset L$ is a minimal field extension. Suppose next that (ii) holds. It will suffice to show that if T is a ring such that $K \subseteq T \subseteq A$, then T is either K or A. We have $1 = \dim_K(K) \leq \dim_K(T) \leq \dim_K(A) = 2$, so that either $\dim_K(T) = 1$ (in which case, $T = K$) or $\dim_K(T) = 2$ (in which case, $T = A$). This proves that (ii) is also sufficient.

We next prove the three statements in the "Moreover" assertion. In view of the earlier part of this proof, the first of those three statements follows from the fact that the "ramified," "decomposed" and "inert" properties are mutually exclusive; the second statement has been proved; and the "if" part of the third statement holds because $R_1 \subset S_1$ being an integral minimal ring extension implies that $M = (R_1 : S_1)$, which is an ideal of S_1. As the "only if" part of the third statement is trivial, the proof of the "Moreover" assertion is complete.

Lastly, we prove the "Furthermore" assertion. By [18, Théorème 2.2], the crucial maximal ideal of $R_1 \subset S_1$ is M and the crucial maximal ideal of $R \subset S$ is

$$(R : S) = (R_1 \times B, S_1 \times B) = (R_1 : S_1) \times B = M \times B.$$

The proof is complete. □

The "Moreover" assertion in Theorem 2.1 clarifies the logical relationship between the conditions (i) and (ii). In particular, neither (i) nor (ii) implies the other, and there exist minimal ring extensions that satisfy both (i) and (ii). Indeed, for arguably the simplest examples illustrating these conclusions, consider the following minimal ring extensions: the ramified (resp., decomposed) extension $\mathbb{F}_2 \subset \mathbb{F}_2[X]/(X^2)$ (resp., $\mathbb{F}_2 \subset \mathbb{F}_2 \times \mathbb{F}_2$) satisfies (ii) but not (i); the (inert) extension $\mathbb{F}_2 \subset \mathbb{F}_8$ satisfies (i) but not (ii), since its $d = 3$; and the (inert) extension $\mathbb{F}_2 \subset \mathbb{F}_4$ satisfies both (i) and (ii), since its $d = 2$.

The next two results consider the possible validity of the analogue of Theorem 2.1 for certain kinds of ring extensions $R \subset S$ where the base ring R may be infinite and S is still assumed to be commutative. Later in this section, we consider the possible validity of analogues of Theorem 2.1 where R is a finite commutative quasi-local ring and S is a finite noncommutative ring (see items 2.5-2.8), as well as analogues of Theorem 2.1 where both the base ring R and the ring extension S are finite noncommutative rings (see items 2.9-2.10).

Corollary 2.2. *Let $R \subset S$ be (distinct) commutative rings. Let $R_1 \subset S_1$ be (necessarily commutative) rings and B a (possibly zero, necessarily commutative) ring such that R is ring-isomorphic to $R_1 \times B$, S is R-algebra isomorphic to $S_1 \times B$, and (R_1, M) is quasi-local. Consider the quantities $K := R_1/M$, $A := S_1/MS_1$ and $d := \dim_K(A)$. Suppose also that*
either (i) $M \in \mathrm{Max}(S_1)$ and d is a prime number
or (ii) M is an ideal of S_1 and $d = 2$. Then $R \subset S$ is a minimal ring extension.

Proof. It suffices to rework the third paragraph of the proof of Theorem 2.1. In detail: assuming either (i) or (ii) (or both), we get that $R_1/M \subset S_1/M$ is a minimal ring extension, whence $R_1 \subset S_1$ is a minimal ring extension, whence $R \subset S$ is a minimal ring extension. □

While Corollary 2.2 retained the "sufficient condition" aspect of Theorem 2.1 even when R is infinite (and S is still commutative), we show next that in this broader context, one loses the "necessary condition" part of the conclusion of Theorem 2.1. Indeed, Remark 2.3 shows that in this broader context, a minimal ring extension may fail to satisfy even one of the conditions (i), (ii).

Remark 2.3. There exists an infinite commutative quasi-local ring (R, M) and a commutative ring S such that $R \subset S$ is an inert (integral minimal ring) extension that satisfies neither condition (i) nor condition (ii) of Theorem 2.1. It can further be arranged that $R = \mathbb{Q}$ (so that $M = 0$) and that S ($\cong S/MS = S/M$) is a Galois minimal field extension of $\mathbb{Q}$ such that

$$d := \dim_K(A) = \dim_{R/M}(S/M) = [S : \mathbb{Q}] = 4.$$

It follows that the converse of Corollary 2.2 is false (as R and S being fields ensures that $B = 0$). Furthermore, if one would delete the hypothesis in Theorem 2.1 that the base ring is finite, then an assertion in Theorem 2.1, to the effect that "either (i) or (ii)" is a necessary condition for $R \subset S$ to be a minimal ring extension, would fail.

For a proof, it suffices to consider the Galois minimal field extension that was denoted by F/K (with $K = \mathbb{Q}$) in [12, Proposition 2.5 (b)], as $\dim_K(F) = 4$ is not a prime number. This completes the remark.

It is worth repeating that the parameter d took the value 4 in the example presented in Remark 2.3. In all the examples to be treated for the rest of this paper, the value of d will turn out to be a prime number.

One should mention the following example [17, page 3482] of a minimal ring extension $R \subset S$, with R infinite, commutative and quasi-local and S noncommutative that satisfies the analogues of both condition (i) and condition (ii): take $R := \mathbb{C} = \mathbb{R}+\mathbb{R}i$ and $S := \mathbb{H} = R+Rj$, noting that $M = 0$ is the unique maximal (two-sided) ideal of both R and S and that $\dim_R(S) = 2$. With this example and Remark 2.3 in hand, **we will consider only finite rings for the rest of this paper**. In that spirit, we next formulate the variants of conditions (i) and condition (ii) that will be applied (for the rest of Section 2) to ring extensions $R \subset S$ where S is finite but neither R nor S may be commutative.

Let $R \subset S$ be finite (but possibly noncommutative) rings. For the rest of this paper, let us agree to say that $R \subset S$ *satisfies* (i) if there exists $M \in \mathrm{Max}(R) \cap \mathrm{Max}(S)$ such that $d := \log_{|R/M|}(|S/M|)$ is a prime number; and that $R \subset S$ *satisfies* (ii) if there exists $M \in \mathrm{Max}(R)$ such that M is an ideal of S and $d := \log_{|R/M|}(|S/M|) = 2$. Note that these reformulations of properties (i) and (ii) agree with the original formulations of (i) and (ii), respectively, in case $R \subset S$ are finite commutative rings such that R is local, as well as with the view of the parameter d as $\dim_{R/M}(S/M)$ for the "finite and commutative rings with local base ring" case of the context in Theorem 2.1 and Corollary 2.2.

We next slightly generalize Corollary 2.2 by proving that (ii) (resp., (i)) is a sufficient condition for a special (resp., very special) kind of ring extension, involving possibly noncommutative rings, to be a minimal ring extension.

Lemma 2.4. (*a*) *Let $R \subset S$ be rings and let M be a (two-sided) ideal of both R and S such that R/M is a field and $\dim_{R/M}(S/M) = 2$. Then $R \subset S$ is a minimal ring extension.*

(*b*) *Let $R \subset S$ be rings and let M be a (two-sided) ideal of both R and S such that S/M is a finite field and $d := \log_{|R/M|}(|S/M|)$ is a prime number. Then $R \subset S$ is a minimal ring extension.*

(*c*) *Let $R \subset S$ be finite (not necessarily commutative) rings. If $R \subset S$ satisfies either (i) or (ii) for some $M \in \mathrm{Max}(R)$ such that S/M is a field, then $R \subset S$ is a minimal ring extension.*

Proof. (a) Applying a standard theorem about surjective ring homomorphisms to the canonical surjection $S \to S/M$, we get that the assignment $\Lambda \mapsto \Lambda/M$ determines a bijection $[R, S] \to [R/M, S/M]$. It follows that $R \subset S$ is a minimal ring extension if and only if $R/M \subset S/M$ is a minimal ring extension. This, in turn, follows as in the third paragraph of the proof of Theorem 2.1 (where the sufficiency of (ii) was established for the context of that result).

(b) As in the proof of (a), it suffices to show that $R/M \subset S/M$ is a minimal ring extension. As S/M is a finite field, $K := R/M$ is a finite integral domain, hence a finite field, so that $\dim_K(S/M) = d$, which is a prime number. Then, as in the proof of Theorem 2.1, an appeal to [21, Exercise 1 (b), page 20] completes the proof.

(c) As in the proof of (b), we have that S/M and $K := R/M$ are finite fields, so that $\dim_K(S/M) = \log_{|R/M|}(|S/M|)$, which is a prime number (regardless of whether (i) or (ii) is assumed). An application of (b) completes the proof. □

As one may surmise from the very special nature of the hypotheses in Lemma 2.4, conditions (i) and (ii) do not serve to capture the diversity exhibited within the class of minimal ring extensions involving noncommutative rings. For the rest of this section, we will provide a variety of examples illustrating that conclusion, while offering some positive results on the logical independence of (i) and (ii) amid some minimal ring extensions for the more general settings.

As we move beyond the context where all the (finite) rings of interest are commutative, the first context that we will examine will be that that of ring extensions $R \subset S$ where R is commutative and local and S is finite. This context seems especially apt in view of the following consequence of Lemma 2.4. Corollary 2.5 establishes that, for this context, satisfying (ii) is a sufficient condition for a ring extension $R \subset S$ to be a minimal ring extension. However, Example 2.6 will show that for this context, satisfying (ii) is not a necessary condition for a ring extension $R \subset S$ to be a minimal ring extension. In this way, Corollary 2.5 and Example 2.6 will combine to show that for the context now at hand, property (ii) plays a different (and lesser) role in the analysis of minimal ring extensions than it did for the "wholly commutative" context that was studied in Theorem 2.1. Example 2.7 will show that, for the context now at hand, it is also the case that satisfying property (i) is not a necessary condition for a ring extension to be minimal.

Corollary 2.5. *Let $R \subset S$ be rings such that (R, M) is commutative and local and S is finite. Suppose also that $R \subset S$ satisfies (ii) (necessarily with respect to M); that is, suppose that M is an ideal of S and $d := \log_{|R/M|}(|S/M|) = 2$. Then $R \subset S$ is a minimal ring extension.*

Proof. As the hypotheses imply that $d = \dim_{R/M}(S/M)$, it suffices to apply Lemma 2.4 (a). □

Example 2.6 makes use of an example of George Bergman, as presented and interpreted by Dorsey and Mesyan in [17, Lemma 6.6 and Remark 6.7]. One should note that Bergman's construction is more general than the use to which it is put in Example 2.6, as Bergman's construction did not require the fields F and k in Example 2.6 to be finite (but he did require that $F \subset k$ be a finite-dimensional field extension).

Example 2.6. (cf. [17, Lemma 6.6 and Remark 6.7]) There is a minimal ring extension $R \subset S$ such that R is a commutative local ring (in fact, a finite field k), S is a finite noncommutative ring (in fact, isomorphic to a matrix ring $M_q(F)$ for some prime number q and some finite field F such that $F \subset k$ is a minimal field extension with $q = [k : F]$), and the minimal ring extension $R \subset S$ satisfies (i) (necessarily with respect to $M := 0 \in \mathrm{Max}(R) \cap \mathrm{Max}(S)$). It can be further arranged that the minimal ring extension $R \subset S$ satisfies (resp., does not satisfy) (ii), namely, by taking $q = 2$ (resp., $q \neq 2$).

Proof. Note that q is a prime number because we have assumed that the partners in the minimal field extension $F \subset k$ are finite fields. In the proof of [17, Lemma 6.6] (where it had only been assumed that $F \subset k$ is an n-dimensional field extension with $2 \leq n < \infty$), S was produced as follows: as k as an n-dimensional vector space over F, view $R := k$ as a subring of $\mathrm{Hom}_F(k, k)$ via the left regular action of k on itself; and take S to be minimal among subrings of $\mathrm{Hom}_F(k, k)$ ($\cong M_n(F)$) that properly contain k. It was shown in [17, Lemma 6.6] that $S \cong M_n(D)$ for some (in our case, necessarily finite) division ring D. By a celebrated theorem of Wedderburn (cf. [19, Theorem 3.1.1 and item (2), page 102]), any finite division ring is a field, and so D is a finite field. This assessment was refined in [17, Remark 6.7] where it was further assumed that $F \subset k$ is a minimal field extension, at which point Dorsey and Mesyan asserted that the proof of [17, Lemma 6.6] showed that, under the additional assumptions of $F \subset k$ being a minimal field extension, $S = \mathrm{Hom}_F(k, k)$ ($\cong M_n(F)$); that is, $D = F$. We will use this next (with, of course, n replaced by q).

It remains to address the assertions concerning properties (i) and (ii). Since S is a simple artinian ring, the maximal ideal M ($= 0$) of R is also the unique maximal (two-sided) ideal of S. We have $d := \log_{|R/M|}(|S/M|) = \log_{|k|}(|M_q(F)|)$. Also, $|F| = p^\nu$ for some prime number p and some integer $\nu \geq 1$; and $|k| = p^{\nu q}$. We get

$$p^{\nu qd} = (p^{\nu q})^d = |k|^d = |M_q(F)| = |F|^{q^2} = (p^\nu)^{q^2} = p^{\nu q^2}.$$

By the Fundamental Theorem of Arithmetic, $\nu qd = \nu q^2$, Therefore, $d = q$, which is a prime number. The assertions concerning (i) and (ii) are now evident from the definitions of (i) and (ii). □

As a counterpoint to Example 2.6, we next provide an example of a minimal ring extension $R \subset S$, with R a commutative local ring and S a finite noncommutative ring, satisfying (ii) but not (i).

Example 2.7. There are minimal ring extensions $R_1 \subset S$ and $R_2 \subset S$ such that R_1 and R_2 are commutative local rings (in fact, R_1 is the finite field $\mathbb{F}_4$), S is a finite noncommutative ring, the minimal ring extension $R_1 \subset S$ satisfies (ii)

(necessarily with respect to $M := 0 \in \mathrm{Max}(R)$) but not (i), and the minimal ring extension $R_2 \subset S$ satisfies both (i) and (ii). One way to produce such data (with $R_1 = \mathbb{F}_4$) is the following. Define $\sigma : \mathbb{F}_4 \to \mathbb{F}_4$ by $\sigma(a) := a^2$ for all $a \in \mathbb{F}_4$; the additive structure of $S = \mathbb{F}_4 + \mathbb{F}_4 x$ is that of a 2-dimensional vector space over $\mathbb{F}_4$ with $\mathbb{F}_4$-basis $\{1, x\}$; the multiplication on S is induced by requiring that $x^2 = 0$ and $xa = \sigma(a)x$ for all $a \in \mathbb{F}_4$; let $I := \mathbb{F}_4 x$; and let $R_2 := \mathbb{F}_2 + M$.

Proof. We can write $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$, where $\alpha^2 = \beta$ and $\beta^2 = \alpha$. It is easy to see that σ is a field automorphism of $\mathbb{F}_4$, σ is not the identity map on $\mathbb{F}_4$ (since $\sigma(\alpha) = \beta \neq \alpha$), and $\sigma \circ \sigma$ is the identity map on $\mathbb{F}_4$. In other words, σ is a non-identity involution (of order 2) on $\mathbb{F}_4$.

For the sake of completeness, let us define the multiplication on S more clearly. For $\xi, \eta \in S$, we have $\xi = a + bx$ and $\eta = c + dx$ for some (uniquely determined) $a, b, c, d \in \mathbb{F}_4$. Then

$$xy := ac + (ad + b\sigma(c))x.$$

It is straightforward to verify that S is a ring, R_1 is a (commutative local) subring of S, and R_2 is a commutative subring of S. Moreover, S is noncommutative, as $x\alpha = \sigma(\alpha)x = \beta x \neq \alpha x$.

It is easy to verify that $I := \mathbb{F}_4 x$ is a (two-sided) ideal of S. As each element of I is nilpotent and $1 \neq 0$ in S, we have $I \neq S$. Of course, $I \neq 0$ (as $x \in I$). Also, if $0 \neq \gamma \in \mathbb{F}_4$, then $S\gamma S + I = S$. (This assertion is clear if $\gamma = 1$, since $S^2 = S$; so, without loss of generality, $\gamma = \alpha$; then it suffices to observe that $\beta = \alpha \cdot \alpha \cdot 1 + 0 \in S\alpha S + I$ and $1 = \beta \cdot \alpha \cdot 1 + 0 \in S\alpha S + I$.) Thus, I is the unique maximal ideal of S. In particular, M $(= 0)$ is not a maximal ideal of S. Hence, the ring extension $R_1 \subset S$ does not satisfy (i). On the other hand, $R_1 \subset S$ does satisfy (ii), since

$$\log_{|R_1/M|}(|S/M|) = \log_{|R_1|}(|S|) = \log_4(16) = 2.$$

Next, Lemma 2.4 (a) ensures that $R_1 \subset S$ is a minimal ring extension, since

$$\dim_{R_1/M}(S/M) = \log_{|R_1/M|}(|S/M|) = 2.$$

Turning to R_2, note first that $1 + I \subseteq U(R_2)$. (Indeed, $(1 + \gamma x)^{-1} = 1 + \gamma x$ for all $\gamma \in \mathbb{F}_4$.) It follows that I is the unique maximal ideal of R_2. Moreover,

$$\dim_{R_2/I}(S/I) = \log_{|R_2/I|}(|S/I|) = \log_{(|R_2|/|I|)}(|S|/|I|)) = \log_2(4) = 2.$$

Then, appealing to Lemma 2.4 (a) and using the definitions of the properties (i) and (ii), we see that $R_2 \subset S$ is a minimal ring extension that satisfies both (i) and (ii). The proof is complete. □

Thanks to Examples 2.6 and 2.7, we now see that, for the class of minimal ring extensions $R \subset S$ with R a commutative local ring and S a finite noncommutative ring, the conditions (i) and (ii) are logically independent.

In view of the above information, it seems apparent that Theorem 2.1 can be of no further motivational use in developing the theory of minimal ring extensions involving finite rings. Accordingly, for the sake of completeness and possible inspiration, Remark 2.8 will examine additional examples of ring extensions with

finite commutative base ring. After that, beginning with Example 2.9, the rest of this section will be set in the "wholly noncommutative" context.

Parts (b) and (c) of Remark 2.8 will assume familiarity with the idealization construction; [20] is a useful reference for the basic facts about this construction.

Remark 2.8. (a) We begin with a modest generalization of the construction and assertions in Example 2.7 for the ring extension that was denoted by $R_1 \subset S$ there. (The ring denoted by S here will be different from the ring that was called S in Example 2.7.)

Let $R := F$ be a finite field admitting a non-identity field automorphism σ that is an involution (that is, $\sigma \circ \sigma$ is the identity map on F). Define a ring S as follows: the additive structure of $S = F + Fx$ is that of a 2-dimensional vector space over F with F-basis $\{1, x\}$; and the multiplication on S is induced by requiring that $x^2 = 0$ and $xa = \sigma(a)x$ for all $a \in F$. Then $R \subset S$ is a minimal ring extension, with R commutative and local and S noncommutative, which satisfies (ii) but does not satisfy (i).

Except possibly for one point, the proof of Example 3.7 carries over. The point in question concerns the assertion that the ideal $I := Fx$ of S is the unique maximal ideal of S. For a reader wishing to see an approach that differs from the one taken in Remark 2.7, we offer the following alternative argument. If $\beta, \gamma \in F$ with $\beta \neq 0$, then

$$1 = \beta^{-1}(\beta + \gamma x) \cdot 1 - \beta^{-1}\gamma x \in S(\beta + \gamma x)S + I,$$

thus completing the (alternative argument and this sketch of) proof.

(b) When (a) is coupled with Example 2.7, one may be led to a false conjecture. Accordingly, we next use an idealization to construct an example whose purpose is to illustrate the following fact. If a minimal ring extension $R \subset S$ of finite rings, with R commutative local and S noncomutative, satisfies (ii) but not (i) and if the multiplication on S is defined by "twisting" via a non-identity involution of a field, then R need not itself be a field.

As in (a), let F be a finite field admitting a non-identity field automorphism σ that is an involution. This time, take R to be the idealization $F(+)F$, and define a ring S as follows: the additive structure of $S = R \oplus Fx$ is that of a 3-dimensional vector space over F with F-basis $\{(1,0,0), (0,1,0), (0,0,x)\}$; and the multiplication on S is induced by requiring that $(a,b,0)x = ax$ $(= (0,0,ax))$ and $x(a,b,0) = \sigma(a)x$ $(= (0,0,\sigma(a)x))$ for all $(a,b) \in R$. Note that R is a finite commutative local ring with maximal ideal $M = 0(+)F$. Using straightforward calculations, one checks that M is an ideal of S. However, M is not a maximal ideal of S, since $M \subset M \oplus Fx \subset S$. Therefore, the ring extension $R \subset S$ does not satisfy (i). On the other hand,

$$d := \log_{|R/M|}(|S/M|) = \log_{(|R|/|M|)}(|S|/|M|)) =$$

$$\log_{(|F|^2/|F|)}(|F|^3/|F|)) = \log_{|F|}(|F|^2) = 2,$$

and so $R \subset S$ does satisfy (ii). It remains only to verify that $R \subset S$ is a minimal ring extension. This, in turn, holds because there is no F-vector subspace properly

contained between R and S, the point being that $\dim_F(R) = 2$ and $\dim_F(S) = 3$ are consecutive integers. The proof is complete.

(c) Let $S := \mathrm{U}_2(\mathbb{F}_2)$, the ring of upper triangular 2×2 matrices over $\mathbb{F}_2$; and, as usual, let I denote the 2×2 identity matrix over $\mathbb{F}_2$. It is well known (and easily checked) that S is a noncommutative ring. View $\mathbb{F}_2 \subset S$ by identifying $\xi \in \mathbb{F}_2$ with the scalar matrix ξI. Let C denote the 2×2 matrix over $\mathbb{F}_2$ whose only nonzero entry is c_{12} $(= 1)$. Since $C^2 = 0$, one checks easily that $(I+C)^2 = 0$ and $(I + C)C = C = C(I + C)$. It follows that $R := \mathbb{F}_2 + \mathbb{F}_2C = \{0, I, C, I + C\}$ is a commutative subring of S and, in fact, that

$$R \cong \mathbb{F}_2(+)\mathbb{F}_2C \cong \mathbb{F}_2(+)\mathbb{F}_2.$$

(A reader who wishes, despite (b), to avoid considering idealizations as much as possible may instead, at this point, verify that $R \cong \mathbb{F}_2[X]/(X^2)$, but one should be advised that Example 2.11 will make serious use of Dorroh extensions, which are the possibly noncommutative generalizations of idealizations.)

As the prime ideals of an idealization $A(+)E$ are well understood (they are the ideals $P(+)E$ as P ranges over the prime ideals of A), the only prime (maximal) ideal of $\mathbb{F}_2(+)\mathbb{F}_2$ is $0(+)\mathbb{F}_2$. Therefore, by tracing through the displayed isomorphisms, we see that the only prime (maximal) ideal of R is $M := \mathbb{F}_2C$. (As M is just $\{0, C\}$, a few easy calculations could have led to this conclusion without appealing to the theory of idealizations.) By performing 16 matrix multiplications, one easily verifies that M is an ideal of S. The most significant fact about M is that M is not a maximal ideal of S. To establish this fact, it is enough to find a matrix $D \in S \setminus M$ such that the (two-sided) ideal of S that is generated by $R \cup \{D\}$ is not S. We claim that it suffices to take D to be the 2×2 matrix over $\mathbb{F}_2$ whose only nonzero entry is d_{22} $(= 1)$. To establish this claim, one need only check that $\mathcal{I} := \{0, C, D, C + D\}$ is an ideal of S; and that, in turn, can be easily checked by showing that $ED, DE \in \mathcal{I}$ for all $E \in S$. With the claim having thus been proved, it now follows, since M is the only maximal ideal of R, that the ring extension $R \subset S$ does not satisfy (i).

As for property (ii), we have that $d := \log_{|R/M|}(|S/M|) =$

$$\log_{(|R|/|M|)}(|S|/|M|) = \log_{(4/2)}(8/2) = \log_2(4) = 2,$$

which is a prime number. Thus, the ring extension $R \subset S$ satisfies (ii).

Next, we claim that $R \subset S$ is a minimal ring extension. We will prove even more, namely, that there is no additive subgroup properly contained between R and S. To prove this stronger version of the claim, it suffices (because of the multiplicativity property of group indexes for towers of groups) to show that the group-theoretic index $[S : R]$ is a prime number. By Lagrange's Theorem, $[S : R] = |S|/|R| = 8/4 = 2$, and so the claim has been proven.

In summary, the data in (c) are such that $\{0, I, C, I + C\} \subset \mathrm{U}_2(\mathbb{F}_2)$ is a minimal ring extension, whose base ring is commutative and local and whose "top" ring is finite and noncommutative, that satisfies (ii) and does not satisfy (i). As ring extensions with this behavior have already been constructed in (a), (b) and Example 2.7, it is natural to ask why we have included a study of the ring extension in (c). The answer is that, by a very slight change to the matrix

C from (c), we will see in (d) that a somewhat similar construction of a different ring (let us call it $\mathcal{R}$ here) will have the property that $\mathcal{R} \subset \mathrm{U}_2(\mathbb{F}_2)$ is a minimal ring extension that satisfies neither (i) nor (ii).

(d) Let us take another look at a ring extension that was studied in [11, Example 2.5]. The matrix denoted by C here will be different from the matrix that was called C in (c); the ring denoted by R here will be different from the ring that was called R in (c); the ring denoted by S here will be the same ring that was called S in (c).

Let $S := \mathrm{U}_2(\mathbb{F}_2)$, the ring of upper triangular 2×2 matrices over $\mathbb{F}_2$. Recall that S is noncommutative. As in (c), let I denote the 2×2 identity matrix in S and view $\mathbb{F}_2 \subset S$. Let $C \in S$ denote the matrix whose only nonzero entry is c_{11} $(= 1)$. (A reminder: this is not the same matrix that was called C in (c).) Since $C^2 = C$, one checks easily that $(I+C)^2 = I+C$ and $(I+C)C = 0 = C(I+C)$. As was proven in [11, Example 2.5], it follows that $R := \mathbb{F}_2 + \mathbb{F}_2 C = \{0, I, C, I+C\}$ is a commutative subring of S and, in fact, that R is the internal direct product $\mathbb{F}_2 \times \mathbb{F}_2 C$, whence $R \cong \mathbb{F}_2 \times \mathbb{F}_2$. By using Lagrange's Theorem (very much as in the above argument in the proof of (c)), it was proven in [11, Example 2.5] that $R \subset S$ is a minimal ring extension.

We claim that $R \subset S$ satisfies neither (i) nor (ii). To prove this claim, it suffices to show that no maximal ideal of R is an ideal of S. As the only maximal (prime) ideals of $\mathbb{F}_2 \times \mathbb{F}_2$ are $0 \times \mathbb{F}_2$ and $\mathbb{F}_2 \times 0$, we see, by tracing through the above-mentioned isomorphism, that the only maximal ideals of R are $M_1 := \{0, C\}$ and $M_2 := \{0, I + C\}$. We will show more than the above claim, namely, that M_1 is not a right ideal of S and M_2 is not a left ideal of S. To that end, consider the matrix $G \in S$ whose only nonzero entry is g_{12} $(= 1)$. It is straightforward to check that $CG = G \notin M_1$ and $G(I + C) = G \notin M_2$, thus proving the claim.

In summary, the data in (d) are such that $\{0, I, C, I+C\} \subset \mathrm{U}_2(\mathbb{F}_2)$ is a minimal ring extension, whose base ring is commutative and local and whose "top" ring is finite and noncommutative, that satisfies neither (i) nor (ii). As mentioned in (c), one reason for including (d) was to indicate how what may seem to be a "small" change in data can lead to a ring extension with qualitatively different behavior with respect to the properties (i) and (ii). By way of contrast, note that this kind of change in behavior did not occur for the data in (a) and (b) when viewed as "small" changes from the data in Example 2.7.

(e) We will shortly give an additional reason for our decision to include a study of the ring extension $R \subset S$ in (d). In working with that ring extension in [11, Example 2.5], Jarboui and the author noted that S is not an R-algebra; that is, R is not contained in the center of S. That led us to introduce a variant (dubbed AFMC) of the FMC property of ring extensions. In that way, it was hoped that some techniques that had been productive in the study of the FMC property for ring extensions involving only commutative rings would adapt to being helpful in the study of ring extensions involving noncommutative rings. In the same spirit, it was decided to define the properties (i) and (ii) (just prior to Lemma 2.4) without reference to any possible descriptions of the relevant rings as direct products. While any commutative finite non-local ring is a nontrivial direct product, many interesting finite noncommutative rings are not expressible as nontrivial direct

products. (It was noted in [11, Remark 2.6 (d)] that $U_2(\mathbb{F}_2)$ is not a nontrivial direct product of rings.) In short, the above-promised "additional reason" was our interest in introducing versions of the conditions appearing in the statement of Theorem 2.1 that would be more widely applicable to noncommutative ring extensions, in recognition of the greater diversity exhibited by such extensions.

On the other hand, one may ask what can be said about the structure of ring extensions $R \subset S$ when R is commutative and S is (possibly noncommutative but) an R-algebra; that is, when R is a finite commutative ring that is contained in the center of S. More generally, suppose that $R \cong \prod_{j=1}^{n} R_j$, a finite direct product of (possibly quasi-local) rings R_j. Then the study of ring extensions $R \subset S$ (and, in particular, the study of minimal ring extensions) such that S is an R-algebra reduces to the case $R = R_j$ (for some j), exactly in the style expressed for commutative ring extensions in [9, Lemma 2.2 (b)]: see [10, Proposition 2.1 (b), (c)]. (In fact, it follows, as a special case of [10, Proposition 2.1 (c)] but also admitting a direct easy proof, that if $R \subset S$ is a minimal ring extension such that R is commutative and S is an R-algebra, then S is commutative.) Just as the genesis of [9, Lemma 2.2 (b)] was a folklore categorical equivalence between the category of commutative R-algebras (when $R \cong \prod_{j=1}^{n} R_j$ as above) and the product (indexed by $j = 1, \ldots, n$) of the categories of commutative R_j-algebras, the above-mentioned better behavior of (not necessarily commutative) R-algebras over a finite direct product of commutative rings grew out of a similar categorical equivalence (constructed as in the "folklore" case) involving the category of (not necessarily commutative) R-algebras due to Kosters [25, Theorem 2.1] (cf. [10, Proposition 2.1 (a)]). While [10, Proposition 2.1 (b)] is expected to be of future help in studying non-minimal ring extensions that are algebras over commutative base rings that are finite direct products, it is now clear that, in any future studies of minimal ring extensions $A \subset B$ where A is commutative and B is definitely noncommutative, the focus must be on the situation where B is not an A-algebra.

(f) The ring $S := U_2(\mathbb{F}_2)$, which occupied us in parts (c)-(e), has been much studied. For some additional information about this ring S and for generalizations of it, see [23, Example 2.13 and Theorem 4.23]. Since the base ring R in (d) is (isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ and hence is) not local, one may ask why the extension $R \subset S$ in (d) was studied in this part of the project where the focus has been on ring extensions with (finite commutative) base rings that *are* local. One answer has to do with our intention to provide a segue toward the upcoming study of more general ring extensions in the remainder of this section. This completes the remark.

Despite items 2.4-2.7, we do not know if there exist rings $R \subset S$, with R commutative and local and S finite and noncommutative, such that this ring extension satisfies (i) but is not a minimal ring extension. We leave this question to any interested readers with more expertise than the author in noncommutative ring theory.

To complete this section, we investigate the themes from Examples 2.6 and 2.7 within the class of minimal ring extensions $R \subset S$ where R is finite and noncommutative (and, necessarily, so is S). For this setting, we begin with a

result whose conclusion has the same qualitative impact as Example 2.6 did for its context (of a commutative local finite base ring). In our opinion, the construction used in proving Example 2.9 is remarkably more prosaic than the construction of Bergman that was used in proving Example 2.6.

Example 2.9. Let $F \subset k$ be a minimal field extension of finite fields, consider the prime number $q := [k : F]$ and any integer $n \geq 2$, and define the matrix rings $R := M_n(F)$ and $S := M_n(k)$. Then $R \subset S$ are finite noncommutative rings, each having $M := 0$ as its only maximal ideal, such that the ring extension $R \subset S$ satisfies (i) (necessarily with respect to M); and, moreover, $R \subset S$ satisfies (ii) (necessarily with respect to M) if and only if $q = 2$.

Proof. It is clear that q is a prime number, that R and S are each finite noncommutative rings, and that $M := 0$ is the only proper ideal of R (resp., of S). Also, by [1, Corollary 1], $R \subset S$ inherits from $F \subset k$ the property of being a minimal ring extension. Since $|k| = |F|^q$, we have

$$d := \log_{|R/M|}(|S/M|) = \log_{|R|}(|S|) = \log_{|F|^{n^2}}(|k|^{n^2}) = \log_{|F|^{n^2}}((|F|^q)^{n^2}) = q,$$

which is a prime number. The assertions concerning (ii) and (i) follow at once. The proof is complete. □

Example 2.10 will show that "satisfies either (i) or (ii)" is not a necessary condition for an arbitrary extension of finite rings to be a minimal ring extension. In other words, one cannot delete the hypothesis of commutativity for the assertion of "necessary condition" in the statement of Theorem 2.1.

Example 2.10. There is a minimal ring extension $R \subset S$ such that R and S are each finite noncommutative rings and the ring extension $R \subset S$ satisfies neither (i) nor (ii). One way to produce such data is the following. Let k be any finite field; let $R := \mathrm{U}_2(k)$, the ring of upper triangular 2×2 matrices over k; and let S be the matrix ring $M_2(k)$.

Proof. It is clear that R and S are each finite noncommutative rings. Dorsey and Mesyan note (for any field k) in [17, page 3468] that, by comparing vector space dimensions over k, one can conclude that $R \subset S$ is a minimal ring extension (the point being that $\dim_k(S) - \dim_k(R) = 1$). As the only ideals of S are 0 and S, the assertion concerning the properties (i) and (ii) comes down to showing that 0 is not a maximal ideal of R. This, in turn, holds since (for instance) the set of matrices in R having only 0 entries in their second rows forms a nonzero proper ideal of R (that properly contains 0). □

Let R be a (possibly noncommutative) ring and let I be an R-rng (in the sense of [17, pages 3465-3466]). We next recall the definition of the *Dorroh extension* $E(R, I)$ of R (from [17, page 3466]). The additive structure of $E(R, I)$ is that of the external direct sum $R \oplus I$, with multiplication given by $(r_1, i_1) \cdot (r_2, i_2) := (r_1 r_2, r_1 i_2 + i_1 r_2 + i_1 i_2)$ for all $r_1, r_2 \in R$ and $i_1, i_2 \in I$. One views R as a subring of $E(R, I)$ via the injective (unital) ring homomorphism $R \to E(R, I)$ given by $r \mapsto (r, 0)$. Particular interest was paid in [17] to the case where $R \neq 0$ and I is taken as the R-R bimodule R/M with trivial (that is, identically zero)

multiplication where $M \in \mathrm{Max}(R)$. It was shown in [17, Lemma 2.4 and Remark 2.5] that, under these conditions, $R \subset E(R, R/M)$ is a minimal ring extension. As indicated in [17, page 3467], the proofs of [17, Lemma 2.4 and Remark 2.5] were inspired by the proofs of [5, Theorem 2.4 and Remark 2.9] that were given for the case where R is a commutative ring and the role of $E(R, R/M)$ had been played by the idealization $R(+)R/M$. For this reason, and because of the prominent role played by Dorroh extensions in the classification results of Dorsey and Mesyan in [17], we devote the next result to an initial study of the interplay between Dorroh extensions and the properties (i) and (ii).

Example 2.11. Let R be a finite nonzero ring, $M \in \mathrm{Max}(R)$ and $S := E(R, R/M)$, the associated Dorroh extension of R. Then $R \subset S$ is a minimal ring extension that satisfies (ii) (with respect to M), and the ring extension $R \subset S$ does not satisfy (i).

Proof. As recalled above, $R \subset S$ is a minimal ring extension [17, Remark 2.5]. When R is identified with the subring $R \oplus 0$ of S, the maximal ideal M of R is identified with $M \oplus 0$. It is then clear from the definition of multiplication in a Dorroh extension that $MS = M$; that is, M is an ideal of S. However, $M \notin \mathrm{Max}(S)$ since $M \subset M \oplus R/M \subset S$. An easy calculation shows that $M \oplus R/M \in \mathrm{Max}(S)$. However, if $N \in \mathrm{Max}(R)$ and $N \neq M$, then $N \notin \mathrm{Max}(S)$. (Indeed, there exist $n \in N$ and $m \in M$ such that $n+m = 1$, so that NS contains the element $n(1, 1 + M) =$

$$(n, 0)(1, 1 + M) = (n, n + M) = (n, 1 - m + M) = (n, 1 + M),$$

which is not an element of $N \oplus 0$.) It follows that $\mathrm{Max}(R) \cap \mathrm{Max}(S) = \{M\}$, and so $R \subset S$ does not satisfy (i). It remains only to show that $R \subset S$ does satisfy (ii). To that end, note that, as abelian groups,

$$S/M = (R \oplus R/M)/(M \oplus 0) \cong R/M \oplus R/M,$$

so that $|S/M| = |R/M|^2$, whence $d := \log_{|R/M|}(|S/M|) = 2$. Therefore, $R \subset S$ does indeed satisfy (ii), thus completing the proof. □

One can summarize part of the conclusions of Examples 2.9 -2.11 as follows. For some finite noncommutative rings, there exists a minimal ring extension $R \subset S$ that satisfies both (i) and (ii) (resp., that satisfies (i) but not (ii); resp., that satisfies (ii) but not (i); resp., that satisfies neither (i) nor (ii)). As we have thus realized all four possibilities for the interplay between the properties (i) and (ii) with minimal ring extensions $R \subset S$ that involve finite noncommutative rings, we will not include further examples along those lines here. (The interested reader will discover that some of our earlier constructions for the context where R was a commutative finite local ring can be generalized to the present context where both R and S are finite and noncommutative.) Instead, we close this section with a couple of theoretical comments in the following remark.

Remark 2.12. (a) If R is a commutative (not necessarily finite) ring and $M \in \mathrm{Max}(R)$, the Dorroh extension $E(R, R/M)$ is merely the idealization $R(+)R/M$. It has been useful, at many points of recent research, to note that the minimal ring extension $R \subset R(+)R/M$ is ramified. Once one knows (from [5]) that

$R \subset R(+)R/M$ is a minimal ring extension, the "ramified" assertion is equivalent to the assertion that $R \subset R(+)R/M$ is a subintegral extension. A more general "subintegral" assertion was given by Picavet and Picavet-L'Hermitte in [29, Lemma 1.1]. A direct verification of the "ramified" assertion may be made as follows. If $K := R/M$ and $S := R(+)K$, then

$$S/MS = (R(+)K)/((M(+)0)(R(+)K)) =$$

$$(R(+)K)/(MR(+)(MK + 0 \cdot R)) = (R(+)K)/(M(+)0) \cong$$

$$R/M \times K/0 \cong K \times K.$$

The detailed argument in the preceding displays motivated the final display (concerning a possibly noncommutative Dorroh extension) in the proof of Example 2.11. We would hope that a bilateral transfusion of methods will continue between practitioners of commutative ring theory and workers in noncommutative ring theory.

(b) To close this section, we address the comment that was made prior to Example 2.10 stating that "satisfies either (i) or (ii)" is not a necessary condition for an arbitrary extension of finite rings to be a minimal ring extension. The reader may have wondered if we were referring there to the definitions of (i) and (ii) that had been made prior to Lemma 2.4 or to the conditions that had been denoted by (i) and (ii) in the statement of Theorem 2.1. In reply, we would point out that there is no difference between the two notions of (i) (resp., of (ii)) if they are being applied to a ring extension $R \subset S$ such that at least one of the finite rings R and S cannot be expressed as a nontrivial direct product of rings. The comment in question had referred to the rings appearing in Example 2.10, namely, $R := \mathrm{U}_2(k)$ and $S := M_2(k)$, where k is a finite field and $n \geq 2$. It is a standard result that $M_n(k)$ has only 0 and itself as ideals (regardless of whether the field k is finite), and so this S certainly cannot be isomorphic to a nontrivial direct product of rings. While it is not necessary to add that the same conclusion holds for $\mathrm{U}_2(\mathbb{F}_2)$, a fact that played a role in both Remark 2.8 (d) and [11, Remark 2.6 (d)], perhaps it is useful to indicate how appropriate it was to use the extension $\mathrm{U}_2(\mathbb{F}_2) \subset M_2(\mathbb{F}_2)$ in making the larger point that was established in Example 2.10 and expressed in the comment which preceded it. The remark is complete.

3. What $|Z(S)|$ says about a minimal ring extension

This section returns to a focus on the minimal ring extensions $R \subset S$ where S is commutative and R is finite. Recall from the Introduction that any such S must be finite and, moreover, integral over R. Thus, $R \subset S$ must be of exactly one of three types, namely, either ramified, decomposed or inert. By [9, Lemma 2.2], there will be no serious loss of generality in assuming that R is also a local ring. For that setting, we will see what information can be gleaned about/from $|Z(S)|$, the number of zero-divisors in S. Let us fix the following **running hypothesis and notation for this section:** (R, M) **is a finite local commutative ring,** $K := R/M$, and so (cf. [27]) $|R| = p^\lambda$ **for some prime number** p **and some**

integer $\lambda \geq 1$, $K \cong \mathbb{F}_{p^\mu}$ for some integer $\mu \geq 1$, and it follows that

$$|M| = |R|/|R/M| = \frac{p^\lambda}{p^\mu} = p^{\lambda-\mu}.$$

Note that $\mu \leq \lambda$, with equality if and only if $M = 0$; that is, if and only if R is a (finite) field.

For any inclusion $D \subset E$ of (distinct) commutative rings, we have $Z(D) \subseteq Z(E)$, but it is possible that $Z(D) = Z(E)$ under these conditions, as for example, when both D and E are fields. One may, therefore, expect that if $R \subset S$ is an inert (integral minimal ring) extension where S is commutative and R is finite, then $Z(R) = Z(S)$. This is, in fact, the case: see parts (a) and (d) of Lemma 3.1 below. However, Lemma 3.1 (e) will also establish that if $R \subset S$ is any other type of (integral) minimal ring extension (that is, either ramified or decomposed) where S is commutative and R is finite, then $Z(R) \subset Z(S)$. In other words, S has more zero-divisors than R whenever finite commutative rings $R \subset S$ form a minimal ring extension which is not inert. Lemma 3.1 will also include more detailed information along these lines, which, in turn, will lead to applications in Theorem 3.2 and some of the subsequent results.

Lemma 3.1. *With this section's running hypothesis and notation remaining in place, we have the following:*

(a) $|Z(R)| = p^{\lambda-\mu}$.

(b) Let S be a (necessarily finite) commutative ring such that $R \subset S$ is a ramified (integral minimal ring) extension. Then $|Z(S)| = p^\lambda$.

(c) Let S be a (necessarily finite) commutative ring such that $R \subset S$ is a decomposed (integral minimal ring) extension. Then

$$|Z(S)| = p^{\lambda-\mu}(2p^\mu - 1).$$

(d) Let S be a (necessarily finite) commutative ring such that $R \subset S$ is an inert (integral minimal ring) extension. Then $|Z(S)| = p^{\lambda-\mu}$.

(e) Let S be a (necessarily finite) commutative ring such that $R \subset S$ is an minimal ring extension. If $R \subset S$ is either ramified or decomposed, then $Z(R) \subset Z(S)$ (that is, $|Z(R)| < |Z(S)|$). If $R \subset S$ is inert, then $Z(R) = Z(S)$ (that is, $|Z(R)| = |Z(S)|$).

Proof. It will be convenient to let $A := S/M$ in (b)-(d).

(a) Since R is a finite nonzero commutative ring, the Krull dimension of R is 0 (cf. [2, Proposition 5.7]). It follows that M is the only prime ideal of R, and so $Z(R) \subseteq R \setminus U(R) = M$. On the other hand, as M is minimal as a prime ideal of R that contains the ideal 0, [22, Theorem 84] ensures that $M \subseteq Z(R)$. Hence $Z(R) = M$, and so $|Z(R)| = |M| = p^{\lambda-\mu}$, as asserted.

(b) By hypothesis, A $(= S/M)$ can be identified with $K[X]/(X^2) = K \oplus Kx$, where $x := X + (X^2)$ satisfies $x^2 = 0$ and $x \neq 0$. The unique maximal ideal of A is $\mathcal{M} = Kx$, and so $|\mathcal{M}| = |K| = p^\mu$. Since $R \subset S$ is ramified (and R is quasi-local), S is quasi-local. Let N denote the unique maximal ideal of S. As $N/M = \mathcal{M}$,

$$|N| = |N/M| \cdot |M| = |\mathcal{M}| \cdot |M| = p^\mu p^{\lambda-\mu} = p^\lambda.$$

Since (S, N) is a quasi-local finite commutative ring, reasoning as in the proof of (a) shows that $Z(S) = N$, and so $|Z(S)| = p^\lambda$, as asserted.

(c) As in the proof of (a), we see that S has Krull dimension 0. Since $R \subset S$ is decomposed, $A\ (= S/M)$ can be identified, as a K-algebra, with $K \times K$, so A has exactly two prime (maximal) ideals, say $\mathcal{N}_1$ and $\mathcal{N}_2$, and $\mathcal{N}_1 \cap \mathcal{N}_2 = 0$. It follows that S has exactly two prime (maximal) ideals, say N_1 and N_2, and these can be labeled so that $N_i/M = \mathcal{N}_i$ for $i = 1, 2$. Consequently, $N_1 \cap N_2 = M$. Furthermore, $N_1 \cup N_2 \subseteq Z(S)$ by [22, Theorem 84], while the reverse inclusion is clear. Thus,

$$|Z(S)| = |N_1 \cup N_2| = |N_1| + |N_2| - |N_1 \cap N_2|.$$

Also,

$$\frac{|S|}{|M|} = |S/M| = |A| = |K \times K| = |R/M|^2 = \frac{|R|^2}{|M|^2}.$$

Hence, $|S| = |R|^2/|M| = (p^\lambda)^2/p^{\lambda-\mu} = p^{\lambda+\mu}$. Next, since the "decomposed" hypothesis gives $R/M \cong S/N_i$ for $i = 1, 2$, we get

$$|N_i| = \frac{|S|}{|R/M|} = \frac{p^{\lambda+\mu}}{p^\mu} = p^\lambda \text{ for } i = 1, 2.$$

Thus, $|Z(S)| = |N_1| + |N_2| - |M| = 2p^\lambda - p^{\lambda-\mu}$. The statement of (c) in the assertion of this result gives a factored version of this formula for $|Z(S)|$ that will be applied in the proof of (e) and also later in this section.

(d) Since $R \subset S$ is inert, we see (by adapting the reasoning in the proofs of (a) and (b)) that M is the only prime ideal of S and that $Z(S) = M$. Thus $|Z(S)| = |M| = p^{\lambda-\mu}$, as asserted.

(e) Of course, $R \subset S$ must be either ramified, decomposed or inert. Recall that $p^{\lambda-\mu}$ is the value for $|Z(R)|$ that was established in (a). By (d), this is also the value of $|Z(S)|$ if $R \subset S$ is inert. Thus, in the "inert" case, we have $|Z(R)| = |Z(S)|$ for finite sets $Z(R) \subseteq Z(S)$, whence $Z(R) = Z(S)\ (= M)$ in the "inert" case. It remains to show that $p^{\lambda-\mu}$ is less than the values for $|Z(S)|$ that are given in (b) and (c). In case $R \subset S$ is ramified, this is easily seen, as $p^{\lambda-\mu} = |M| < |R| = p^\lambda$. In case $R \subset S$ is decomposed, this follows from the factored version of the formula established in (c), as $2p^\mu - 1 \geq 2 \cdot 2 - 1 > 1$. □

Since the hypotheses in parts (b), (c) and (d) of Lemma 3.1 exhaust all possibilities for a minimal ring extension when R is finite and S is commutative, one can infer the following result. Notice that Theorem 3.2 significantly improves upon Lemma 3.1 (e).

Theorem 3.2. *With this section's running hypothesis and notation in place: Let S be a (necessarily finite) commutative ring such that $R \subset S$ is a minimal ring extension which is either ramified or decomposed (that is, which is not inert). Then $|Z(S)| \geq p\,|Z(R)|$, with equality if and only if $R \subset S$ is ramified with $K \cong \mathbb{F}_p$.*

Proof. If $R \subset S$ is ramified, we see from parts (a) and (b) of Lemma 3.1 that

$$\frac{|Z(S)|}{|Z(R)|} = \frac{p^\lambda}{p^{\lambda-\mu}} = p^\mu \geq p,$$

with equality if and only if $\mu = 1$; that is, if and only $|K| = p$; that is, if and only if $K \cong \mathbb{F}_p$.

If $R \subset S$ is decomposed, we see from parts (a) and (c) of Lemma 3.1 that

$$\frac{|Z(S)|}{|Z(R)|} = \frac{p^{\lambda-\mu}(2p^\mu - 1)}{p^{\lambda-\mu}} = 2p^\mu - 1 \geq 2p - 1 > p.$$

The proof is complete. □

If $D \subset E$ are finite rings, there is a finite upper bound on the length L of any chain of proper ring extensions going from D to E. Indeed, if $D = D_0 \subset \cdots \subset D_{i-1} \subset D_i \subset \ldots \subset D_{L-1} \subset D_L = E$ is such a chain, then $2 \leq [D_i : D_{i-1}]$ for all $i \in \{1, \ldots, L\}$, and so $|D_i| \geq 2|D_{i-1}|$ for all i. It follows that

$$|E| = |D_L| \geq 2|D_{L-1}| \geq 2^2|D_{L-2}| \geq \ldots \geq 2^L|D_0| = 2^L|D|,$$

so that $L \leq \log_2(|E|/|D|) < \infty$, as asserted. This observation has the following application.

Corollary 3.3. *With this section's running hypothesis and notation in place: Let $R \subset S$ be finite commutative rings such that (S, N) is local and let L be the greatest possible length of a chain of rings $R = A_0 \subset \ldots \subset A_L = S$. Then:*

(a) $1 \leq L \leq \log_2(|S|/|R|)$.

(b) View K as a subfield of S/N in the usual way, and consider the unique (apart from the ordering of factors) expression of $\dim_K(S/N)$ as $\prod_{j=1}^k q_j$, where $q_1, \ldots, q_k$ are prime numbers (possibly $k = 0$ and possibly $q_{i_1} = q_{i_2}$ for some $i_1 \neq i_2$) and k is some non-negative integer. Then $k \leq L$. Furthermore, as i runs through the set $\{1, \ldots, L\}$, exactly k of the steps of the form $A_{i-1} \subset A_i$ are inert and the other $L - k$ steps of that form are ramified. Moreover, $|Z(S)| \geq p^{L-k}|Z(R)|$, with equality if and only if both of the following conditions hold: (1) the $L - k$ ramified steps must be all of the initial $L - k$ steps (namely, $A_{i-1} \subset A_i$ for $1 \leq i \leq L - k$); and (2) if $k \neq L$, then $K \cong \mathbb{F}_p$.

Proof. (a) The above comments established (a).

(b) Recall that every finite commutative ring has Krull dimension 0. In particular, S has only one prime ideal. Therefore, by a downward-iterative argument, it follows from integrality (cf. [2, Theorem 5.10 and Corollary 5.8]), that each A_i is a (finite quasi-)local ring. Observe, from the maximality of L, that each step $A_{i-1} \subset A_i$ is a minimal ring extension. Hence, by another downward-iterative argument, it follows that none of these steps can be a decomposed extension (the point being that if $A \subset B$ is a decomposed extension of commutative rings, then B is not quasi-local). Thus, for all i, the extension $A_{i-1} \subset A_i$ is either ramified or inert.

Observe that

$$\frac{|Z(S)|}{|Z(R)|} = \frac{|Z(A_L)|}{|Z(A_0)|} = \frac{|Z(A_L)|}{|Z(A_{L-1})|} \cdot \cdots \frac{|Z(A_i)|}{|Z(A_{i-1})|} \cdot \cdots \frac{|Z(A_1)|}{|Z(A_0)|}.$$

Consider any of the L factors, each of the form $|Z(A_i)|/|Z(A_{i-1})|$ with $1 \leq i \leq L$, appearing in the right-most item of the above display. According to Theorem 3.2 (resp., Lemma 3.1 (e)), if the extension $A_{i-1} \subset A_i$ is ramified (resp., inert), that

factor is at least p (resp. is 1). Next, suppose that exactly s of the steps of the form $A_{i-1} \subset A_i$ are inert (and so the other $L-s$ steps of that form are ramified). Thus, exactly s of the factors of the form $|Z(A_i)|/|Z(A_{i-1})|$ have the value 1, while the other $L-s$ factors of the form $|Z(A_i)|/|Z(A_{i-1})|$ are each greater than or equal to p. Then it follows from the last display that

$$|Z(S)| \geq p^{L-s}\,|Z(R)|.$$

We will next show that $s = k$.

It is known that if $(D, \mathcal{M}) \subset (E, \mathcal{N})$ are finite commutative local rings forming a minimal ring extension that is inert (resp., ramified), then $\dim_{D/\mathcal{M}}(E/\mathcal{N})$ is a prime number (resp., is 1). Next, observe that the field extensions K and S/N are the first and last items in a finite (weakly increasing) tower of field extensions whose typical item is the residue field of one of the rings of the form A_j (for $j = 0, \ldots, L$). By the definition of s and the multiplicativity property of field degrees in a tower, it follows that $\dim_K(S/N)$ $(= [S/N : K])$ is the product of exactly s prime numbers (where one also counts repeated factors). Therefore, in view of the definition of k, it follows from the Fundamental Theorem of Arithmetic that $s = k$. Thus $k \leq L$.

It remains only to characterize when $|Z(S)| = p^{L-k}\,|Z(R)|$. By combining Theorem 3.2 (or parts (a) and (b) of Lemma 3.1) with the argument of two paragraphs ago, we see that this equality holds if and only if, for each ramified extension of the form $A_{i-1} \subset A_i$, we have that the residue field of A_{i-1} is canonically isomorphic to $\mathbb{F}_p$. Now, recall that if $(D, \mathcal{M}) \subset (E, \mathcal{N})$ are *any* commutative local rings forming a minimal ring extension that is ramified, the residue fields $D/\mathcal{M}$ and $E/\mathcal{N}$ are canonically isomorphic. Therefore, as the residue fields of the rings A_j form a weakly increasing tower, we obtain the following necessary and sufficient condition for $|Z(S)| = p^{L-k}\,|Z(R)|$: the $L-k$ ramified steps must be all of the initial $L-k$ steps (that is, $A_{i-1} \subset A_i$ for $1 \leq i \leq L-k$) and, if $k \neq L$, then $K \cong \mathbb{F}_p$. The proof is complete. □

Remark 3.4. (a) The reader may have noticed that the proof of Corollary 3.3 (b) did not use the hypothesis that the chain of rings $\{A_i\}$ going from R to S has maximum length L. Indeed, the proof of Corollary 3.3 (b) is valid without that assumption, even for maximal chains of rings going from R to S that may be of length less than L. In that way, as a practical matter, (the proof of) Corollary 3.3 (b) may be applied to any accessible maximal chain of rings going from R to S, regardless of its length. Of course, we hypothesized a chain of maximal length in Corollary 3.3 (b) in order to get the strongest possible inequality of the form $|Z(S)| \geq p^{L-k}|Z(R)|$. Indeed, while the length of a maximal chain of rings going from R to S may vary from one such chain to another, the parameter k is independent of the ambient chain, as the proof of Corollary 3.3 (b) shows that k is the number of (not necessarily pairwise distinct) prime numbers appearing in the canonical factorization of the integer $\dim_K(S/N)$.

(b) The extreme cases, where $k = L$ and where $k = 0$, of Corollary 3.3 (b) are of special interest. The easiest example of the case where $k = L$ (that is, where $A_{i-1} \subset A_i$ is an inert extension for all $i = 1, \ldots, L$) arises when $R \subset S$ are

distinct finite fields. Even for this kind of example, there may exist more than one chain of rings of maximal length going from R to S. To see this, let q_1 and q_2 be distinct prime numbers, let p be a prime number, let n be a positive integer, and put $R := \mathbb{F}_{p^n}$, $S := \mathbb{F}_{p^{nq_1q_2}}$, $A_1 := \mathbb{F}_{p^{nq_1}}$, and $A_2 := \mathbb{F}_{p^{nq_2}}$. Then $R \subset A_1 \subset S$ and $R \subset A_2 \subset S$ are distinct maximal chains, of maximal length, consisting of inert ring extensions going from R to S.

On the other hand, let us consider the other extreme case of Corollary 3.3 (b), where $k = 0$ (that is, the case where $A_{i-1} \subset A_i$ is a ramified extension for all $i = 1, \ldots, L$). This case has been studied extensively when $L = 2$. For its subcase where ($L = 2$ and) $R = \mathbb{Z}/p^\alpha\mathbb{Z}$ with p a prime number and $\alpha \geq 2$, necessary and sufficient conditions characterizing when there exists a unique maximal chain of rings going from R to S have been given in [8, Theorem 3.1 (b)]. Examples where ($R \subset S$ are commutative finite local rings and) these conditions are satisfied (resp., are not satisfied) can be found in [8, Corollary 3.7], the final paragraph of [16, Remark 4.2 (m)], and [6, Theorem 2.9 (c)] (resp., in [6, Theorem 2.2 (xiii)]). This completes the remark.

We next repeat and also supplement some material from Lemma 3.1 and Theorem 3.2 in order to collect in one result some formulas that will be useful later in this section.

Lemma 3.5. *With this section's running hypothesis and notation remaining in place, we have the following:*

(a) $|R| = p^\lambda$, $|Z(R)| = p^{\lambda-\mu} = |M|$, $U(R) = p^{\lambda-\mu}(p^\mu - 1)$, $|Z(K)| = 1$ *and* $|U(K)| = p^\mu - 1$.

(b) Let (S, N) *be a (necessarily finite) commutative ring such that* $R \subset S$ *is a ramified (integral minimal ring) extension. Then* $|S| = p^{\lambda+\mu}$, $|Z(S)| = p^\lambda = |N|$, $|U(S)| = p^\lambda(p^\mu - 1)$, $|S/M| = p^{2\mu}$, $|Z(S/M)| = p^\mu$ *and* $|U(S/M)| = (p^\mu - 1)p^\mu$.

(c) Let S *be a (necessarily finite) commutative ring such that* $R \subset S$ *is a decomposed (integral minimal ring) extension. Let* N_1 *and* N_2 *denote the (distinct) prime (maximal) ideals of* S. *Then* $|S| = p^{\lambda+\mu}$, $|N_1| = |N_2| = p^\lambda$, $|Z(S)| = p^{\lambda-\mu}(2p^\mu - 1)$, $|U(S)| = p^{\lambda-\mu}(p^\mu - 1)^2$, $|S/M| = p^{2\mu}$, $|Z(S/M)| = 2p^\mu - 1$ *and* $|U(S/M)| = (p^\mu - 1)^2$.

(d) Let S *be a (necessarily finite) commutative ring such that* $R \subset S$ *is an inert (integral minimal ring) extension. Let* q *denote the (necessarily prime) number such that* $S/M \cong \mathbb{F}_{p^{\mu q}}$. *Then* $|S| = p^{\lambda+\mu(q-1)} = p^{\lambda-\mu}p^{\mu q}$, $|Z(S)| = p^{\lambda-\mu} = |M|$, $|U(S)| = p^{\lambda-\mu}(p^{\mu q} - 1)$, $|S/M| = p^{\mu q}$, $|Z(S/M)| = 1$ *and* $|U(S/M)| = p^{\mu q} - 1$.

Proof. In (a), the asserted values for $|Z(K)|$ and $|U(K)|$ follow since K is a field of cardinality p^μ. Similarly, in (d), the asserted values for $|Z(S/M)|$ and $|U(S/M)|$ follow since S/M is a field of cardinality $p^{\mu q}$. Also, it is clear from the proofs of parts (b) and (c) of Lemma 3.1 that if $R \subset S$ is either ramified or decomposed, then $|S/M| = p^{2\mu}$. Furthermore, in both part (b) and (c), the asserted values of $|Z(S/M)|$ and $|U(S/M)|$ follow from the corresponding values that are asserted in that part for $|Z(S)|$ and $|U(S)|$ (by replacing the extension $R \subset S$ with the extension $R/M \subset S/M$, which has the effect of replacing λ with μ while leaving μ unchanged). Hence, in view of the statement and proof of Lemma 3.1, only the

following six items remain to be established: in (a), the asserted value of $|U(R)|$; in (b), the asserted values of $|S|$ and $|U(S)|$; in (c), the asserted value of $|U(S)|$; and in (d), the asserted values of $|S|$ and $|U(S)|$.

(a) Since (R, M) is quasi-local and finite,

$$|U(R)| = |R \setminus M| = |R| - |M| = p^{\lambda} - p^{\lambda-\mu} = p^{\lambda-\mu}(p^{\mu} - 1).$$

(b) Since $S/M \cong K[X]/(X^2)$, we have

$$|S/M| = |K|^2 = |R|^2/|M|^2 = p^{2\lambda-2(\lambda-\mu)} = p^{2\mu},$$

and so $|S| = |S/M| \cdot |M| = p^{2\mu}p^{\lambda-\mu} = p^{\lambda+\mu}$. Also, since (S, N) is quasi-local and finite, we see, as in the proof of (a), that $|U(S)| = |S \setminus N| = |S| - |N|$, which simplifies to the asserted value.

(c) By the proof of Lemma 3.1 (c), $|N_1 \cup N_2| = p^{\lambda-\mu}(2p^{\mu} - 1)$. So,

$$|U(S)| = |S \setminus (N_1 \cup N_2)| = |S| - |N_1 \cup N_2| = p^{\lambda+\mu} - p^{\lambda-\mu}(2p^{\mu} - 1) =$$
$$p^{\lambda-\mu}(p^{2\mu} - (2p^{\mu} - 1)) = p^{\lambda-\mu}(p^{\mu} - 1)^2.$$

(d) As $|S/M| = |\mathbb{F}_{p^{\mu q}}| = p^{\mu q}$,

$$|S| = |S/M| \cdot |M| = p^{\mu q}p^{\lambda-\mu} = p^{\mu q+\lambda-\mu} = p^{\lambda+\mu(q-1)} = p^{\lambda-\mu}p^{\mu q}.$$

Also, since (S, M) is quasi-local and finite, we see, as in the proof of (a), that $|U(S)| = |S \setminus M| = |S| - |M| = p^{\lambda-\mu}p^{\mu q} - p^{\lambda-\mu}$, which factors to give the asserted value. The proof is complete. □

For a commutative minimal ring extension S of a finite local ring R, Theorem 3.2 gave a lower bound for the non-negative integer $|Z(S)| - |Z(R)|$. Its proof relied heavily on Lemma 3.1. The proof of Lemma 3.5 also relied heavily on (the proof of) Lemma 3.1. We next give an application of Lemma 3.5. If commutative rings S and T are each minimal ring extensions of the same finite local ring R, Corollary 3.6 will include information about $|Z(S)|/|Z(T)|$ and $|U(S)|/|U(T)|$.

Corollary 3.6. *With this section's running hypothesis and notation remaining in place, we have the following:*

(a) Let the commutative rings S and T each be ramified (resp., decomposed; resp., inert) extensions of R. Then $|Z(S)| = |Z(T)|$ and $|U(S)| = |U(T)|$.

For parts (b)-(d), let S_r, S_i and S_d be commutative rings such that the ring extension $R \subset S_r$ is ramified, the ring extension $R \subset S_d$ is decomposed, and the ring extension $R \subset S_i$ is inert.

(b) $\frac{|Z(S_i)|}{|Z(S_r)|} = \frac{1}{p^{\mu}} \leq \frac{1}{p} \leq \frac{1}{2}$, $\frac{|Z(S_r)|}{|Z(S_d)|} = \frac{p^{\mu}}{2p^{\mu}-1} \leq \frac{p}{2p-1} \leq \frac{2}{3}$, *and*
$\frac{|Z(S_i)|}{|Z(S_d)|} = \frac{1}{2p^{\mu}-1} \leq \frac{1}{2p-1} \leq \frac{1}{3}$.

(c) $|Z(S_i)| < |Z(S_r)| < |Z(S_d)|$.

(d) $|U(S_d)| < |U(S_r)| < |U(S_i)|$.

Proof. (a) It suffices to observe that, by parts (b)-(d) of Lemma 3.5, there is a formula, that depends on (at most) p, λ and μ, by means of which both $|Z(S)|$ and $|Z(T)|$ (resp., both $|U(S)|$ and $|U(T)|$) can be calculated.

An alternate proof of the second assertion in (a) is available as follows. Having established that $|Z(S)| = |Z(T)|$, one can get $|U(S)| = |U(T)|$ by using the fact

(cf. [22, Theorem 84]) that any finite commutative ring Λ is the disjoint union of $Z(\Lambda)$ and $U(\Lambda)$, so that $|U(\Lambda)| = |\Lambda| - |Z(\Lambda)|$.

(b) After one substitutes the formulas for $|Z(S_r)|$, $|Z(S_d)|$ and $|Z(S_i)|$ from parts (d)-(d) of Lemma 3.5, the assertions follow easily.

(c) Apply (b).

(d) We will apply the relevant formulas from parts (b)-(d) of Lemma 3.5. First, observe that

$$\frac{|U(S_d)|}{|U(S_r)|} = \frac{p^{\lambda-\mu}(p^\mu - 1)^2}{p^\lambda(p^\mu - 1)} = \frac{p^\mu - 1}{p^\mu} < 1.$$

If follows that $|U(S_d)| < |U(S_r)|$.

It remains only to prove that $|U(S_r)| < |U(S_i)|$. Observe that

$$\frac{|U(S_r)|}{|U(S_i)|} = \frac{p^\lambda(p^\mu - 1)}{p^{\lambda-\mu}(p^{\mu q} - 1)} = \frac{p^\mu(p^\mu - 1)}{p^{\mu q} - 1}.$$

Our task is to show that the last-displayed quantity is less than 1. This fact holds in case $q = 2$, since

$$\frac{p^\mu(p^\mu - 1)}{p^{2\mu} - 1} = \frac{p^\mu}{p^\mu + 1} < 1.$$

Therefore, we can assume, without loss of generality, that $q \geq 3$. Then $p^{\mu q} - 1 \geq (p^{2\mu} + p^\mu + 1)(p^\mu - 1)$, and so it follows that

$$\frac{p^\mu(p^\mu - 1)}{p^{\mu q} - 1} = \frac{p^\mu}{(p^{\mu q} - 1)/(p^\mu - 1)} \leq \frac{p^\mu}{p^{2\mu} + p^\mu + 1} < \frac{1}{p+1} < 1.$$

The proof is complete. □

We next isolate the main upshot of combining parts (a)-(d) of Corollary 3.6.

Corollary 3.7. *With this section's running hypothesis and notation remaining in place, we have the following. Let S and T be commutative minimal ring extensions of a (finite local) ring R. Then the following conditions are equivalent:*

(1) $|Z(S)| = |Z(T)|$;

(2) $|U(S)| = |U(T)|$;

(3) $R \subset S$ and $R \subset T$ are the same type of minimal ring extension of R (that is, either (i) both are ramified or (ii) both are decomposed or (iii) both are inert).

Remark 3.8. (a) In stating Corollary 3.7, we emphasized this section's running hypothesis that R is a finite commutative local ring because that hypothesis cannot be weakened to R being a denumerable commutative local ring of Krull dimension 0. To see this, take $\mathcal{R}$ to be any denumerable field that is not algebraically closed (for instance, $\mathbb{Q}$ or $\mathbb{F}_p(X)$, for any prime number p). Let $\mathcal{S}_r$ (resp., $\mathcal{S}_d$; resp., $\mathcal{S}_i$) be a commutative ring that is a ramified (resp., decomposed; resp., inert) extension of $\mathcal{R}$. In other words, take (up to isomorphism) $\mathcal{S}_r = \mathcal{R}[Y]/(Y^2)$ (where Y and X are algebraically independent over $\mathcal{R}$) and $\mathcal{S}_d = \mathcal{R} \times \mathcal{R}$; and take $\mathcal{S}_i$ to be any minimal field extension of $\mathcal{R}$. Then, although $\mathcal{S}_r$, $\mathcal{S}_d$ and $\mathcal{S}_i$ are pairwise distinct types of minimal ring extensions of $\mathcal{R}$ (and $\mathcal{R}$ is a denumerable commutative local ring of Krull dimension 0), we have $|U(\mathcal{S}_r)| = |U(\mathcal{S}_d)| = |U(\mathcal{S}_i)| = \aleph_0$.

In fact, there is no upper bound on the cardinality of a commutative local ring $\mathfrak{R}$ of Krull dimension 0 such that $\mathfrak{R}$ is not a field and there exist commutative

rings $\mathcal{S}$ and $\mathcal{T}$ with the following properties: $\mathfrak{R} \subset \mathcal{S}$ is a ramified extension, $\mathfrak{R} \subset \mathcal{T}$ is a decomposed extension, and $|U(\mathcal{S})| = |U(\mathcal{T})| = |Z(\mathcal{S})| = |Z(\mathcal{T})|$. To see this, fix any infinite cardinal number κ, take F to be any (necessarily infinite) field such that $|F| > \kappa$, take Y to be an indeterminate over F (such that, for any ambient indeterminate X that may have already been specified, Y and X are algebraically independent over F), and put $\mathfrak{R} := F[Y]/(Y^2)$. It will be useful to note that $\mathfrak{R}$ is an SPIR (but not a field) whose only prime ideal, say $\mathfrak{M}$, is generated by the nonzero nilpotent element $y := Y + (Y^2)$. It follows that $|\mathfrak{R}| = |F|^2 = |F| = |Fy| = |\mathfrak{M}| = |Z(\mathfrak{R})| > \kappa$ and hence that $|U(\mathfrak{R})| = |U((F \setminus \{0\}) + Fy)| = |F|$ as well. (Our calculations involving infinite cardinal numbers in this paragraph are, of course, using the standard consequences of the Axiom of Choice, but we are not necessarily assuming the Continuum Hypothesis.) Put $\mathcal{S} := \mathfrak{R}(+)\mathfrak{R}/\mathfrak{M}$ (identified with $\mathfrak{R}(+)F$) and $\mathcal{T} := \mathfrak{R} \times \mathfrak{R}/\mathfrak{M}$ (identified with $\mathfrak{R} \times F$). By [15, Proposition 2.12], $\mathfrak{R} \subset \mathcal{S}$ is ramified and $\mathfrak{R} \subset \mathcal{T}$ is decomposed. It is now straightforward to identify the sets $U(\mathcal{S})$, $U(\mathcal{T})$, $Z(\mathcal{S})$ and $Z(\mathcal{T})$ and to confirm that each of these four sets has cardinality $|\mathfrak{R}|$ $(= |F|) > \kappa$, as asserted.

(b) Some readers may wish to draw a probabilistic inference from Corollary 3.6 (b), as follows. As in the running hypothesis, let R be a finite local ring. Suppose also that one has drawn a random zero-divisor ζ of S, where "randomness" is determined by a constant (that is, "uniform") probability function and S is known only to be a commutative minimal ring extension of R. Let S_r, S_d and S_i be as in parts (b)-(d) of Corollary 3.6. Put $N := |Z(S_r)| + |Z(S_d)| + |Z(S_i)|$. Assume also that the (finitely many) ring-isomorphism classes represented by minimal ring extensions of R are distributed with a constant probability function. It may then seem reasonable to say that the probability that ζ has been drawn from a ramified (resp., a decomposed; resp., an inert) extension of R is $|Z(S_r)|/N$ (resp., $|Z(S_d)|/N$; resp., $|Z(S_i)|/N$). If so, what can we say about these probabilities (let us denote them by p_r, p_d and p_i, respectively) as $p \to \infty$?

Recall from Corollary 3.6 (b) that

$$|Z(S_i)|/|Z(S_r)| \leq 1/p \text{ and } |Z(S_r)|/|Z(S_d)| = p^\mu/(2p^\mu - 1) \leq p/(2p-1).$$

Letting $p \to \infty$, we would find, using the standard limit theorems from calculus, that the limit of p_i is 0 and that the limit of p_r/p_d is 1/2. It would follow that for all sufficiently "large" values of p, the probability that ζ has been drawn from an inert extension of R is vanishingly small (one would say that this probability is 0 "in practical terms"); the probability that ζ has been drawn from a ramified extension of R is (approximately) 1/3; and the probability that ζ has been drawn from a decomposed extension of R is (approximately) 2/3. Readers who are attuned to such musings may then conclude that, as determined from the point of view of the relative prevalence of zero-divisors, for all sufficiently "large" values of p, the probability that a commutative minimal ring extension of a finite local ring R (of cardinality an integral power of p) is ramified (resp., decomposed; resp., inert) is approximately 1/3 (resp., approximately 2/3; resp., vanishingly small). For a reader who may view these conclusions as counter-intuitive, we would suggest focusing instead on the asymptotics in the above argument that

involved calculus-inspired calculations of limits of certain ratios that had arisen naturally in Corollary 3.6.

(c) Regardless of whether one is seeking probabilistic interpretations, it is interesting to consider the analogue of the asymptotics from (b) when the role of the zero-divisor operator $Z(-)$ is played, instead, by the unit operator $U(-)$. It turns out that one of the relevant quotients has a limit (as $p \to \infty$) that depends on the value of the prime number q (which arises when one is considering an inert minimal ring extension). As is often the case in algebra and number theory, the behavior of the prime number 2 is an outlier. We next give the main asymptotic results for $U(-)$, using formulas from the proof of Corollary 3.6 (d) as needed.

It is easy to see that

$$\lim_{p\to\infty} \frac{|U(S_d)|}{|U(S_r)|} = \lim_{p\to\infty} \frac{p^\mu - 1}{p^\mu} = 1.$$

It remains to evaluate only to evaluate

$$L := \lim_{p\to\infty} \frac{|U(S_r)|}{|U(S_i)|} = \lim_{p\to\infty} \frac{p^\mu(p^\mu - 1)}{p^{\mu q} - 1}.$$

If $q = 2$, then $L = \lim_{p\to\infty}(p^\mu/(p^\mu + 1)) = 1$. However, if $q \geq 3$, it follows from the proof of Corollary 3.6 (d) that

$$0 < \frac{p^\mu(p^\mu - 1)}{p^{\mu q} - 1} < \frac{1}{p+1}.$$

Thus, if $q \geq 3$, it follows from the so-called "Squeeze Limit Theorem" of calculus that $L = 0$. This completes the remark.

The next result gives an interesting connection between a commutative minimal ring extension $(R, M) \subset S$ and the related minimal ring extension $R/M \subset S/M$.

Corollary 3.9. *With this section's running hypothesis and notation remaining in place, we have the following. Let S be a (necessarily finite) commutative ring such that $R \subset S$ is a minimal ring extension. Then*

$$\frac{|Z(S/M)|}{|Z(R/M)|} = \frac{|Z(S)|}{|Z(R)|}.$$

Proof. We will offer two proofs. For the first proof, it suffices to treat separately the three possible cases (that is, where the minimal ring extension $R \subset S$ is either ramified, decomposed or inert) by using the formulas for $|Z(S/M)|$, $|Z(R/M)|$, $|Z(S)|$ and $|Z(R)|$ from the appropriate parts of Lemma 3.5. Indeed, after substituting those formulas, one can then verify the asserted equation by performing very straightforward calculations.

We turn to the second proof, where we will establish the following equivalent assertion:

$$\frac{|Z(S/M)|}{|Z(S)|} = \frac{|Z(R/M)|}{|Z(R)|}.$$

The second proof will also consider the three possible cases (where the minimal ring extension $R \subset S$ is either ramified, decomposed or inert), but will not need all of the specific formulas from Lemma 3.5. (Those formulas have already been of

significant use in proving Corollaries 3.6 and 3.7 and Remark 3.8 (c).) The proofs for the ramified and inert contexts will amount to little more than Lagrange's Theorem, while the proof for the decomposed case will replicate the derivation of some of the corresponding formulas from Lemmas 3.1 and 3.5. Suppose first that $R \subset (S, N)$ is ramified. Then S/M is quasi-local with maximal ideal N/M and

$$\frac{|Z(S/M)|}{|Z(S)|} = \frac{|N/M|}{|N|} = \frac{|N|/|M|}{|N|} = \frac{1}{|M|} = \frac{|Z(R/M)|}{|Z(R)|}.$$

Suppose next that $R \subset (S, M)$ is inert. Then, by replacing the symbol N with M in the last display, one gets a proof for the inert case. For the final (and hardest) case, suppose that $R \subset S$ is decomposed. Let N_1 and N_2 denote the two (distinct) prime (maximal) ideals of S. As we have seen (with the aid of [22, Theorem 84]), $Z(S) = N_1 \cup N_2$. Similarly, $Z(S/M) = N_1/M \cup N_2/M$. Then, since $N_1/M \cap N_2/M = (N_1 \cap N_2)/M = M/M = 0$,

$$|Z(S/M)| = |N_1/M \cup N_2/M| = |N_1/M| + |N_2/M| - |0| =$$
$$\frac{|N_1|}{|M|} + \frac{|N_1|}{|M|} - 1 = \frac{|N_1| + |N_2| - |M|}{|M|} = \frac{|Z(S)|}{|Z(R)|}.$$

Because of the last display, we see that the assertion is equivalent to $|Z(R/M)| = 1$. This, in turn, is evident, since R/M is a field. This completes the (second) proof. □

We next give an analogue of Corollary 3.9 in which the zero-divisor operator $Z(-)$ is replaced by the units operator $U(-)$. In the proof of Corollary 3.10, it will be convenient to let $J(\Lambda)$ denote the Jacobson radical of a ring Λ.

Corollary 3.10. *With this section's running hypothesis and notation remaining in place, we have the following. Let S be a (necessarily finite) commutative ring such that $R \subset S$ is a (necessarily integral) minimal ring extension. Then there is an isomorphism of multiplicative groups*

$$U(S/M)/U(R/M) \cong U(S)/U(R), \quad \textit{and so} \quad \frac{|U(S/M)|}{|U(R/M)|} = \frac{|U(S)|}{|U(R)|}.$$

In particular, the group-theoretic indexes $[U(S/M) : U(R/M)]$ and $[U(S) : U(R)]$ are equal.

Proof. The canonical surjective ring homomorphism $\pi : S \to S/M$ induces a group homomorphism $f : U(S) \to U(S/M)$. We claim that f is surjective. Indeed, let $\xi \in U(S/M)$. Then there exists $\eta \in U(S/M)$ such that $\xi\eta = 1$ $(= 1+M) \in S/M$. Pick $s, t \in S$ such that $\pi(s) = \xi$ and $\pi(t) = \eta$; that is, such that $\xi = s+M$ and $\eta = t+M$. Since $st+M = (s+M)(t+M) = 1+M \in S/M$, we have $st-1 \in M$, and so $st \in 1+M = 1+J(R)$. As the ring extension $R \subset S$ is integral, $J(R) \subseteq J(S)$ (cf. [2, Exercise 5 ii), page 67]), and so $st \in 1 + J(S) \subseteq U(S)$. Let $v := (st)^{-1} \in S$ and consider $w := tv \in S$. As $sw = (st)v = 1$, we get $s \in U(S)$. Hence, working inside S/M gives $f(s) = \pi(s) = \xi \in U(S/M)$. This proves the claim that f is surjective.

As the ring extension $R \subset S$ is unital, we have that $U(R)$ is an abelian (hence normal) subgroup of the multiplicative group $U(S)$. Also, by repeating the above

reasoning for $f|_{U(R)}$, we see that $f(U(R)) = U(R/M)$. Therefore, by a standard homomorphism theorem in group theory,

$$U(S)/U(R) \cong f(U(S))/f(U(R)) = U(S/M)/U(R/M),$$

thus proving the first assertion. The final two assertions are then immediate.

Note that the second and third assertions are equivalent by Lagrange's Theorem. For an alternate (and direct) proof of the second assertion (and hence of the third assertion) that avoids establishing a group isomorphism, we can argue as in the style of the first proof of Corollary 3.9. Indeed, for that purpose, it suffices to treat separately the three possible cases (that is, where the minimal ring extension $R \subset S$ is either ramified, decomposed or inert) by using the formulas for $|U(S/M)|$, $|U(R/M)|$, $|U(S)|$ and $|U(R)|$ from the appropriate parts of Lemma 3.5. □

We close by collecting some comments pertinent to the title of this section.

Remark 3.11. Suppose that we "know" a finite commutative local ring R. (This would include knowing the maximal ideal M of R and, hence, both $|Z(R)|$ $(= |M|)$ and the relevant prime number p.) What do the results of this section allow us to conclude about a commutative ring S if we know only $|Z(S)|$ and the fact that S is a minimal ring extension of R? Note first that S is finite. Next, by Lemma 3.1 (e), we can conclude that $R \subset S$ is inert if and only if $|Z(S)| = |Z(R)|$. Next, by Theorem 3.2, if $|Z(S)| = p|Z(R)|$, then $R \subset S$ is ramified and $R/M \cong \mathbb{F}_p$.

One could ask some related questions. One of those was answered in Corollary 3.7. Here is another question. Suppose that we "know" a commutative ring S. What do the results of this section allow us to conclude about a finite local ring (R, M) if we know only that S is a minimal ring extension of R? If S is not local, then $R \subset S$ is decomposed and so we can conclude, by Lemma 3.5, that $|R| = (p^\lambda =)\ |S|$. If S is local, then $R \subset S$ is either ramified or inert. If we knew that we were in the "ramified" context, then we could conclude that $|R| = (p^\lambda =)\ |Z(S)|$. However, we could not determine $|R|$ in the "inert" context. Indeed, there exist inert extensions (in fact, minimal field extensions) $A \subset C$ and $B \subset C$ such that C is a finite commutative ring, both A and B are local, and $|A| \neq |B|$. Somewhat elaborate examples of this situation can be gleaned from [14, Examples 2.2 and 2.3]. (However, to use the first (resp., second) of these just-cited examples, one would have to find a Galois extension of finite fields having Galois group the symmetric group S_5 (resp., the alternating group A_4) and then use Galois Theory to conclude that $|A| \neq |B|$.) For the easiest example (with p any prime number), take $A := \mathbb{F}_{p^2}$, $B := \mathbb{F}_{p^3}$ and $C := \mathbb{F}_{p^6}$.

References

1. N. Al-Kuleab and N. Jarboui, *A note on intermediate matrix rings*, Far East Journal Math. Edu. **17** (4) (2018), 227-229.
2. M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, MA, 1969.
3. G. Bini and F. Flamini, Finite Commutative Rings and their Applications, Kluwer International Series in Engineering and Computer Science, Vol. 680, Kluwer, Boston, 2002.

4. M. E. Charkani and J. Kabore, *Primitive idempotents and constacyclic codes over finite chain rings*, Gulf J. Math. **8** (2) (2020), 55-67.
5. D. E. Dobbs, *Every commutative ring has a minimal ring extension*, Comm. Algebra **34** (10) (2006), 3875-3881.
6. D. E. Dobbs, *When the juxtaposition of two minimal ring extensions produces no new intermediate rings*, Pales. J. Math. **6** (1) (2017), 31-44. *Corrigendum* (unrelated to the present article), Pales. J. Math. **7** (1) 2018, 32-34.
7. D. E. Dobbs, *On the commutative rings with at most two proper subrings*, Int. J. Math. Math. Sci., Vol. 2016, Article ID 6912360, 13 pages, 2016. doi:10.1155/2016/6912360.
8. 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.
9. 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.
10. D. E. Dobbs, *On algebras over a finite direct product of commutative rings*, Moroccan Journal of Algebra and Geometry with Applications, to appear.
11. D. E. Dobbs and N. Jarboui, *Characterizing finite Boolean rings by using finite chains of subrings*, Gulf J. Math. **10** (1) (2021), 69-94.
12. D. E. Dobbs and B. Mullins, *On the lengths of maximal chains of intermediate fields in a field extension*, Comm. Algebra **29** (10) (2001), 4487-4507.
13. 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.
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. D. E. Dobbs and J. Shapiro, *A classification of the minimal ring extensions of certain commutative rings*, J. Algebra **308** (2007), 800-821.
16. D. E. Dobbs and J. Shapiro, *When only finitely many intermediate rings result from juxtaposing two minimal ring extensions*, Pales. J. Math. **5** (Spec1) (2016), 13-31.
17. T. J. Dorsey and Z. Mesyan, *On minimal extensions of rings*, Comm. Algebra **37** (2009), 3463-3486.
18. D. Ferrand and J.-P. Olivier, *Homomorphismes minimaux d'anneaux*, J. Algebra **16** (1970), 461-471.
19. I. N. Herstein, Noncommutative Rings, Math. Assn. America, Carus Monographs, Vol.15, distributed by John Wiley and Sons, Inc., New York, 1968.
20. J. A. Huckaba, Commutative Rings with Zero Divisors, Monographs and Textbooks in Pure Appl. Math., Vol. 117, Marcel Dekker, Inc., New York, 1988.
21. T. W. Hungerford, Algebra, Graduate Texts in Math., Vol. 73, Springer-Verlag, New York-Berlin, 1980.
22. I. Kaplansky, Commutative Rings, revised edition, Univ. Chicago Press, Chicago/London, 1974.
23. O. A. S. Karamzadeh and N. Nazari, *On maximal commutative subrings of non-commutative rings*, Comm. Algebra **46** (12) (2018), 5083-5115.
24. A. A. Klein, *The finiteness of a ring with a finite maximal subring*, Comm. Algebra **21** (4) (1993), 1389-1392.
25. M. Kosters, *Algebras with only finitely many subalgebras*, J. Algebra Appl. **14** (6) (2015), 1550086, 19 pp.
26. T. J. Laffey, *A finiteness theorem for rings*, Proc. Roy. Irish Acad. Sect. A **92** (2) (1992), 285–288.
27. B. R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.
28. 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.

29. G. Picavet and M. Picavet-L'Hermitte, *Modules with finitely many submodules*, Internat. Electron. J. Algebra **19** (2016), 119-131.
30. S. Visweswaran and H. Patel, *The union of two graphs associated with the set of all non-zero annihilating ideals of a commutative ring*, Gulf J. Math. **11** (1) (2021), 83-104.

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