



ISSN: 2820-7114

# Moroccan Journal of Algebra and Geometry with Applications

Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco

Volume 2, Issue 2 (2023), pp 272-290

**Title :**

**On the nature and number of the noncommutative minimal ring extensions of a field**

**Author(s):**

**David E. Dobbs**

## On the nature and number of the noncommutative minimal ring extensions of a field

David E. Dobbs

Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320  
e-mail: [ddobbs1@utk.edu](mailto:ddobbs1@utk.edu)

Communicated by Najib Mahdou

(Received 06 June 2023, Revised 20 August 2023, Accepted 05 September 2023)

**Abstract.** It is known that if  $k$  is a field, then any noncommutative minimal ring extension of  $k$  is either a prime ring or a non-semiprime ring. Our results include the following. If  $R$  is a ring, the collection of  $R$ -isomorphism classes represented by minimal ring extensions of  $R$  is a set. If  $X$  is an indeterminate over a field  $k$ , the cardinal number of the set of  $k(X)$ -isomorphism classes represented by noncommutative minimal ring extensions of  $k(X)$  is infinite, at least denumerably many of those classes have representatives which are simple (and left- and right-Artinian) rings (and, hence, prime rings), and if one also assumes that the field  $k$  is infinite, then at least denumerably many of those classes have representatives which are non-semiprime rings. If  $k$  is any algebraically closed field (more generally, a field with infinitely many automorphisms), the set of  $k$ -isomorphism classes represented by noncommutative minimal ring extensions of  $k$  is infinite and the representatives of infinitely many of those classes are non-semiprime rings. If  $k$  is a finite field of characteristic  $p$  and of cardinality  $p^n$  with  $n > 1$ , the cardinal number of the set of  $k$ -isomorphism classes represented by noncommutative minimal ring extensions of  $k$  is at least  $n$ , and at least  $n - 1$  of those classes can be represented by a non-semiprime ring. If  $p$  is a prime number, then for finite fields  $k$  of characteristic  $p$ , there is no absolute finite upper bound on the cardinal number of the set of  $k$ -isomorphism classes represented by noncommutative minimal ring extensions of  $k$  that are simple (hence, prime) rings.

**Key Words:** Unital associative ring, minimal ring extension, field, simple ring, prime ring, noncommutative, field extension, finite field, algebraically closed field, Dorroh extension, ring bimodule, Lüroth's Theorem, skew polynomial ring.

**2010 MSC:** Primary 16B99; Secondary 12F05, 12F10, 16S50, 16D20, 13B99, 12F20, 16P10.

### 1 Introduction

All rings considered here are assumed to be unital and associative, but not necessarily commutative; unless adorned with one of the adjectives "left," "right" or "one-sided," an "ideal" will be assumed to be a two-sided ideal. All inclusions of rings, ring extensions, subrings, algebras, (bi)modules and ring/algebra homomorphisms will be assumed unital. Proper inclusions will be denoted by  $\subset$ . Recall that if  $\Lambda \subset \Gamma$  are (distinct) rings, then  $\Lambda \subset \Gamma$  is called a *minimal ring extension* (and  $\Gamma$  is called a *minimal ring extension of  $\Lambda$* ) if there does not exist a ring  $\Omega$  such that  $\Lambda \subset \Omega \subset \Gamma$ . Although the original definition of "minimal ring extension" (in [14]) also required ( $\Lambda$  and)  $\Gamma$  to be commutative and minimal ring extensions involving commutative rings have been extensively investigated, the "minimal ring extension" concept has been fruitfully studied for arbitrary rings in recent years, in papers such as [13] and [1]. There is some evidence indicating that noncommutative minimal ring extensions may be plentiful. For instance, it was shown in [1] that if  $\Lambda \subset \Gamma$  are rings and  $n \geq 2$  is an integer, then the ring extension consisting of the (noncommutative) matrix rings  $M_n(\Lambda) \subset M_n(\Gamma)$  is a minimal ring extension if and only if  $\Lambda \subset \Gamma$  is a minimal ring extension. On the other hand, it was shown recently that for any prime number  $p$ , the finite field  $\mathbb{F}_p$  is, up to isomorphism, the only field of characteristic  $p$  that does not have a noncommutative minimal ring extension [8, Theorem 2.1], although  $\mathbb{F}_p$  has infinitely many pairwise non-isomorphic commutative minimal ring extensions

(some of which are given by the fields  $\mathbb{F}_q$  as  $q$  ranges over the set of prime numbers, the point being that any minimal field extension is necessarily algebraic and, hence, a minimal ring extension: cf. [2, Proposition 5.7], [18, Theorem 44]). The deepest study to date of possibly noncommutative minimal ring extensions was in [13], and several results from that paper by Dorsey and Mesyan will be of use here.

In [13], Dorsey and Mesyan have given a clearly delineated overview of the minimal ring extensions of an arbitrary ring. I believe that additional work in this area may benefit from the development of a few more concrete examples. If one grants the appropriateness of such work, it is natural to ask where/how it should begin. Any objective record of the studies of the minimal ring extensions where the “top” ring is commutative (that is, where both partners in the ring extension are commutative) would begin with the following classification result, due to Ferrand and Olivier [14, Lemme 1.2]: if  $K$  is a field and  $S$  is a commutative ring such that  $K \subseteq S$ , then  $K \subset S$  is a minimal ring extension if and only if (exactly) one of the following three conditions holds:  $S$  is  $K$ -algebra isomorphic to  $K[X]/(X^2)$  where  $X$  is a commuting indeterminate over  $K$  (and where we view  $K \subseteq K[X]/(X^2)$  via the unique  $K$ -algebra homomorphism  $K \rightarrow K[X]/(X^2)$ );  $S$  is  $K$ -algebra isomorphic to  $K \times K$  (where we view  $K \subseteq K \times K$  via the unique  $K$ -algebra homomorphism  $K \rightarrow K \times K$ );  $S$  is  $K$ -algebra isomorphic to a minimal field extension of  $K$ . In reporting activity since 2006 in this area, an objective record would note that the study naturally bifurcated into separate studies of the integral minimal ring extensions (with commutative “top” ring) and of the integrally closed minimal ring extensions (with commutative “top” ring), with the “integral” studies further segmenting into the now-familiar “ramified-decomposed-inert” trifurcation [11, Lemma II.3] (see another approach to the “integral” case in [22]) and the “integrally closed” studies intimately involved with Kaplansky transforms (cf. [12, Section 3]) and various generalized Kaplansky transforms (cf. [3]). In the just-mentioned studies, classifications of the minimal ring extensions  $R \subset S$  were attempted (and often achieved) up to  $R$ -algebra isomorphism. Perhaps it would be too much to hope to obtain that kind of information when the minimal ring extensions  $S$  are not commutative. After all, even if  $R \subset S$  is a minimal ring extension and  $R$  is commutative, there is no reason to expect  $S$  to be commutative. Indeed, the fact that  $S$  need not be an  $R$ -algebra under these conditions was deeply involved in my construction, in [8, Theorem 2.1], of a noncommutative minimal ring extension for “most” base fields of positive characteristic. As the work of more than the past half-century in noncommutative ring theory does not seem to have developed a variant of integrality (or of integrally closedness) for arbitrary ring extensions that would be sufficiently tractable for our purposes, it seems prudent to begin looking for what I called “a few more concrete examples” by focusing on base rings which are fields. That is what we will do here.

By way of partial summary of the preceding paragraph, this work will study the noncommutative minimal ring extensions  $S$  of a field  $k$ . Although we cannot use algebraicity-related concepts in such a study, it would be nice (given the nature of the “commutative” work summarized above) if one could classify such  $S$  up to ring isomorphism, possibly even up to something that could be called “ $k$ -isomorphism.” More generally, if such studies make progress, one could hope to eventually study minimal ring extensions  $S$  of a noncommutative ring  $R$  and to concretely classify such objects up to “ $R$ -isomorphism.” Fortunately, several of the results in [13] assert classifications of the minimal ring extensions of a ring  $R$  (with sharper information if  $R$  is further restricted) and it is asserted that these classifications are “up to  $R$ -isomorphism.” Unfortunately, I maintain (with some sadness) that *when  $R$  is a ring, the term “ $R$ -isomorphism” is not explicitly defined in [13].* (A similar comment applies to the term “ $R$ -homomorphism.”) Possibly fortunately, when  $R$  is an rng (that is, what used to be called “a ring possibly without identity” – or just a “ring” in older, but very good, books such as [23]) and  $R \subset S$  is an rng-extension in the obvious sense, the term “ $R$ -isomorphism” is defined in [13]. So, we will have to take extra care when appealing to results from [13]. This extra care will be of three kinds. First, when certain rng-isomorphisms from [13] are applied to rings, we will need to check that the

maps in questions are unital. Second, instead of applying a complicated rng-theoretic proof or series of such proofs from [13], we may give a short *ad hoc* proof of a special case that will be adequate for the present purposes. (Note that many computational details in proofs in [13] were left to the reader, and so settling for proofs of special cases will save us a lot of time and space here.) Third, and most urgently, we must define, when  $R \subseteq S$  and  $R \subseteq T$  are rings, what it means for a ring homomorphism  $S \rightarrow T$  to be an “ $R$ -homomorphism” or an “ $R$ -isomorphism.” The next two paragraphs give those definitions.

The next two sentences are the result of slightly editing part of the first paragraph of [9, Remark 2.10 (b)]. It seems clear from reading [13] that its authors intended an “ $R$ -isomorphism”  $S \rightarrow T$  to have as many of the familiar properties of an algebra isomorphism (over a commutative base ring) that would be reasonable in a not-necessarily-commutative setting. This feeling is only reinforced by reading the definitions in [13, pages 3465-3466], given a ring  $R$ , of an  $R$ -ring, an  $R$ -rng, and an  $R$ -homomorphism from one  $R$ -rng to another. The rest of this paragraph is, apart from a few mild stylistic changes, a direct quotation of material from [13, pages 3465-3466]. Given a ring  $R$ , an  $R$ -ring (resp.,  $R$ -rng)  $I$  is a ring (resp., rng) that is a (unital)  $R$ - $R$  bimodule for which the actions of  $R$  are compatible with multiplication in  $I$ , in the following sense:

$$(rx)y = r(xy), (xr)y = x(ry) \text{ and } (xy)r = x(yr) \text{ if } r \in R, x \in I, y \in I.$$

Note that a ring homomorphism  $R \rightarrow I$  equips  $I$  with the structure of an  $R$ -ring in a natural way; in particular, in this way every ring extension of  $R$  may be viewed as an  $R$ -ring. We will call a nonzero  $R$ -rng a *minimal  $R$ -rng* if it and 0 are its only  $R$ -subrngs. We note that if  $I$  is a minimal  $R$ -rng with  $I^2 \neq 0$ , then  $I$  is simple as an rng (in the sense that it has precisely two distinct two-sided ideals). If  $I$  and  $J$  are (possibly equal)  $R$ -rngs, then we define an  $R$ -( $R$ -rng)-homomorphism from  $I$  to  $J$  to be any homomorphism of  $R$ -rngs  $I \rightarrow J$  which is also an  $R$ - $R$  bimodule homomorphism  $I \rightarrow J$ .

Using the material in the previous paragraph, the next sentence gives the crucial definition. If  $R$  is a ring, with  $S$  and  $T$  (possibly equal)  $R$ -rings (for instance, if both  $R \subseteq S$  and  $R \subseteq T$  are ring extensions), then we define an  $R$ -( $R$ -ring)-homomorphism from  $S$  to  $T$  to be any unital  $R$ -( $R$ -rng)-homomorphism from  $S$  to  $T$ ; that is, any ring homomorphism  $S \rightarrow T$  which is also an  $R$ - $R$  bimodule homomorphism. As the composite of  $R$ - $R$  bimodule homomorphisms is also an  $R$ - $R$  bimodule homomorphism, it follows easily that the composite of any  $R$ -ring-homomorphisms is itself an  $R$ -ring-homomorphism. One then has, in the obvious way, the category of  $R$ -rings and hence, on categorical grounds, one knows what should be meant by an “isomorphism” in that category. Of course, that amounts to a bijective unital  $R$ -( $R$ -rng)-homomorphism; that is, a ring isomorphism that is an  $R$ - $R$  bimodule homomorphism. **Accordingly, we will say that  $S$  and  $T$  are isomorphic as  $R$ -rings (or that  $S$  and  $T$  are  $R$ -ring-isomorphic or that  $S$  and  $T$  are  $R$ -isomorphic) if and only if there exists a ring isomorphism  $f : S \rightarrow T$  that is an  $R$ - $R$  bimodule homomorphism, in which case we also say that  $f$  is an  $R$ -( $R$ -ring)-isomorphism (from  $S$  to  $T$ ).**

Some readers may find the following observations to be useful. Let  $R$  be a commutative ring. Then an  $R$ -ring is the same as an  $R$ -algebra and if  $S$  and  $T$  are  $R$ -rings, an  $R$ -ring-homomorphism (resp., an  $R$ -ring-isomorphism) from  $S$  to  $T$  is the same as an  $R$ -algebra homomorphism (resp., an  $R$ -algebra isomorphism) from  $S$  to  $T$ .

Now that we have argued for a purposeful development of some concrete examples of noncommutative minimal ring extensions of a field, it is time to decide on a vantage point from which alleged success could be measured. I would suggest that our collective experience in learning/teaching about groups and rings can play a role in selecting such a vantage point. Consider, in group theory, the value obtained in answering a question asking for the classification, up to isomorphism, of all the groups of a specific order (that is, cardinality)  $n$ : for a mild example of such a question, see [16, Exercise 9, page 100]. In ring theory (actually, rng theory), it was considerably more difficult, for a given prime number  $p$ , to classify up to isomorphism, all the rngs of cardinality  $p^3$  (and I would assert that

even more value was obtained when this was accomplished): see [6, Remark 3.10 (a)] (as well as the works cited there, as well as the Math Reviews of those works). These experiences suggest to me that a suitable focus for our work here should be on the question of *how many* isomorphism classes (or on the question of how many  $k$ -isomorphism classes) can be represented by noncommutative minimal ring extensions of a given field  $k$ . Before that question can be addressed, one would first need to show that the collection of isomorphism classes at issue has a cardinal number, that is, that this collection is a set. Accordingly, we begin Section 2 with a result (Proposition 2.1) which essentially does just that. Then, in Proposition 2.2, we recall the classification by Dorsey and Mesyan of the classification up to  $R$ -isomorphism, of the minimal ring extensions of a simple ring  $R$ . That helps to sharpen some of the findings in Proposition 2.1 and, together with an enhanced “unital” version of a result of G. Bergman that was reported in [13] and an application of the classical Galois theory for finite fields, we find in Theorem 2.8 (c) that for any finite field of cardinality  $p^n$ , where  $p$  is a prime number and  $n > 1$ , the cardinal number of the set of  $k$ -isomorphism classes that are represented by noncommutative minimal ring extensions of  $k$  is at least  $n$ . Sharper information is available, as we use the cited work from [13] to show that any noncommutative minimal ring extension of a field  $k$  either is a prime ring or is not a semiprime ring. (Background on prime and simple rings is given in Section 2 before the statement of Proposition 2.2.) The work here goes well beyond the example given in the main result of [8], and it also shows that for any prime number  $p$ , there is no finite absolute upper bound on the cardinal number of the set of  $k$ -isomorphism classes represented by the noncommutative minimal ring extensions that are prime rings (resp., that are non-semiprime rings) of a given finite field  $k$  of characteristic  $p$ : see Corollary 2.9. But we have not settled the question of whether – for any one such  $k$  – the corresponding cardinal number is finite. (Of course, the classical theory of field extensions shows that the cardinal number of the set of commutative minimal ring extensions of any given finite field is  $\aleph_0$ .) This work leads naturally to the question of whether there exist some “naturally occurring” infinite fields  $k$  for which the collection of  $k$ -isomorphism classes represented by the noncommutative minimal ring extensions of  $k$  is infinite. In that regard, we give affirmative answers for two classes of infinite fields, namely, the algebraically closed fields (see Theorem 2.12 (ii)) and the fields generated by a transcendental element over some subfield (see Theorem 2.10). As the cardinal number of the collection of  $k$ -ring-isomorphism classes of a given field  $k$  that can be represented by noncommutative minimal ring extensions of  $k$  can be finite (consider  $k := \mathbb{F}_p$  for any prime number  $p$  or  $k := \mathbb{Q}$ ) and we show in Section 2 that this number can be infinite for certain infinite fields  $k$ , we close with Remark 2.14 which discusses some possibilities for future work in this area.

Minimal ring extensions  $R \subset S$  where  $R$  and  $S$  are finite rings will be of special interest here (especially in case  $R$  is a finite field). Actually, if  $R \subset S$  is a minimal ring extension and  $R$  is a finite ring, then  $S$  is also a finite ring. This fact was recently easily proven in [10, Lemma 2.1 (c)] as a consequence of a deep noncommutative result on ring extensions, due independently to Klein [19] and Laffey [20].

As usual,  $|\mathcal{U}|$  denotes the cardinal number of a set  $\mathcal{U}$ ;  $\mathbb{F}_s$  denotes the finite field of cardinality  $s$ , for any prime-power  $s$ ; a *simple ring* is a nonzero ring (which is not necessarily left- or right-Artinian ring, but) whose only ideals are 0 and itself;  $\deg(h)$  denotes the degree of a polynomial  $h$ ; and  $X$  denotes an indeterminate over any ambient commutative ring(s). Unexplained material is standard, as in [2], [16].

## 2 Results

As we will be interested in finding an upper bound on the (cardinal) number of the collection of isomorphism classes represented by minimal ring extensions of a given ring  $R$ , it will first be necessary to show that this collection is a set (since only sets can have cardinal numbers). Showing

that will follow rather easily from a crude upper bound on the cardinality of any such minimal ring extension. That upper bound is given in Proposition 2.1 (a). Parts (b)-(e) of Proposition 2.1 collect applications of that upper bound which will be useful below. Since it was noted in the Introduction that any minimal ring extension of a finite ring must itself be finite, those applications emphasize infinite cardinal numbers. As we are assuming the ZFC foundations of set theory, the familiar laws of arithmetic with cardinal numbers (as in, for instance, [15]) can and will be used in the proof of Proposition 2.1. These laws include the facts that if  $n$  is a nonzero finite cardinal number, while  $\kappa_1$  and  $\kappa_2$  are (possibly equal) infinite cardinal numbers, then

$$n + \kappa_i = \kappa_i = n \cdot \kappa_i \text{ and } \kappa_1 + \kappa_2 = \max(\kappa_1, \kappa_2) = \kappa_1 \cdot \kappa_2.$$

The interested reader will find that the method of proof of Proposition 2.1 can be tweaked so that it applies to arbitrary ring extensions  $R \subset T$  where the cardinal numbers of  $R$  and  $S$  are given, where  $S$  is a subset of  $T \setminus R$  such that  $R \cup S$  generates  $T$  as a ring.

**Proposition 2.1.** (a) Let  $R \subset T$  be a minimal ring extension. Let  $s \in T \setminus R$  (so that  $T$  is generated as a ring by  $R \cup \{s\}$ ). Put  $\kappa := |R|$  and  $\sigma := \max(\kappa, \aleph_0)$ . Then  $|T| \leq \sigma$ .

(b) Let  $\sigma$  be any nonzero cardinal number. Then the collection of ring isomorphism classes represented by rings of cardinality  $\sigma$  is a set, and the cardinality of that set is at most  $\sigma^{(2\sigma^2)}$ . If  $\sigma$  is infinite, this upper bound is  $2^\sigma$ .

(c) Let  $N$  be a positive integer (that is, a nonzero finite cardinal number). Then the collection of ring isomorphism classes represented by a minimal ring extension of a ring of cardinality  $N$  is a set. Moreover, the cardinality of that set is at most  $\aleph_0$ ; that is, that set is either finite or denumerable.

(d) Let  $k$  be a denumerable field; that is, let  $|k| = \aleph_0$ . (For instance, take  $k := F(X)$ , where  $F$  is a finite field and  $X$  is a (commuting) indeterminate over  $F$ .) Then the collection of  $k$ -isomorphism classes represented by a minimal ring extension of  $k$  is a set, and the cardinality of that set is at most  $2^{\aleph_0}$ .

(e) Let  $R$  be an infinite ring. Put  $\kappa := |R|$ . Then the collection of  $R$ -isomorphism classes represented by a minimal ring extension of  $R$  is a set, and the cardinality of that set is at most  $2^\kappa$ .

*Proof.* (a) Let  $n \geq 2$  be an integer. It will be convenient to say (but only in this proof) that each element of  $R$  has length 1 and that an element  $t \in T \setminus R$  has length  $n$  if

$$t = r_1 s r_2 s r_3 \cdots s r_n,$$

where  $r_j \in R$  for all  $j = 1, 2, \dots, n$ . Note that an element of  $T \setminus R$  can have length  $n_1$  and can also have length  $n_2$  with  $n_1 \neq n_2$ , while it is possible that an element of  $T \setminus R$  may not have any "length" at all. Notice also that the subset of  $T$  consisting of the elements having length 1 is  $R$ , which is a set of cardinality  $\kappa$ . Also, the element  $s$  has length 2, since  $s = 1 \cdot s \cdot 1$ . It will also be useful to note, as the result of an easy case analysis, that if  $t_1$  has length  $n_1$  and  $t_2$  has length  $n_2$ , then  $t_1 t_2$  has length  $n_1 + n_2 - 1$ . Note also that for each integer  $n \geq 2$ , the cardinal number of the set of elements of  $T$  which have length  $n$  is at most  $\kappa^n$ ; of course, if  $R$  is infinite, this upper bound is just  $\kappa$ . Hence, for each positive integer  $n$ , the cardinal number of the set of elements of  $T$  which have length  $n$  is at most  $\max(\kappa, \aleph_0) = \sigma$ .

In this paragraph, let us consider a finite, strictly increasing list of positive integers

$$n_1, n_2, \dots, n_d.$$

Then the cardinal number of the set of elements  $t \in T$  which can be expressed as

$$t = t_1 + t_2 + \cdots + t_d,$$

where  $t_j \in T$  has length  $j$  for each  $j = 1, 2, \dots, d$  is at most

$$\sigma \cdot \sigma \cdot \dots \cdot \sigma = \sigma^d = \sigma$$

(since there are at most  $\sigma$  independent choices for each of the  $t_j$ ).

Now consider the set  $\mathcal{T}$  of elements  $t \in T$  that can be expressed as

$$t = u_1 + u_2 + \dots + u_e,$$

where  $e$  is a positive integer and there exists a finite, strictly increasing list  $\nu_1, \nu_2, \dots, \nu_e$  of positive integers such that  $u_j \in T$  has length  $\nu_j$  for each  $j = 1, 2, \dots, e$ . It is easy to show (by using the result of an above-mentioned easy case analysis) that  $\mathcal{T}$  is closed under addition. Then, by using the distributive property, one sees easily that  $\mathcal{T}$  is also closed under multiplication. Since  $R \subseteq \mathcal{T}$  and  $s \in \mathcal{T}$ , we have that  $\mathcal{T}$  is a subring of  $T$  which contains  $R \cup \{s\}$ . Consequently  $\mathcal{T} = T$ . As the cardinal number of the set of finite, strictly increasing lists of positive integers is easily seen to be  $\aleph_0$ , it therefore follows from the preceding paragraph that  $T$  is the (not necessarily disjoint) union, with index set of cardinality at most  $\aleph_0$ , of sets each of which has cardinality at most  $\sigma$ . Hence,  $|T| \leq \aleph_0 \cdot \sigma = \max(\aleph_0, \sigma) = \sigma$ , as asserted.

(b) Pick a set  $\mathcal{S}$  such that  $|\mathcal{S}| = \sigma$ . Any ring of cardinality  $\sigma$  can be given, up to isomorphism, by prescribing suitable binary operations of addition and multiplication on  $\mathcal{S}$ . The collection of binary operations on  $\mathcal{S}$  is in one-to-one correspondence with the collection of functions from  $\mathcal{S} \times \mathcal{S}$  to  $\mathcal{S}$ . The cardinal number of *that* collection is

$$|\mathcal{S}|^{|\mathcal{S} \times \mathcal{S}|} = |\mathcal{S}|^{|\mathcal{S}| \cdot |\mathcal{S}|} = \sigma^{\sigma \cdot \sigma}.$$

Thus, the number of ways of independently choosing candidates for the binary operations of addition and multiplication for a ring having  $\mathcal{S}$  as its underlying set (note that many of those choices do not satisfy the axioms for a ring) is  $(\sigma^{\sigma \cdot \sigma})^2 = \sigma^{(2\sigma^2)}$ . Hence, the just-mentioned cardinal number is an upper bound for the cardinal number of the collection of ordered pairs whose first (resp., second) "coordinate" is the addition (resp., multiplication) operation on  $T$ , as  $T$  runs through a preassigned set of isomorphism class representatives of the rings of cardinality  $\sigma$  (where, without loss of generality, each such  $T$  has underlying set  $\mathcal{S}$ ). Bearing in mind that any "subclass" of a set is a set, we have proved the first assertion in (b). The final assertion in (b) follows from the Schroeder-Bernstein Theorem. (In detail: observe that  $2\sigma^2 = 2\sigma = \sigma$  and  $2^\sigma \leq \sigma^\sigma \leq (2^\sigma)^\sigma = 2^{(\sigma^2)} = 2^\sigma$ .)

(c) If  $R \subset T$  is a minimal ring extension and  $|R| = N$ , then it follows from the above comments (about [19], [20] and [10]) that  $n := |T|$  is a positive integer (and, of course,  $n > N$ ). Again bearing in mind that any "subclass" of a set is a set, it follows from (b) that for any integer  $n > N$ , the collection of ring isomorphism classes represented by a minimal ring extension  $T$  of some ring of cardinality  $N$  such that  $|T| = n$  is at most  $n^{(2n^2)}$ . Thus, since the disjoint union of a denumerable collection of sets is a set, we get that the cardinal number of the collection of ring isomorphism classes represented by a minimal ring extension of some ring of cardinality  $N$  is at most

$$\sum_{n > N} n^{(2n^2)} \leq \sum_{n > N} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0.$$

The assertion now follows, since the only cardinal numbers that are majorized by  $\aleph_0$  are the finite cardinal numbers and  $\aleph_0$  itself.

(d), (e): Note that (d) is the special case of (e) where  $\kappa = \aleph_0$ . So, it will suffice to prove the parenthetical assertion in (d) and the assertion in (e).

Let  $k = F(X)$  where  $F$  is a finite field and  $X$  is transcendental over  $F$ . For each nonnegative integer  $n$ , the set of  $h \in F[X]$  such that  $\deg(h) = n$  is in one-to-one correspondence with the Cartesian product

of  $n + 1$  copies of  $k$  (by identifying each such  $h$  with its list of coefficients). Thus, for each nonnegative integer  $n$ , the cardinal number of the set of  $h \in F[X]$  such that  $\deg(h) = n$  is  $|k|^{n+1} = \aleph_0^{n+1} = \aleph_0$ . Hence,  $F[X] \setminus \{0\}$  is a denumerable union of denumerable sets, and so  $|F[X] \setminus \{0\}| = \aleph_0$ . Therefore,

$$|F[X]| = |(F[X] \setminus \{0\}) \cup \{0\}| = |F[X] \setminus \{0\}| + |\{0\}| = \aleph_0 + 1 = \aleph_0.$$

Then  $|k| = \aleph_0$  since  $\aleph_0 \leq |k| \leq |F[X] \times F[X]| = |F[X]|^2 = \aleph_0^2 = \aleph_0$ .

Finally, we next prove (e). Let  $T$  be a minimal ring extension of  $R$ . Since  $\kappa := |R|$  is infinite by hypothesis, we have that  $\sigma := \max(\kappa, \aleph_0) = \kappa$ . Hence, by (a),  $|T| \leq \kappa$ . It follows from (b) that as  $\tau$  runs over the set of cardinal numbers that are less than or equal to  $\kappa$ , the cardinal number of the collection of ring isomorphism classes represented by a minimal ring extension of  $R$  is at most

$$\sum_{\tau \leq \kappa} \tau^{(2\tau^2)}.$$

What we are really interested in here is ostensibly a “larger” sum than the just-displayed sum. Indeed, we need to consider (not just the *ring isomorphism* classes represented by minimal ring extensions of  $R$ , but) the  $R$ -isomorphism classes represented by minimal ring extensions of  $R$ . In this paragraph, we will show that if  $T$  is a minimal ring extension of  $R$ , then the cardinal number of the collection of  $R$ -isomorphism classes that have a representative which is ring isomorphic to  $T$  is at most  $\kappa$ . (Once this fact has been proven, we will get at once that the cardinal number that we are really interested in here is at most the product of  $\kappa$  and the last-displayed sum. As we *will* prove below that the value of that last-displayed sum is at most  $2^\kappa$ , it will follow that the cardinal number that we are really interested in here is at most  $\max(\kappa, 2^\kappa) = 2^\kappa$ , as desired.) Recall that  $|T| \leq \kappa$ . An  $R$ - $R$  bimodule structure that can be placed on the ring  $T$  is given by a particular kind of pair of functions,  $R \times T \rightarrow T$  (for the “left module” part of the bimodule structure) and  $T \times R \rightarrow T$  (for the “right module” part of the bimodule structure). The cardinal number of the set of such ordered pairs of functions which actually produce bimodule structures is at most

$$(|T|^{|R \times T|})(|T|^{|T \times R|}) \leq (\kappa^{|R| \cdot |T|})(\kappa^{|T| \cdot |R|}) = (\kappa^{\kappa \cdot \kappa})(\kappa^{\kappa \cdot \kappa}) = \kappa^{2\kappa^2} = 2^\kappa,$$

where the last step followed from the final assertion of (b). Therefore, as explained earlier in *this* paragraph, it now suffices to show that the sum which was displayed at the end of the *last* paragraph is at most  $2^\kappa$ .

In the sum that was displayed at the end of the paragraph just before the last paragraph, the summands corresponding to finite values of  $\tau$  sum to  $\aleph_0$  (since that “partial” sum is at least  $\sum_{n=1}^\infty 1 = \aleph_0$  and is at most  $\sum_{n=1}^\infty \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$ ). So, it will suffice to prove that the “partial” sum of the summands corresponding to the infinite values of  $\tau$  (that are less than or equal to  $\kappa$ ) is at most  $2^\kappa$ . We claim that the index set of this “partial” sum has cardinality at most  $\kappa$ . Granting this claim for the moment (we *will* prove this claim in the next paragraph), we get from the final assertion in (b) that this “partial” sum is at most

$$\sum_{\tau} 2^\tau \leq \sum_{\tau} 2^\kappa = \kappa \cdot 2^\kappa = \max(\kappa, 2^\kappa) = 2^\kappa,$$

as desired.

It remains only to prove the above claim that the set of infinite cardinal numbers which are less than or equal to  $\kappa$  has cardinality at most  $\kappa$ . Recall that since  $\kappa$  is a cardinal number, it is the set of all ordinal numbers less than  $\kappa$  (where the last use of “less than” was in the sense of ordinal numbers). Thus, since  $\kappa + 1 = \kappa$  (where this sum is in the sense of cardinal numbers), it will suffice to prove that the set of all ordinal numbers that are less than  $\kappa$  (where this “less than” is in the sense of ordinal numbers) has cardinal number  $\kappa$ . This, in turn, follows from the well known fact that the cardinal number of  $\kappa$  (when  $\kappa$  is viewed as a set of ordinal numbers) is  $\kappa$ . The proof is complete.  $\square$



Many of the results from [13] that we will apply here use the notion of a “prime ring.” According to one standard definition, a ring  $R$  is said to be a *prime ring* if  $aRb \neq 0$  whenever  $a$  and  $b$  are nonzero elements of  $R$ . It is easy to see that a ring  $R$  is a prime ring if and only if  $IJ \neq 0$  whenever  $I$  and  $J$  are nonzero ideals of  $R$ . (Here is a hint for a proof of the “if” assertion: if  $a$  and  $b$  are nonzero elements of  $R$  such that  $aRb = 0$ , consider the ideals  $I = RaR$  and  $J = RbR$ , bearing in mind that  $R$  being unital ensures that  $R^2 = R$  and  $a \in I$ .) Since any ring is an ideal of itself, it now follows easily (and it is well known) that each simple ring is a prime ring. (The converse is false, even in the commutative case: consider  $\mathbb{Z}$ .) Since any field is a simple ring, this fact will next enable us to apply a result from [13] to get a classification of the (not necessarily commutative) minimal ring extensions of a field that has some of the flavor of the classification for the commutative case that was given in [14, Lemme 1.2] by Ferrand and Olivier.

In what is perhaps their deepest result [13, Theorem 5.1], Dorsey and Mesyan classified the minimal ring extensions of any given prime ring  $R$ , up to  $R$ -isomorphism, into five mutually exclusive types of extensions. In Proposition 2.2, we will state their application of that result to the case where the base ring  $R$  is a simple ring. That application will be strong enough to help with our concerns here, since any field is a prime ring; and the result stated in Proposition 2.2 is “simpler” (pun intended) than the more general result in [13, Theorem 5.1] because, for a base ring  $R$  that is a simple ring, one needs only four of the above-mentioned mutually exclusive types of extensions in order to describe the desired classification. Nevertheless, the statement of Proposition 2.2 unavoidably involves some specialized notation and terminology from [13]. So, to make that statement self-contained, we devote the next paragraph to that background material.

The next four sentences result from lightly editing a passage from [7]. Let  $R$  be a ring and let  $I$  be an  $R$ -rng. As in [13, page 3466], the *Dorroh extension*  $E(R, I)$  of  $R$  is defined as follows. 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 ring homomorphism  $R \rightarrow E(R, I)$  given by  $r \mapsto (r, 0)$ . For the special case where the  $R$ -rng  $I$  is just an  $R$ - $R$  bimodule with the zero multiplication (that is, an  $R$ -rng  $I$  such that  $I^2 = 0$ ), one denotes  $E(R, I)$  by  $R \rtimes I$ , which is called an *idealization*; one views  $R$  as a subring of  $R \rtimes I$  precisely as above (for more general Dorroh extensions). Lastly, if  $R \subseteq S$  are rings,  $S$  is said to be a *central extension of  $R$*  if  $S$  can be generated as a left  $R$ -module by the centralizer of  $R$  in  $S$ . Readers are advised that a different notion of a “central extension” is widespread and time-honored in the literature, but we will adhere here to the definition that was just given because it was used in [13].

**Proposition 2.2.** (Dorsey and Mesyan, [13, Theorems 6.1 and 5.1]) *Let  $R$  be a simple ring. Then, up to  $R$ -isomorphism, the minimal ring extensions  $S$  of  $R$  can be classified via the following four mutually exclusive types of extensions:*

- (P)  $S$  is a simple ring which is a minimal ring extension of  $R$ ;
- (PI)  $S$  is the Dorroh extension  $E(R, I)$  for some minimal  $R$ -rng  $I$  such that  $I^2 \neq 0$  and  $I$  is not  $R$ -isomorphic to  $R$ ;
- (SI)  $S = R \times R$ ;
- (N)  $S$  is the idealization  $R \rtimes M$  for some simple  $R$ - $R$  bimodule  $M$ .

*If a ring  $S$ , up to  $R$ -isomorphism, satisfies (P) or (PI) (resp., satisfies (SI); resp., satisfies (N)), then  $S$  is a prime ring (resp., is a semiprime ring but is not a prime ring; resp., is not a semiprime ring and, hence, is not a prime ring).*

*For a given type-(PI) extension,  $I$  is unique up to  $R$ -isomorphism. For a given type-(N) extension,  $M$  is unique up to  $R$ - $R$  bimodule isomorphism. Also, for a given type-(N) extension,  $M$  is isomorphic to  $R$  as an  $R$ - $R$  bimodule if and only if  $S$  is a central extension of  $R$ .*

Before moving toward the results announced in the Abstract or the Introduction, we pause to collect some comments about some connections between Proposition 2.2 and the literature (including

this paper).

**Remark 2.3.** (a) The uniqueness assertions in Proposition 2.2 concerning  $I$  (for a type-(PI) extension) and  $M$  (for a type-(N) extension) were taken from [13, Theorem 5.1]. The rest of the statement of Proposition 2.2 was taken from [13, Theorem 6.1].

(b) For commutative extension rings  $S$  and (then necessarily commutative simple base rings, that is) base fields  $R$ , it is natural to ask how the four types of  $R$ -isomorphism classes in Proposition 2.2 align with the three types of  $R$ -algebra isomorphism classes in the classification result of Ferrand and Olivier [14, Lemme 1.2]. For traditional reasons, let us put  $k := R$  here. It is clear that up to  $k$ -ring-isomorphism, that is up to  $k$ -algebra isomorphism, we have the following: (the commutative extension ring)  $S$  satisfies (P) if and only if  $S$  is a minimal field extension of  $k$ ; and  $S$  satisfies (N) if and only if  $S = k \rtimes k$ . Since  $k \rtimes k$  is  $k$ -algebra isomorphic to  $k[X]/(X^2)$ , with  $X$  any transcendental over  $k$  (and the condition (SI) "aligns" with itself), we see that three of the four types of  $R$ -isomorphism classes in Proposition 2.2 match up perfectly with the types of  $R$ -algebra isomorphism classes in [13, Theorem 6.1]. This circumstance raises (at least) the following two questions. Why is there no instance/example satisfying the condition (PI) with  $S$  commutative and  $k = R$  a field? Why has the author formulated the statement of Proposition 2.2 so as to mention the condition (PI) when his focus in this paper is mainly on base fields? I will answer these questions in the next paragraph.

The first of the above questions can be answered as follows: it was observed by Dorsey and Mesyan in [13, Remark 6.3] that each type-(PI) (minimal ring) extension of a simple ring must be non-Artinian, but note that each of the three (commutative) possibilities in the classification result of Ferrand-Olivier [14, Lemme 1.2] is a (left- and right-) Artinian ring. The second of the above questions can be answered by pointing to an example of G. Bergman [13, Example 6.4] of a simple ring (but notably *not* a field)  $R$  and a minimal ring extension  $R \subset S$  such that  $S$  is a non-simple prime ring. (By Proposition 2.2, that extension is necessarily of type-(PI).) Of course, that example leads naturally to another question, and Bergman answered *it*, too, by giving an example, in [13, Example 6.11], of a *field*  $k$  and a non-simple prime ring  $S$  such that  $k \subset S$  is a minimal ring extension (necessarily of type-(PI)). As explained in the first sentence of this paragraph, the ring  $S$  in *any* such example must be noncommutative.

(c) The description of the condition (SI) leads naturally to the question of which rings  $R$  have the property that  $R \hookrightarrow R \times R$  is a minimal ring extension. We showed in [4, Proposition 2.3] that fields are the only such nonzero commutative rings. Nevertheless, direct products have played significant roles in the recent history of minimal ring extensions involving commutative rings. For instance, it was shown by Shapiro and the author in the final three sentences prior to the statement of [12, Theorem 2.4] that if  $R$  is a nonzero commutative ring and  $\mathcal{M}$  is a maximal ideal of  $R$ , then  $R \hookrightarrow R \times R/\mathcal{M}$  is a decomposed (necessarily integral) minimal ring extension. By way of a partial converse, it was also shown in [12, Corollary 2.5] that if  $R \subset S$  is a decomposed (necessarily integral) minimal ring extension (with  $S$  necessarily commutative) such that the total quotient ring of  $R$  is a von Neumann regular ring and no maximal ideal of  $R$  is a minimal prime ideal of  $R$ , then there exists a maximal ideal  $\mathcal{M}$  of  $R$  such that  $S$  is  $R$ -algebra isomorphic to  $R \times R/\mathcal{M}$ .

As our interest here is in *noncommutative* minimal ring extensions, we will not mention condition (SI) again in this paper. Also, we will mention (PI) seldom again in this paper because the construction of additional examples of this condition will require deeper analysis of  $R$ -rings than what is included below. Thus, in view of Proposition 2.2, the reader will see that our focus here will be on examples satisfying either (P) or (N). That emphasis will begin explicitly in the statement of Corollary 2.4 and will culminate with examples in Theorem 2.10 (resp., Theorem 2.12) of an infinite field  $k$  having infinitely many  $k$ -isomorphism classes which are represented by noncommutative minimal ring extensions of  $k$  that satisfy condition (P) (resp., that satisfy condition (N)).

(d) Idealizations have played arguably more important roles than direct products in the recent history of minimal ring extensions involving commutative rings. For instance, we showed in [4,

Corollary 2.5] that if  $\mathcal{M}$  is a maximal ideal of a (nonzero) commutative ring  $R$ , then  $R \hookrightarrow R \rtimes R/\mathcal{M}$  is a minimal ring extension; it was noted, in the final sentence prior to the statement of [12, Theorem 2.4], that any such  $R \hookrightarrow R \rtimes R/\mathcal{M}$  is a ramified (integral) minimal ring extension. Also, by way of a partial converse, it was shown in [12, Corollary 2.5] that if  $R \subset S$  is a ramified (necessarily integral) minimal ring extension (with  $S$  necessarily commutative) such that the total quotient ring of  $R$  is a von Neumann regular ring and no maximal ideal of  $R$  is a minimal prime ideal of  $R$ , then there exists a maximal ideal  $\mathcal{M}$  of  $R$  such that  $S$  is  $R$ -algebra isomorphic to  $R \rtimes R/\mathcal{M}$ . Thus, commutative minimal ring extensions of type-(N) have considerable significance. In Theorems 2.8 (b) and 2.12, we will give some concrete examples of noncommutative minimal ring extensions of type-(N) having base rings that are fields.

(e) In dealing with idealizations as a special kind of Dorroh extensions in [13], Dorsey and Mesyan paid particular interest to the case where the base ring  $R$  is nonzero and the  $R$ -rng  $I$  is taken as the  $R$ - $R$  bimodule  $R/\mathcal{M}$  with trivial (that is, identically zero) multiplication, where  $\mathcal{M}$  is a maximal ideal of  $R$ . It was shown in [13, Lemma 2.4 and Remark 2.5] that, under these conditions,  $R \subset E(R, R/\mathcal{M})$  is a minimal ring extension. As indicated in [13, page 3467], the proofs of [13, Lemma 2.4 and Remark 2.5] were inspired by the proofs of [4, Theorem 2.4 and Remark 2.9] that were given for the case where  $R$  is a commutative ring and the role of  $E(R, R/\mathcal{M}) = R \rtimes R/\mathcal{M}$  had been played by that same idealization (which was denoted by  $R(+)\mathcal{M}$  in [4]).

(f) The final sentence in (d) promised some upcoming constructions that will enrich our collection of concrete examples of noncommutative minimal ring extensions of certain fields. In those constructions which produce examples of type-(N) (minimal ring) extensions, it will be important to use certain non-identity injective self-maps of the base field. It is instructive to observe that the construction underlying the proof of the main result in [8] was of that type. In constructing the ring extension  $k \subset S$  in that result, we took  $S$  to be the skew polynomial ring over any field  $k$  of characteristic  $p > 0$  that is not isomorphic to  $\mathbb{F}_p$ , with the "variable"  $x$ , where the multiplication in the skew polynomial ring was "twisted" so as to satisfy  $xa = a^p x$  for each  $a \in k$ . (Notice the role of the Frobenius map  $k \rightarrow k$ , given by  $a \mapsto a^p$ , in this "twisted" noncommutative multiplication.) This skew polynomial ring is nothing more than the idealization  $k \rtimes kx$ , that is,  $k \rtimes I$  where  $I := kx$  has been given a certain  $k$ - $k$  bimodule structure. I believe that there is pedagogic value in noting that skew polynomial rings, which have been extensively studied for their own sake for many years, are generalized by idealization constructions of type-(N). The remark is complete.

The next two corollaries will help to direct the program of this paper. In their statements and proofs – and later in the paper – we will feel free to use the notations (P), (PI), (SI) and (N) from Proposition 2.2 without further explanation.

**Corollary 2.4.** *Let  $k$  be a field and let  $S$  be a noncommutative minimal ring extension of  $k$ . Then, up to  $k$ -isomorphism,  $S$  satisfies either (P), (PI) or (N). Therefore, either  $S$  is a prime ring or  $S$  is a non-semiprime ring.*

*Proof.* As  $S$  is noncommutative, Proposition 2.2 ensures that the three asserted options are the only allowed possibilities for  $S$  (up to  $k$ -isomorphism). If  $S$  satisfies (P) or (PI), then  $S$  is a prime ring. If  $S$  satisfies (N), then  $S$  is not semiprime. The proof is complete.  $\square$

**Corollary 2.5.** *Let  $k$  be a finite field and let  $S$  be a noncommutative minimal ring extension of  $k$ . Then, up to  $k$ -isomorphism,  $S$  satisfies either (P) or (N). If  $S$  satisfies (P), then there exist a finite field  $K$  and an integer  $n \geq 2$  such that  $S$  is ring-isomorphic to  $M_n(K)$ , whence  $S$  is a finite simple ring (and, in particular, a finite prime ring). If  $S$  satisfies (N), then  $S$  is a finite non-semiprime ring.*

*Proof.* By [10, Lemma 2.1 (c)],  $S$  is a finite ring and, hence, a left- and a right-Artinian ring. To prove the first assertion, Corollary 2.4 reduces our task to showing that (up to  $k$ -isomorphism)  $S$  cannot

satisfy (PI). This, in turn, follows from the above-mentioned observation by Dorsey and Mesyan in [13, Remark 3.6] that each type-(PI) (minimal ring) extension of a simple ring must be non-Artinian.

It remains to prove the second assertion. Recall that  $S$  is a finite ring. So, by Corollary 2.4 (and the fact that each simple ring is a prime ring), it remains only to prove that if  $S$  satisfies (P), then  $S \cong M_n(K)$  for some finite field  $K$  and some integer  $n \geq 2$ . Recall that  $S$  is a left- (and a right-) Artinian ring. Since  $S$  is also a simple ring, it follows from Artin-Wedderburn theory that  $S \cong M_n(\Delta)$  for some division ring  $\Delta$  and some integer  $n \geq 2$  (cf. [16, Theorem 1.14, pages 421-422]). Then

$$|\Delta| < |\Delta|^{(n^2)} = |M_n(\Delta)| = |S| < \infty,$$

whence  $\Delta$  is a finite division ring. Therefore, by a celebrated theorem of Wedderburn (cf. [16, Proposition 1.17, page 423]),  $\Delta$  is a field. Putting  $K := \Delta$  completes the proof.  $\square$

There are many known proofs of the above-mentioned "celebrated theorem of Wedderburn." The above-cited proof of that result used a well known lemma in group theory [16, Lemma 6.10, page 462]. Many years ago, I informed T. W. Hungerford that there is a typo in the published proof of that lemma in his book (specifically, on the second line of that proof, " $H < N$ " should be " $H \leq N$ "). Hungerford acknowledged receipt of my message and he agreed to correct that typo in a subsequent printing or edition of his book, but I have not checked whether that correction was ever made.

The statement of Corollary 2.5 is striking in at least the following sense: in case  $S$  satisfies (P) (up to  $k$ -isomorphism), the isomorphism between  $S$  and  $M_n(K)$  was described as a ring isomorphism, rather than as a  $k$ -isomorphism. We chose the weaker formulation of the assertion for the following three reasons: the appeal to Artin-Wedderburn theory in the proof of Corollary 2.5 yielded a ring isomorphism; it is not at all clear from the statement of the above-cited version of Artin-Wedderburn theory whether/why the matrix ring  $M_n(K)$  is a  $k$ -ring; and it would seem that on the basis of general principles, it may not be clear whether a given ring isomorphism from one  $k$ -ring to another  $k$ -ring is necessarily a  $k$ -isomorphism.

**Proposition 2.6.** (Bergman-Dorsey-Mesyan, cf. [13, Lemma 6.6 and Remark 6.7]) *Let  $F \subset k$  be a minimal field extension. (So, this field extension is proper and finite-dimensional.) Define  $n := [k : F]$ . (Necessarily,  $2 \leq n < \infty$ ). Then there exists a noncommutative minimal ring extension  $S$  of  $k$  such that  $S$  is ring isomorphic to  $M_n(F)$ . In particular,  $S$  is a simple (and left- and right-Artinian) ring, and hence a prime ring.*

*Proof.* If  $f : A \rightarrow B$  is a ring homomorphism, then one has the following conclusions:  $B$  is a left  $A$ -module via  $a \cdot b := f(a)b$  for all  $a \in A$  and all  $b \in B$ ;  $B$  is a right  $A$ -module via  $b \cdot a := bf(a)$  for all  $a \in A$  and all  $b \in B$ ;  $B$  is thereby an  $A$ - $A$  bimodule; and  $f$  is then an  $A$ - $A$  bimodule homomorphism. Let us apply these generalities to the following situation. Consider the ring  $R := \text{End}_F(k)$  of  $F$ -linear endomorphisms of  $k$ , along with the "left regular representation"  $L : k \rightarrow R$  which sends each  $a \in k$  to  $L_a$ , the left multiplication (of elements of  $k$ ) by  $a$ . (In detail, if  $b \in k$ , then  $L_a(b) := ab$ .) Notice that  $L$  is a ring homomorphism (since it is easy to check that if  $a_1, a_2 \in k$ , then  $L_{a_1+a_2} = L_{a_1} + L_{a_2}$  and  $L_{a_1 a_2} = L_{a_1} L_{a_2}$ , and that  $L_1$  is the identity endomorphism of  $k$ ). By a comment in the Introduction,  $L$  being a ring homomorphism allows us to view  $R$  as a  $k$ -ring. We also have, of course, that  $L$  is an injection. (This can be seen in several ways; for instance, observe that  $R \neq 0$ .) Viewing  $L$  as an inclusion map, we can view  $k$  as subring of  $R$ . Moreover, the generalities at the beginning of this paragraph show that  $R$  is a  $k$ - $k$  bimodule and that  $L$  is a  $k$ - $k$  bimodule homomorphism. Hence, by a comment in the Introduction,  $L$  is a  $k$ -ring-homomorphism. It was observed in [13] that  $k \subset R$  is a minimal ring extension and that  $R$  is ring isomorphic to  $M_n(F)$ . The proof is complete.  $\square$

Before beginning to build examples with the desired isomorphism classes having representatives that are prime rings, we next give the result that will lead to companion results that will be used

to construct examples with the desired isomorphism classes having representatives that are non-semiprime rings (that is, being represented by minimal ring extensions of  $k$  that are type-(N) extensions).

**Proposition 2.7.** *Let  $k$  be a field. Let  $x$  be a “variable” not in  $k$ . For each (necessarily injective) ring homomorphism  $\sigma : k \rightarrow k$ , let  $S_\sigma$  denote the associated skew polynomial ring, which is a ring with underlying additive structure the two-dimensional vector space over  $k$  with basis  $\{1, x\}$  and with “twisted” multiplication satisfying  $xa = \sigma(a)x$  for all  $a \in k$ . For each such  $\sigma$ , view  $k \subset S_\sigma$  via the injective ring homomorphism  $k \rightarrow S_\sigma$  given by  $a \mapsto a \cdot 1 + 0 \cdot x$  for all  $a \in k$ . Then:*

- (a) *For each injective ring homomorphism  $\sigma : k \rightarrow k$ ,  $S_\sigma$  is a  $k$ -ring.*
- (b) *For each injective ring homomorphism  $\sigma : k \rightarrow k$ , the ring extension  $k \subset S_\sigma$  is a minimal ring extension of type-(N).*
- (c) *If a ring homomorphism  $\sigma : k \rightarrow k$  is not the identity map, then  $S_\sigma$  is a noncommutative ring.*
- (d) *If  $\sigma$  and  $\tau$  are distinct ring homomorphisms from  $k$  to  $k$ , then  $S_\sigma$  and  $S_\tau$  are not isomorphic as  $k$ -rings.*
- (e) *If  $G$  is the set of injective ring homomorphisms from  $k$  to  $k$ , then the cardinal number of the collection of  $k$ -ring-isomorphism classes represented by noncommutative minimal ring extensions of  $k$  of type-(N) is at least  $|G| - 1$  (where, by convention,  $\kappa - 1 := \kappa$  for any infinite cardinal number  $\kappa$ ).*

*Proof.* Let us first explicate in greater detail, for any given ring homomorphism  $\sigma : k \rightarrow k$ , the multiplication and ring-theoretic structure of  $S_\sigma$ . Most of the rest of this paragraph is the result of lightly editing a passage from [8]. We can induce a multiplication on  $S_\sigma$  by requiring that  $xa = \sigma(a)x$  for all  $a \in k$  and  $x^2 = 0$ . More precisely, define the binary operation of multiplication on  $S_\sigma$  as follows: if  $\{\alpha, \beta, \gamma, \delta\} \subseteq K$ , then

$$(\alpha + \beta x)(\gamma + \delta x) := \alpha\gamma + (\alpha\delta + \beta\sigma(\gamma))x.$$

As  $\sigma$  preserves addition and multiplication in  $k$ , it is straightforward to verify that the above multiplication on  $S_\sigma$  is left- and right-distributive over addition; and that this multiplication is associative. As the multiplicative identity element of the ring (field)  $k$  also serves as a/the multiplicative identity element for  $S_\sigma$ , it follows that  $S_\sigma$  is a ring.

(a) The ring-theoretic structure of  $S_\sigma$  was addressed above. Since the inclusion map  $k \hookrightarrow S_\sigma$  is a ring homomorphism, it follows from a comment in the Introduction that  $S_\sigma$  thereby obtains the structure of a  $k$ -ring.

(b) We have already seen that  $k \subset S_\sigma$  is a ring extension. As  $\dim_k(S_\sigma) = 2$ , this extension must be a minimal ring extension (cf. also [7, Lemma 2.4 (a)]). It remains only to show that this extension is of type-(N), that is, that  $S_\sigma = k \ltimes M$  for some simple  $k$ - $k$  bimodule  $M$ . This, in turn, holds by taking  $M := kx$ , because of the following three facts: the nature of the addition and multiplication operations in  $S_\sigma$  ensures that  $S_\sigma = k \ltimes M$  (note, in particular, that if  $a, b \in k$ , then  $(ax)(bx) = a\sigma(b)x^2 = a\sigma(b) \cdot 0 = 0$ ); the additive group  $M$  is a  $k$ - $k$  bimodule, for if  $a, b \in k$ , then  $(ax)b = a(xb) (= a\sigma(b)x)$ ; and this bimodule is clearly simple since  $\dim_k(kx) = 1$ .

(c) We have already seen that  $S_\sigma$  is a ring. It remains to show that the multiplication in this ring is not commutative. By hypothesis, there exists  $a \in k$  such that  $\sigma(a) \neq a$ . For any  $b \in K$ , we have the following:  $\sigma(b) \neq b$  in  $k \Leftrightarrow \sigma(b)x \neq bx$  in  $kx \Leftrightarrow xb \neq bx$  in  $S_\sigma$ . Hence, the assumed behavior of the element  $a$  ensures the assertion.

(d) By hypothesis, there exists  $c \in k$  such that  $\sigma(c) \neq \tau(c)$ . Suppose that the assertion fails. Then there exists a  $k$ -isomorphism  $f : S_\sigma \rightarrow S_\tau$ . So, there exist unique  $a, b \in k$  such that  $f(x) = a + bx$ . For all  $d \in k$ ,

$$f(d) = f(d \cdot 1) = d \cdot f(1) = d \cdot 1 = d.$$

As  $a \neq x$  and  $f$  is injective, it follows that  $a = f(a) \neq f(x) = a + bx$ , and so  $bx \neq 0$ . Hence  $b \neq 0$ . Consider the following equations:

$$ac + b\tau(c)x = ac + bxc = (a + bx)c = f(x)f(c) = f(xc) = f(\sigma(c)x) =$$

$$f(\sigma(c))f(x) = \sigma(c)(a + bx) = \sigma(c)a + \sigma(c)bx.$$

Since  $kx$  is a free left  $k$ -module on the basis  $\{1, x\}$ , ( $ac = \sigma(c)a$  and)  $b\tau(c) = \sigma(c)b$  in  $k$ . As  $b \neq 0$  in  $k$  and  $k$  is a field, we can multiply both sides of this equation by  $b^{-1}$ , giving the result that  $\tau(c) = \sigma(c)$ , the desired contradiction.

(e) Let  $H$  be the subset of  $G$  consisting of the non-identity maps in  $G$ . Then, using the above-announced convention, we have  $|H| = |G| - 1$ . Consider the function that sends each  $\sigma \in H$  to the  $k$ -isomorphism class represented by  $S_\sigma$ . This function is well defined by (a) and it is an injection by (d). The image of this function is of the desired kind, by (b) and (c). The proof is complete.  $\square$

As promised, we now begin to carry out our program of constructing some concrete examples of noncommutative minimal ring extensions of a field  $k$ . We begin with the case of a finite field  $k$ . Theorem 2.8 is the first of our three main results. Of course, we make the assumption in Theorem 2.8 that  $k$  is not isomorphic to  $\mathbb{F}_p$  because  $\mathbb{F}_p$  has no noncommutative minimal ring extensions.

**Theorem 2.8.** Let  $k$  be a finite field of characteristic  $p$  ( $> 0$ ) such that  $k$  is not isomorphic to  $\mathbb{F}_p$ . Then  $|k| = p^n$  for some uniquely determined integer  $n \geq 2$ . Let the prime-power factorization of  $n$  be  $n = \prod_{j=1}^t q_j^{e_j}$ , where  $q_1, \dots, q_t$  are finitely many pairwise distinct prime numbers,  $t \geq 1$  and  $e_j \geq 1$  for each  $j$ . Then:

- (a) The cardinal number of the collection of  $k$ -ring-isomorphism classes that are represented by noncommutative simple rings (necessarily, each of type-(P)) is at least  $t$  ( $\geq 1$ ). Each ring  $S$  in one of those  $k$ -ring-isomorphism classes is ring isomorphic to a ring of the form  $M_m(K)$  for some integer  $m \geq 2$  and some finite field  $K$  (with both  $m$  and  $K$  possibly depending on  $S$ ).
- (b) The cardinal number of the collection of  $k$ -ring-isomorphism classes that are represented by noncommutative non-semiprime rings (necessarily, each of type-(N)) is at least  $n - 1$ .
- (c) The cardinal number of the collection of  $k$ -ring-isomorphism classes that are represented by noncommutative minimal ring extensions of  $k$  is at least  $n + t - 1$  ( $\geq n$ ).

*Proof.* (a) Let us work inside a fixed algebraic closure  $\bar{k}$  of  $k$  (equivalently, an algebraic closure of  $\mathbb{F}_p$  that contains  $k$ ). Recall that for each positive integer  $m$ , there exists a unique subfield of  $\bar{k}$  which is isomorphic to  $\mathbb{F}_{p^m}$  (that is, which has cardinality  $p^m$ ). For each positive integer  $m$ , it will be convenient to identify the subfield of  $\bar{k}$  having cardinality  $p^m$  with  $\mathbb{F}_{p^m}$ . In particular, we view  $k$  as  $\mathbb{F}_{p^n}$ . Fix any  $j \in \{1, \dots, t\}$ . Consider the integer  $n_j := n/q_j$ . Then  $F_j := \mathbb{F}_{p^{n_j}}$  is a subfield of  $k = \mathbb{F}_{p^n}$  (inside  $\bar{k}$ ). As  $[k : F_j] = n/n_j = q_j$  is a prime number,  $F_j \subset k$  must be a minimal field extension (cf. [16, Exercise 1 (b), page 240]). Therefore, by Proposition 2.6, there exists a noncommutative minimal ring extension, say  $S_j$ , of  $k$  such that  $S_j$  is ring isomorphic to the matrix ring  $M_{q_j}(F_j)$ . Note that  $S_j$  is a finite simple ring and that the minimal ring extension  $k \subset S_j$  is of type-(P). Now, letting  $j$  vary over  $\{1, \dots, t\}$ , note that one consequence of the uniqueness part of Artin-Wedderburn theory (as in [16, Proposition 1.17 (ii), page 423]) is that if  $j_1$  and  $j_2$  are distinct elements of  $\{1, \dots, t\}$ , then  $S_{j_1}$  is not ring isomorphic to  $S_{j_2}$  (since  $q_{j_1} \neq q_{j_2}$ ). Therefore, *a fortiori*,  $S_{j_1}$  and  $S_{j_2}$  are not  $k$ -ring-isomorphic. Consequently,  $\{S_j \mid 1 \leq j \leq t\}$  is a set of representatives of  $t$  pairwise distinct  $k$ -ring-isomorphism classes represented by noncommutative simple rings that are minimal ring extensions of  $k$ . Lastly, by Proposition 2.2, each such extension must be of type-(P).

(b) By Proposition 2.2, each minimal ring extension of  $k$  of type-(N) is a non-semiprime ring. Hence, by Proposition 2.7 (e), it suffices to find a set  $H$  of non-identity ring homomorphisms from  $k$  to  $k$  such that  $|H| \geq n - 1$ . It is well known that the Galois group, say  $\mathcal{G}$ , of  $k$  over  $\mathbb{F}_p$  is a finite (and cyclic) group of cardinality  $n$  (cf. [16, Proposition 5.10, page 281; and Theorem 2.5 (i), page 246]). Therefore, it suffices to take  $H$  to be the set  $\mathcal{G} \setminus \{1\}$ .

(c) By Proposition 2.2, no minimal ring extension of  $k$  of type-(P) can be  $k$ -isomorphic to a minimal ring extension of  $k$  of type-(N). So, the lower bound in question can be found by adding the lower bounds that were established in (a) and (b). The proof is complete.  $\square$

**Corollary 2.9.** *Let  $p$  be a prime number. Then there does not exist a finite upper bound on the cardinal number of the collection of  $k$ -ring-isomorphism classes represented by noncommutative minimal ring extensions of  $k$  having type-(P) (resp., having type-(N)) as  $k$  varies over finite fields of characteristic  $p$ . Hence, there does not exist a finite upper bound on the cardinal number of the collection of  $k$ -ring-isomorphism classes represented by noncommutative minimal ring extensions of  $k$  that are prime rings (resp., that are non-semiprime rings) as  $k$  varies over finite fields of characteristic  $p$ .*

*Proof.* We first address the “(P)” assertion. It suffices to show that, for each positive integer  $\nu$ , there exists a finite field  $k_\nu$  such that the cardinal number of the collection of  $k_\nu$ -ring-isomorphism classes represented by noncommutative minimal ring extensions of  $k_\nu$  having type-(P) is at least  $\nu$ . Let  $q_1, \dots, q_\nu$  be  $\nu$  pairwise distinct prime numbers. Put  $n := \prod_{j=1}^\nu q_j$ . By Theorem 2.8 (a),  $k_\nu := \mathbb{F}_{p^n}$  has the asserted property.

We turn now to the “(N)” assertion. It suffices to show that, for each positive integer  $\nu$ , there exists a finite field  $k_\nu^*$  such that the cardinal number of the collection of  $k_\nu^*$ -ring-isomorphism classes represented by noncommutative minimal ring extensions of  $k_\nu^*$  having type-(N) is at least  $\nu$ . By Theorem 2.8 (b),  $k_\nu^* := \mathbb{F}_{p^{\nu+1}}$  has the asserted property.

Lastly, the “Hence” assertion follows from Proposition 2.2. The proof is complete. □

Despite the information collected in the last two results, I have not been able to determine whether each finite field  $k$  of characteristic  $p$  which is not isomorphic to  $\mathbb{F}_p$  must have infinitely many pairwise distinct non- $k$ -isomorphic noncommutative minimal ring extensions. I would encourage interested readers to pursue this question. At this point in the present paper, I take leave of finite base fields, turning instead to some infinite base fields  $k$  which will be shown to have infinitely many  $k$ -isomorphism classes represented by noncommutative simple (resp., noncommutative non-semiprime) minimal ring extensions of  $k$ . For the first of these classes of  $k$ , we turn to one of the kinds of base rings that Bergman used for other (more specifically, type-(PI)) purposes in [13, Example 6.11].

We next present the second main result of this paper. It gives the first example of a family of fields  $k$  that each have infinitely many pairwise  $k$ -ring-isomorphism classes represented by noncommutative minimal ring extensions which are prime rings. In contrast to the conclusion from [13, Example 6.11], each of the noncommutative minimal ring extensions obtained in Theorem 2.10 is a simple ring (hence, a prime ring), hence of type-(P).

**Theorem 2.10.** *Let  $X$  be an indeterminate over a field  $k$ . Then the cardinal number of the collection of  $k(X)$ -ring-isomorphism classes that are represented by noncommutative simple rings (hence, prime rings) (which happen also to be both left- and right-Artinian rings, and are necessarily each of type-(P)) is at least  $\aleph_0$ .*

*Proof.* Let  $p_1 < p_2 < p_3 < \dots$  be the prime numbers, listed in increasing order. For the moment, fix an integer  $m \geq 1$ . Put  $Y_m := 1/X^{p_m}$ . Note that  $f_m := 1$  and  $g_m := X^{p_m}$  are relatively prime polynomials in the unique factorization domain  $k[X]$ . We have  $n_m := \max(\deg(f_m), \deg(g_m)) = \max(0, p_m) = p_m$ . Next, note that  $k(X)$  can be viewed as the field obtained by adjoining  $X$  to the field  $k(Y_m)$ . Moreover, one sees the following facts from the proof of [17, Theorem 7, page 158] (which leads to Jacobson’s approach to Lüroth’s Theorem):  $X$  is algebraic over  $k(Y_m)$ ; if  $t$  denotes an indeterminate over  $k(Y_m)$ , then the minimum polynomial of  $X$  over  $k(Y_m)$  is the monic associate of the polynomial

$$F(t) := f(t) - g(t)Y_m$$

in the unique factorization domain  $k(Y_m)[t]$ ; and  $[k(X) : k(Y_m)] = n_m$  (noting that the degree in  $t$  of  $F$  is  $n_m$  since  $Y_m \notin k$ ). Consequently,  $[k(X) : k(Y_m)] = p_m$ . As this is a prime number,  $k(Y_m) \subset k(X)$  is a minimal field extension (cf. [16, Exercise 1 (b), page 240]). Therefore, by Proposition 2.6, there exists

a (noncommutative) minimal ring extension  $k(X) \subset S_m$  such that  $S_m$  is ring isomorphic to  $M_{p_m}(k(Y_m))$ . Hence,  $S_m$  is (ring isomorphic to) a simple ring (which is also a left- and right-Artinian ring): cf. [16, Exercise 9 (a), page 133; Theorem 3.3, page 435; and Corollary 3.4, page 436]. Thus,  $S_m$  is a prime ring, and it also follows from the classification in Proposition 2.2 that the minimal ring extension  $k(X) \subset S_m$  must be of type-(P). Note also that the very existence of that ring extension ensures that  $S_m$  is a  $k$ -ring.

Now, allow  $m$  to vary over the set of positive integers. By a uniqueness result in Artin-Wedderburn theory (cf. [16, Proposition 1.17, page 423]),  $S_{m_1}$  and  $S_{m_2}$  are not ring-isomorphic if  $m_1$  and  $m_2$  are distinct positive integers (the point being that the prime numbers  $p_{m_1}$  and  $p_{m_2}$  are then distinct integers). Thus, *a fortiori*,  $S_{m_1}$  and  $S_{m_2}$  are not  $k$ -ring-isomorphic. The proof is complete.  $\square$

The direction toward our third main result will be informed by the following special, but very useful, case of Proposition 2.7 (e).

**Corollary 2.11.** *Let  $k$  be a field such that there exist infinitely many ring homomorphisms from  $k$  (in)to  $k$  (for instance, let  $k$  be a field whose group of automorphisms is infinite). Let  $\kappa$  be the cardinal number of the set of those (injective) homomorphisms. Then the cardinal number of the set of  $k$ -ring-isomorphism classes that can be represented by minimal ring extensions of  $k$  that are non-semiprime rings (that is, that are of type-(N)) is at least  $\kappa$ .*

We next give our third main result. Even though it is, in a sense, a corollary of a corollary, I believe that it deserves its designation as a "theorem" for the following three reasons: it provides many new examples of noncommutative minimal ring extensions; its proof is interesting inasmuch as it involves classical parts of several different mathematical genres; and its emphasis on automorphisms of certain structures related to the base ring may point the way to future innovations featuring rather general base rings. If the expectation that was just raised in the third reason is eventually realized, one may hope to discover new families of non-semiprime rings. In that regard, I am reminded of J. L. Kelley's wise observation, in his classical 1955 textbook, *General Topology*, to the effect that what may once have seemed like a mathematical "pathology" to one generation has often become understood by later generations as being a fundamental part of the reimagined foundation for their mathematical area. In that spirit, I would hope that at least some kinds of "non-semiprime rings" will become so widely appreciated that they will be given more positive names.

In the proof of Theorem 2.12, it will be convenient to use the following notation. If  $K$  is a field,  $\text{char}(K)$  denotes the characteristic of  $K$  and  $\bar{K}$  denotes an algebraic closure of  $K$ ; and if  $K \subseteq L$  is a field extension, then  $\text{t.d.}_K(L)$  denotes its transcendence degree and  $\text{Gal}(L/K)$  denotes its Galois group.

**Theorem 2.12.** Let  $k$  be a field that satisfies (exactly) one of the following two conditions:

- (i)  $k$  is a purely transcendental extension of some proper infinite subfield  $F$ , that is, there exists an infinite field  $F$  and a nonempty set  $\mathcal{S} := \{Y_\alpha \mid \alpha \in I\}$  of commuting algebraically independent indeterminates over  $F$  such that  $k = F(\mathcal{S})$ ;
- (ii)  $k$  is an algebraically closed field.

Then the cardinal number of the set of  $k$ -ring-isomorphism classes that can be represented by minimal ring extensions of  $k$  that are non-semiprime rings (that is, that are of type-(N)) is at least  $\aleph_0$ .

*Proof.* Both (i) and (ii) will be established as consequences of Corollary 2.11. In other words, it will suffice to show that  $k$  has infinitely many automorphisms.

(i) Pick  $\beta \in I$ . As  $Y := Y_\beta \in k$  is transcendental over  $F$ , it is well known that the Galois group, say  $G$ , of  $F(Y)$  over  $F$  is infinite. For the sake of completeness, we provide some supporting details. Up to group isomorphism,  $G$  is the projective group  $\text{PL}(2, F) := \text{GL}(2, F)/N_2$ , where  $N_2$  denotes the (normal subgroup) of all nonzero scalar  $2 \times 2$  matrices with entries in  $F$  (cf. [17, pages 158-159]). Note that if  $\xi$  and  $\eta$  are distinct nonzero elements of  $F$ , then the nonsingular matrix  $\begin{pmatrix} 0 & \xi \\ 1 & 0 \end{pmatrix}$  is not the product of



the nonsingular matrix  $\begin{pmatrix} 0 & \eta \\ 1 & 0 \end{pmatrix}$  with some matrix in  $N_2$ . As  $F$  is infinite, it follows that  $GL(2,F)/N_2$  is infinite, and so  $F(Y)$  has infinitely many  $F$ -algebra automorphisms.

By the universal mapping property of polynomials (in arbitrarily many commuting, algebraically independent indeterminates) over a commutative ring, each of the just-mentioned automorphisms extends to a ring automorphism of the (commutative) integral domain  $D := F[\mathcal{S}]$  (by sending each  $Y_\alpha \in \mathcal{S} \setminus \{Y\}$  to itself); notice that at this stage, we have infinitely many  $F$ -algebra automorphisms of  $D$ ; and then by the universal mapping property of rings of fractions (or, if you will, its special case, the universal mapping property of quotient fields), each of *those* automorphisms extends to a ring automorphism of the quotient field of  $D$ , that is, to a ring automorphism of  $F(\mathcal{S}) = k$ . We have obtained infinitely many  $F$ -algebra automorphisms of  $k$ .

(ii) Five cases will be considered. Besides what is specified below for the individual cases, it is also assumed in each of those cases that  $k$  is algebraically closed (that is,  $k = \bar{k}$ ) and that  $F$  denotes the prime subfield of  $k$  (so that, without loss of generality,  $F = \mathbb{F}_p$  if  $\text{char}(k) = p > 0$ , and  $F = \mathbb{Q}$  if  $\text{char}(k) = 0$ ).

Case 1:  $\text{t.d.}_F(k) \geq 2$ : Choose a transcendence basis  $\mathcal{S}$  for the field extension  $F \subset k$ , and then choose distinct elements, say  $X$  and  $Y$ , of  $\mathcal{S}$ . Since  $F(X)$  is an infinite field, it follows from the proof of (i) that there are infinitely many  $F(X)$ -algebra automorphisms of  $F(X)(Y) (= F(X, Y))$ . Each of these automorphisms can be extended to an automorphism of  $F(\mathcal{S})$  which is induced by sending each element of  $\mathcal{S} \setminus \{X, Y\}$  (if any such elements exist) to itself. (In greater detail: the extension process that was mentioned in the last sentence is, just as in the proof of (i), a two-step affair: first, each of the known  $F(X)$ -algebra automorphisms of  $F(X, Y)$  is extended to an automorphism of  $F[\mathcal{S}]$  by using a universal mapping property of polynomial rings, and then each of *those* automorphisms is extended to an automorphism of  $F(\mathcal{S})$  by using the universal mapping property of quotient fields.) Next, since  $k$  is an algebraically closed field that is an algebraic extension of  $F(\mathcal{S})$ , it follows that  $k$  is an algebraic closure of  $F(\mathcal{S})$ . Therefore, by the universal mapping theory of algebraic closures (cf. [16, Theorem 3.8, page 260; and Theorem 1.12, page 317]), each of the known (infinitely many) automorphisms of  $F(\mathcal{S})$  extends to an automorphism of  $k$ . We have now obtained infinitely many automorphisms of  $k$ .

Case 2:  $\text{char}(k) = p > 0$  and  $\text{t.d.}_F(k) = 1$ : Choose a transcendence basis  $\mathcal{S}$  for the field extension  $F \subset k$ . Let  $X$  denote the unique element of  $\mathcal{S}$ . Since  $F$  is a subfield of the algebraically closed field  $k$ , it follows that we can view  $\bar{F}$  as a subfield of  $k$ . As  $X$  is transcendental over  $F$ ,  $X$  is not algebraic over  $F$ , and so  $X \notin \bar{F}$ . So, since  $\bar{F}$  is algebraically closed in  $k$ , we get that  $X$  is not algebraic over  $\bar{F}$ . Hence,  $\text{t.d.}_{\bar{F}}(\bar{F}(X)) = 1$ . Thus, by the additivity of transcendence degree in towers for fields (cf. [16, Theorem 1.11, page 316]),

$$0 + 1 + \text{t.d.}_{\bar{F}(X)}(k) = \text{t.d.}_F(\bar{F}) + \text{t.d.}_{\bar{F}}(\bar{F}(X)) + \text{t.d.}_{\bar{F}(X)}(k) =$$

$\text{t.d.}_F(k) = 1$ . Hence  $\text{t.d.}_{\bar{F}(X)}(k) = 0$ ; that is,  $k$  is an algebraic extension of  $\bar{F}(X)$ . Therefore, since  $k$  is algebraically closed, we get that  $\overline{\bar{F}(X)} = k$ ; that is,  $k$  is an algebraic closure of  $\bar{F}(X)$ . Hence, to get infinitely many automorphisms of  $k$ , it follows from the universal mapping property of algebraic closures that it suffices to have infinitely many automorphisms of  $\bar{F}(X)$ . *Those* desired maps are, in turn, available thanks to (i), because  $\bar{F}$  is an infinite field (the point being that no finite field can be algebraically closed).

Case 3:  $\text{char}(k) = p > 0$  and  $k$  is algebraic over  $F$  (that is,  $\text{char}(k) = p > 0$  and  $k = \bar{F} = \overline{\mathbb{F}_p}$ ): It follows from standard field theory that, for *any* finite field  $\mathbb{F}_{p^m}$  of characteristic  $p$ ,

$$\text{Gal}(\overline{\mathbb{F}_{p^m}}/\mathbb{F}_{p^m}) \cong \varprojlim_n \text{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^m}) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

It is well known that the just-displayed profinite group  $\widehat{\mathbb{Z}}$  is infinite.

In view of the above treatments of Cases 1-3, the assertion in (ii) has now been proved if  $\text{char}(k) > 0$ .

Case 4:  $\text{char}(k) = 0$  and  $\text{t.d.}_F(k) = 1$ : Choose a transcendence basis  $\mathcal{S}$  for the field extension  $F \subset k$ . Let  $Y$  denote the unique element of  $\mathcal{S}$ . Then the proof of Case 4 can be completed by tweaking the above proof for Case 1 as follows: for the proof of Case 4, let (the infinite field)  $\mathbb{Q}$  play the role which had been played by  $F(X)$  in the proof for Case 1. In greater detail: once we obtain infinitely many automorphisms of  $\mathbb{Q}(Y)$  by using the fact that  $\text{PL}(2, \mathbb{Q})$  is an infinite group, each of those automorphisms can be extended to an automorphism of  $k$  by using the universal mapping property of algebraic closures.

Case 5:  $\text{char}(k) = 0$  and  $k$  is algebraic over  $F$  (that is,  $\text{char}(k) = 0$  and  $k = \bar{F} = \bar{\mathbb{Q}}$ ): There seems to be some controversy in the recent literature as to whether the elements of the group  $G := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  can be “explicitly described”, but it is certain that  $G$  is an infinite group and that, in fact,  $|G| > \aleph_0$ .

In view of the above treatments for Cases 1, 4 and 5, the assertion in (ii) has now been proved if  $\text{char}(k) = 0$ . The proof is complete. □

Happily, we can now present a family of fields  $L$  having infinitely many  $L$ -ring-isomorphism classes of both kinds that we have focused on here (that is, the kind with representatives that are simple (hence prime) rings and the kind with representatives that are non-semiprime rings).

**Corollary 2.13.** *Let  $X$  be an indeterminate over an infinite field  $k$ . Then the collection of  $k(X)$ -ring-isomorphism classes that are represented by noncommutative simple rings (which happen also to be both left- and right-Artinian rings, and are necessarily each of type-(P)) is infinite, and the collection of  $k(X)$ -ring-isomorphism classes that are represented by noncommutative non-semiprime rings (necessarily each of type-(N)) is also infinite.*

*Proof.* Apply Theorem 2.10 for the “type-(P)” assertion, and apply case (i) of Theorem 2.12 for the “type-(N)” assertion. □

We close our contributions to the study of minimal ring extensions with the following comments.

**Remark 2.14.** (a) The proof of Theorem 2.12 (i) has left open the following question. If a field  $k = F(X)$ , where  $F$  is a finite field and  $X$  is transcendental over  $F$ , must the set of automorphisms of  $k$  be infinite? We show next that, in contrast to the situation where the field of coefficients is infinite, the answer to this question is “No” when  $F \cong \mathbb{F}_p$  (for any prime number  $p$ ). For *this* situation, since every ring (field) automorphism of  $k$  fixes  $F$  elementwise, the number of automorphisms of  $k$  is

$$|\text{Gal}(k/F)| = |\text{PL}(2, F)| = |\text{GL}(2, F)/N_2| = \frac{|\text{GL}(2, F)|}{|N_2|} = \frac{(p^2 - 1)(p^2 - p)}{p - 1} = p(p^2 - 1) < \infty.$$

In view of the preceding paragraph, we see that the proof of Corollary 2.13 has left open the following question. If  $X$  is an indeterminate over a finite field  $k$ , is the collection of  $k(X)$ -ring-isomorphism classes that are represented by noncommutative non-semiprime rings (necessarily each of type-(N)) an infinite set? By Proposition 2.2 (and the preceding paragraph), an answer to this question will depend on investigating the simple  $k(X)$ - $k(X)$  bimodules which are not isomorphic to  $k(X)$  (as  $k(X)$ - $k(X)$  bimodules). I will make some related comments toward the end of the second paragraph of (b).

(b) We have not settled the questions whether some finite field (most finite fields)  $k$  has (have) infinitely many  $k$ -isomorphism classes represented by noncommutative minimal ring extensions of  $k$ . However, we have shown in Corollary 2.13 that for certain infinite fields  $k$  (namely, fields generated by a transcendental element over some infinite subfield), the “prime ring” (resp., the “not semiprime ring”) option can apply to (representatives of) infinitely many such  $k$ -isomorphism classes. Given

that some (admittedly limited) progress has been made here toward achieving our (admittedly limited) goals for this paper, one may ask whether we have been overly cautious by restricting attention here to base rings that are fields. The next two paragraphs respond, in some sense, to that query.

Given the record of studies of minimal ring extensions all of whose rings are commutative, it may seem reasonable to suggest generalizing the above work by examining the noncommutative minimal ring extensions of a quasi-local commutative base ring that is not a field. After all, that broader context was shown to be rather tractable, at least for finite commutative (quasi-)local base rings, in [7]. However, we would like to point out that what may seem like a small change to the setting of [14, Lemme 1.2] can lead to a strikingly different conclusion. Indeed, consider the following result. If  $R$  is a finite commutative local ring, then the class of commutative  $R$ -algebras represented by commutative minimal ring extensions of  $R$  is infinite (if and) only if  $R$  is a field [5, Corollary 2.6]. Moreover, for any such  $R$ , the ramified (resp., decomposed) analogues of  $k[X]/(X^2)$  (resp., of  $k \times k$ ) account for only finitely many such  $R$ -algebra isomorphism classes [5, Proposition 2.2]; and it follows that the collection of  $R$ -algebra isomorphism classes in question is infinite if and only if the inert analogues of the minimal field extensions of  $k$  represent infinitely many of those  $R$ -algebra isomorphism classes. This would seem to suggest that any attempt to improve Theorem 2.8 (c) should focus initially on finding more  $k$ -isomorphism classes with representatives which are prime (perhaps, even simple) rings. Workers choosing this “prime” path of inquiry, especially beyond the context of finite base rings, should note the detail and creativity that were needed in the constructions upon which two examples due to Bergman [13, Examples 6.4 and 6.11] were based. On the other hand, it may be fruitful to look for additional such isomorphism classes with representatives that are not semiprime rings. Doing so would require a deeper study of simple bimodules. Note that we have considered only one-dimensional (necessarily simple) such bimodules in Proposition 2.7, as that context was enough to give the applications which we sought here.

I hope that the community will eventually develop a family of concrete examples to fully illustrate the diversity that is implicit in the classification results of Dorsey and Mesyan [13]. The preceding paragraph should not be construed to indicate a belief that the stratagem of factoring out a unique maximal (two-sided) ideal will prove decisive in advancing the overall theory of minimal ring extensions. On the contrary, I agree with the sentiment of Lambek, who in 1966 wrote that “The intersection of *all* [italics mine] maximal [two-sided] ideals of [a noncommutative ring]  $R$  does not seem to be a important concept” [21, page 57, lines 6-7]. Furthermore, I suggest that, in studying the minimal ring extensions of noncommutative rings, one should take note of some of the “recent” work on noncommutative ring theory, including what I see as its (probably reasonable) preoccupations with special kinds of ring extensions, representation theory, Hopf algebras, etc. Those choosing to engage in deepening our understanding of minimal ring extensions along those – or other – lines have my best wishes.

## References

- [1] N. Al-Kuleab and N. Jarboui, A note on intermediate matrix rings, *Far East J. Math. Educ.* 17 (4) (2018) 227–229.
- [2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.
- [3] P.-J. Cahen, D. E. Dobbs and T. G. Lucas, Characterizing minimal ring extensions, *Rocky Mountain J. Math.* 41 (4) (2011) 1081–1125.
- [4] D. E. Dobbs, Every commutative ring has a minimal ring extension, *Comm. Algebra* 34 (10) (2006) 3875–3881.

- [5] D. E. Dobbs, Characterizing finite fields via minimal ring extensions, *Comm. Algebra* 47 (12) (2019) 4945–4957. DOI: 10.1080/00927872.2019.1603303.
- [6] 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.
- [7] D. E. Dobbs, On minimal ring extensions of finite rings, *Gulf J. Math.* 12 (2) (2022) 1–30.
- [8] D. E. Dobbs, A characterization of  $\mathbb{F}_p$  via noncommutative minimal ring extensions, *Pales. J. Math.* 11 (4) (2022) 23–25.
- [9] D. E. Dobbs, Direct limits and minimal ring extensions, *Moroccan J. Algebra Geom. Appl.* 2 (2)(2023) 226–245
- [10] D. E. Dobbs and N. Jarboui, Characterizing finite Boolean rings by using finite chains of sub-rings, *Gulf J. Math.* 10 (1) (2021) 69–94.
- [11] D. E. Dobbs, B. Mullins, G. Picavet, and M. Picavet-L’Hermitte, On the FIP property for extensions of commutative rings, *Comm. Algebra* 33 (2005) 3091–3119.
- [12] D. E. Dobbs and J. Shapiro, A classification of the minimal ring extensions of certain commutative rings, *J. Algebra* 308 (2007) 800–821.
- [13] T. J. Dorsey and Z. Mesyan, On minimal extensions of rings, *Comm. Algebra* 37 (2009) 3463–3486.
- [14] D. Ferrand and J.-P. Olivier, Homomorphismes minimaux d’anneaux, *J. Algebra* 16 (1970) 461–471.
- [15] P. R. Halmos, *Naïve Set Theory*, The University Series in Undergrad. Math., Van Nostrand, Princeton, 1960.
- [16] T. W. Hungerford, *Algebra*, Graduate Texts in Math. 73, Springer-Verlag, New York-Berlin, 1980.
- [17] N. Jacobson, *Lectures in Abstract Algebra, Vol. III: Theory of Fields and Galois Theory*, Van Nostrand, Princeton, 1964.
- [18] I. Kaplansky, *Commutative Rings*, rev. ed., Univ. of Chicago Press, Chicago, 1974.
- [19] A. A. Klein, The finiteness of a ring with a finite maximal subring, *Comm. Algebra* 21 (4) (1993) 1389–1392.
- [20] T. J. Laffey, A finiteness theorem for rings, *Proc. Roy. Irish Acad. Sect. A*, 92 (2) (1992) 285–288.
- [21] J. Lambek, *Lectures on Rings and Modules*, Blaisdell, Waltham (MA), 1966.
- [22] T. G. Lucas, Minimal integral ring extensions, *J. Commut. Algebra* 3 (1) (2011) 47–81.
- [23] N. H. McCoy, *The Theory of Rings*, Macmillan, New York, 1964.