Palestine Journal of Mathematics

Vol. 9(2)(2020) , 604–619

ASSOCIATIVE RINGS IN WHICH 1 IS THE ONLY UNIT

David E. Dobbs and Noômen Jarboui

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 13A15; Secondary 13B21, 13B25, 13C15, 13H99, 16B99.

Keywords and phrases: Unit, von Neumann regular, idempotent element, reduced ring, Jacobson radical, Boolean ring, polynomial ring, algebraic extension, subring, integral extension.

Abstract Examples are given of associative rings in which 1 is the only unit. These rings coincide with the Boolean rings within the universe of one-sided Artinian rings (resp., of von Neumann regular rings; resp., of nonzero algebraic $\mathbb{Z}_2$-algebras; resp., of commutative semi-quasi-local rings). The class of these rings is stable under direct limits and arbitrary direct products. New examples of such rings include polynomial rings over $\mathbb{F}_2$ in an arbitrary (possibly infinite) number of algebraically independent commuting indeterminates. The 0- and 1-generated rings in which 1 is the only unit are classified up to isomorphism. Emphasis is given to the role of the 2-generated one-dimensional integral domains in which 1 is the only unit. Several open questions are identified.

1 Introduction

All rings and algebras considered in this paper are assumed to be associative with identity element; all subrings, ring extensions, algebras and ring/algebra homomorphisms are assumed unital. For any ring R, we let $\mathrm{U}(R)$ be its group of units, that is, its group of (two-sided) invertible elements. As the title indicates, our interest here is in studying the rings R such that $\mathrm{U}(R)$ is as small as possible, that is, the rings R such that $\mathrm{U}(R) = \{1\}$. In [9], Heinzer and Roitman considered certain principal ideal domains with this property. It was shown in [9] that, up to isomorphism, $\mathbb{Z}_2$ (the finite field with only two elements) and $\mathbb{Z}_2[X]$ (the polynomial ring in one indeterminate over $\mathbb{Z}_2$) are the only finitely generated Euclidean domains R such that $\mathrm{U}(R) = \{1\}$; and that this assertion does not hold if "Euclidean domains" is replaced by "principal ideal domains." One also finds examples in [9] of principal ideal domains R of infinite transcendence degree over $\mathbb{Z}_2$ such that $\mathrm{U}(R) = \{1\}$. The present work will pursue only a few analogues of the last-mentioned examples, as it seems more natural to organize at least part of this work in terms of n-generated rings where n is a non-negative integer, our point being that a ring R has $\mathrm{U}(R) = \{1\}$ if (and only if) $\mathrm{U}(A) = \{1\}$ for each finitely generated subring A of R. Indeed, if $r \in \mathrm{U}(R) \setminus \{1\}$, then $r \in \mathrm{U}(A)$ where A denotes the subring of R that is generated by $\{0, 1, r, r^{-1}\}$. This A is visibly n-generated for some $n \leq 2$, as we will adopt the terminology that a ring B is *n-generated* (over its prime ring Γ) if n is the least non-negative integer such that B can be generated as a Γ-algebra by adjoining a set of cardinality n to Γ.

Proposition 2.4 establishes the following easy but useful facts: if R is a ring such that $\mathrm{U}(R) = \{1\}$, then the Jacobson radical of R is trivial, R has no nonzero nilpotent elements, and if, in addition, $R \neq 0$, then the characteristic of R is 2. Proposition 2.3 records the fact that it is easy to give an example of a ring R that is not a principal ideal domain (indeed, not an integral domain at all) such that $\mathrm{U}(R) = \{1\}$: consider any Boolean ring R other than $\mathbb{Z}_2$. (Recall that a ring is said to be a *Boolean ring* if each of its elements is idempotent; it is well known that every Boolean ring is commutative and every nonzero Boolean ring has characteristic 2.) In fact, finite Boolean rings can be characterized in several ways (see Proposition 2.5), such as being the one-sided Artinian rings R with $\mathrm{U}(R) = \{1\}$, the semisimple rings R with $\mathrm{U}(R) = \{1\}$, and the semi-quasi-local commutative rings R with $\mathrm{U}(R) = \{1\}$. Moreover, arbitrary Boolean rings can be characterized as the (not necessarily commutative) von Neumann regular rings R such that $\mathrm{U}(R) = \{1\}$ (see Corollary 2.10). In addition (cf. Corollary 2.11), a (not necessarily commutative) ring R such that $\mathrm{U}(R) = \{1\}$ is algebraic as an algebra over $\mathbb{Z}_2$ if and only if R is a Boolean ring.

All our examples of rings R such that $\mathrm{U}(R) = \{1\}$ that were noted above were either Boolean or semi-quasi-local. Theorem 2.13 adds considerable diversity to the family of known examples, by establishing that a commutative ring A satisfies $\mathrm{U}(A) = \{1\}$ if and only if the polynomial ring $R := A[\{X_i\}]$ (in arbitrarily many indeterminates) satisfies $\mathrm{U}(R) = \{1\}$. The most accessible examples, taking A to be either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, are featured in Example 2.17. Additional families of "large" examples become available, thanks to Proposition 2.18, where it is shown that the class of rings R such that $\mathrm{U}(R) = \{1\}$ is stable under the formation of direct limits, arbitrary direct products and ultraproducts.

However, in keeping with the program suggested by the comments at the end of the first paragraph of this Introduction, our deepest results address the question of classifying, for $n \leq 2$, the n-generated rings having 1 as the only unit. Theorem 2.21 includes the following assertions. The 0-generated (resp., 1-generated) rings R such that $\mathrm{U}(R) = \{1\}$ are, up to isomorphism, 0 and $\mathbb{Z}_2$ (resp., $\mathbb{Z}_2[X]$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$). (Moreover, according to Proposition 2.20 (c), $\mathbb{Z}_2 \times \mathbb{Z}_2$ has the additional distinction of being, up to isomorphism, the only (not necessarily commutative) ring R such that $\mathrm{U}(R) = \{1\}$ and R is a minimal ring extension of its prime ring.) Any 2-generated commutative ring R such that $\mathrm{U}(R) = \{1\}$ must either be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or else have (Krull) dimension either 1 or 2. The only 2-generated two-dimensional integral domain R such that $\mathrm{U}(R) = \{1\}$ is, up to isomorphism, the polynomial ring $\mathbb{Z}_2[X, Y]$. The 2-generated one-dimensional integral domains R such that $\mathrm{U}(R) = \{1\}$ include an example of the coordinate ring of an affine curve of genus 1 over $\mathbb{Z}_2$ which was given by Heinzer and Roitman [9, Example 2.3]. The issue of classifying the 2-generated one-dimensional integral domains R such that $\mathrm{U}(R) = \{1\}$ is highlighted in Question 2.23. (See also Remark 2.22 (b).) In fact, a number of open questions are interspersed throughout the paper, as are several remarks indicating the sharpness of our results.

If R is a ring, $\mathrm{J}(R)$ denotes the Jacobson radical of R and $\mathrm{char}(R)$ denotes the characteristic of R. If $F \subseteq L$ are fields, then $\mathrm{td}_F(L)$ denotes the transcendence degree of L over F. As usual, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$; X, Y or $\{X_i\}$ will denote commuting, algebraically independent indeterminates over the ambient base ring(s); $\mathbb{F}_q$ denotes the finite field of cardinality q, for any prime-power q; and $|G|$ denotes the cardinal number of a set G. Any undefined notation or terminology is standard, as in [7], [14], [15].

2 Results

Although our main focus is on the case of commutative rings, we begin with a family of non-commutative rings whose only unit is 1.

Theorem 2.1. *If $\mathbf{X}$ is a set and $R := \mathbb{Z}_2\langle \mathbf{X} \rangle$, the free $\mathbb{Z}_2$-algebra on $\mathbf{X}$, then* $\mathrm{U}(R) = \{1\}$.

Proof. One way to view R is as the tensor algebra, over the ring $\mathbb{Z}_2$, of the $\mathbb{Z}_2$-vector space with basis $\mathbf{X}$. We will instead use a somewhat more concrete construction of R. (The following construction of R is in the spirit of [12, pages 67 and 123], whose treatment of the case of finite $\mathbf{X}$ extends easily to the general case.) As usual, let a *word* (or *monomial*) *in* $\mathbf{X}$ be either the empty word or an expression $u_1 \cdots u_n$ for some positive integer n such that each $u_i \in \mathbf{X}$. Two nonempty words in $\mathbf{X}$, say $u_1 \cdots u_n$ and $v_1 \cdots v_m$, are declared equal if and only if $n = m$ and $u_i = v_i$ for each i. Then the free monoid on $\mathbf{X}$ can be viewed as the monoid M whose underlying set is the collection of words in $\mathbf{X}$, with concatenation serving as the monoid operation in M (and the empty word serving as the identity element of M). We can take R as the monoid ring $\mathbb{Z}_2[M]$. From this point of view, an element of R is simply the sum of an element of $\mathbb{Z}_2$ and a (possibly empty) sum of finitely many nonempty monomials in $\mathbf{X}$. Hence, if $\mathbf{X} = \emptyset$, then $M = 0$ and $R = \mathbb{Z}_2$ (whose only unit is 1). Thus, we can assume, without loss of generality, that $\mathbf{X} \neq \emptyset$.

Let w be a nonempty word in $\mathbf{X}$. Then $w = u_1 \cdots u_n$ for some (uniquely determined) positive integer n and elements $u_i \in \mathbf{X}$ (possibly with $u_i = u_j$ for some $i \neq j$). It will be convenient to say that the *length* of w is n; and, for each positive integer k, to let R_k denote the set of (possibly empty) sums of finitely many nonempty words (in $\mathbf{X}$) of length k.

Suppose the assertion fails. Pick $\xi \in \mathrm{U}(R) \setminus \{1\}$, and put $\eta := \xi^{-1} \in R$. Evidently, $\eta \neq 1$.

Hence, by the above construction of R, there exist positive integers n and m such that

$$\xi = 1 + \sum_{i=1}^{n} s_i \quad \text{and} \quad \eta = 1 + \sum_{j=1}^{m} t_j,$$

where each $s_i \in R_i$, each $t_j \in R_j$, $s_n \neq 0$ and $t_m \neq 0$. Since the above expressions for ξ and η involve only finitely many elements of $\mathbf{X}$, we may assume, without loss of generality, that $\mathbf{X}$ is finite, say of cardinality N for some positive integer N. Denote the elements of $\mathbf{X}$ by $x_1, \ldots, x_N$.

Next, decree that $x_i < x_j$ if and only if $1 \leq i < j \leq N$. Extend this ordering to an ordering on the set of monomials in $\mathbf{X}$ by using the lexicographic ordering. To facilitate some subsequent reasoning, we next make this ordering explicit. First, decree that the empty word is $<$-related to any nonempty word. Next, if $u = u_1 \cdots u_n$ and $v = v_1 \cdots v_m$ are distinct nonempty words in $\mathbf{X}$ (with $u_i \in \mathbf{X}$ for each i and $v_j \in \mathbf{X}$ for each j), decree that $u < v$ if either $n < m$ or $n = m$ and there exists a positive integer $k \leq n$ such that $u_\lambda = v_\lambda$ whenever $1 \leq \lambda < k$ and $u_k < v_k$. It will be useful to observe the following fact.

(*) Let u, v and w be nonempty words in $\mathbf{X}$ such that $u < v$. Then $wu < wv$.

The proof of (*) follows easily from the above explication of $<$.

Now, since $s_n \neq 0$, we can write $s_n = \sum_{i=1}^{p} u_i$ where $u_1, \ldots, u_p$ are each nonempty words (in $\mathbf{X}$) of length n, for some positive integer p. Similarly, $t_m = \sum_{j=1}^{q} v_j$ where $v_1, \ldots, v_q$ are each nonempty words of length m, for some positive integer q. Using the above lexicographic ordering, we can relabel so that $u_{i_1} < u_{i_2}$ whenever $1 \leq i_1 < i_2 \leq p$ and $v_{j_1} < v_{j_2}$ whenever $1 \leq j_1 < j_2 \leq q$. Then, as

$$1 = \xi\eta = (1 + \sum_{i=1}^{n} s_i)(1 + \sum_{j=1}^{m} t_j) = 1 + \sum_{i=1}^{n} s_i + \sum_{j=1}^{m} t_j + \sum_{i,j} s_i t_j,$$

it follows that $s_n t_m = 0$, since each term other than 1 in the right-hand side of the above display can be expressed as a sum of monomials of length less than $n + m$ (whereas $s_n t_m$ can be expressed as a nonempty sum of monomials each of which has length $n+m$). Since $\text{char}(R) = 2$ and

$$s_n t_m = (\sum_{i=1}^{p} u_i)(\sum_{j=1}^{q} v_j) = \sum_{i=1}^{p} \sum_{j=1}^{q} u_i v_j,$$

with $u_1 v_1 \neq 0$, it follows that $u_1 v_1 = u_i v_j$ for some $(i, j) \neq (1, 1)$. There are two cases: either $i = 1$ or $1 < i$. If $i = 1$, then $1 < j$ (since $(i, j) \neq (1, 1)$), so that $v_1 < v_j$ (by the above relabeling), whence (*) ensures that $u_1 v_1 < u_1 v_j$, which is a contradiction since $u_1 v_j = u_i v_j = u_1 v_1$. Hence $1 < i$. Then the above explication of the ordering ensures that $u_1 v_1 < u_i v_j$, since u_1 and u_i are nonempty words of the same length such that $u_1 < u_i$. This, too, is a contradiction, since $u_1 v_1 = u_i v_j$. As each case led to a contradiction, no ξ with the above properties can exist, thus completing the proof.

□

Remark 2.2. Let $R := \mathbb{Z}_2\langle \mathbf{X} \rangle$, as in Theorem 2.1. It can be shown, by reasoning as in the final paragraph of the proof of Theorem 2.1, that R has no nonzero zero-divisors. (This can also be shown by viewing R as a tensor algebra.) Moreover, the ring R is noncommutative if (and only if) $|\mathbf{X}| \geq 2$. In that case, since R is a somewhat tractable noncommutative $\mathbb{Z}_2$-algebra that is $|\mathbf{X}|$-generated, one may be led to suspect that for commutative rings, polynomial rings (in commuting indeterminates) over $\mathbb{Z}_2$ will satisfy the "1 is the only unit" property and, more generally, the study of this property for commutative rings with suitably "small" generating sets will be especially fruitful for (commutative) integral domains. These suspicions will be borne out below: see Theorems 2.13 and 2.21.

Next, we record what is perhaps the simplest class of rings with the property in question.

Proposition 2.3. *If R is a Boolean ring, then* $\mathrm{U}(R) = \{1\}$.

Proof. We need only prove that if $a \in \mathrm{U}(R)$, then $a = 1$. As R is a Boolean ring, $a^2 = a$. Multiplying both sides of the equation by a^{-1} leads to $a = 1$, as desired.

□

Note that the proof of Proposition 2.3 shows more, namely, that 1 is the only possible idempotent unit of any ring.

Extending some terminology that is well established for the commutative case, we will say that a (not necessarily commutative) ring is *reduced* if it has no nonzero nilpotent elements. The next result gives some elementary, but useful, consequences of the "$\mathrm{U}(R) = \{1\}$" property.

Proposition 2.4. *Let R be a ring such that* $\mathrm{U}(R) = \{1\}$. *Then* $\mathrm{J}(R) = 0$ *and R is reduced. If, in addition, $R \neq 0$, then* $\mathrm{char}(R) = 2$.

Proof. If $r \in \mathrm{J}(R)$, then $1 - r \in \mathrm{U}(R)$, whence $1 - r = 1$ and $r = 0$. Hence $\mathrm{J}(R) = 0$. Next, since $1 = -1$, we get $2a = 0$ for all $a \in R$; and so, if $R \neq 0$, then $\mathrm{char}(R) = 2$. Finally, to show that R is reduced, it suffices to show that if $a \in R$ with $a^2 = 0$, then $a = 0$. This, in turn, holds since $(1 + a)^2 = 1 + 2a + a^2 = 1 + 0 + 0 = 1$ (whence $1 + a \in \mathrm{U}(R)$ and $1 + a = 1$).

□

After this research was completed, we came across [1]. In [1, page 6], D. F. Anderson and Badawi conjecture that if a commutative ring R is such that each non-zero-divisor of R is an idempotent element, then R is a Boolean ring. (The converse, which is clear, was included in the formulation of their conjecture, presumably so that it could be stated as a conjectured characterization of Boolean rings.) It was shown in [1, Theorem 2.8 (1)] that if R satisfies the hypothesis of the Anderson-Badawi conjecture, then $\mathrm{U}(R) = \{1\}$. Along those lines, we next offer Corollary 2.5, parts of which can be viewed as a strengthening of [1, Theorem 2.8 (2)]. As a whole, Corollary 2.5 shows that the archetypical examples of rings R satisfying $\mathrm{U}(R) = \{1\}$ from Proposition 2.3 are the typical examples within a number of important classes of (not necessarily commutative) rings. In fact, (5) is the only one of the seven equivalent conditions in the statement of Corollary 2.5 which stipulates commutativity.

Corollary 2.5. *For any ring R, the following conditions are equivalent:*
(1) R is finite and $\mathrm{U}(R) = \{1\}$*;*
(2) R is a finite Boolean ring;
(3) R is isomorphic to a direct product of finitely many copies of $\mathbb{Z}_2$;
(4) R is a semi-quasi-local Boolean ring;
(5) R is a semi-quasi-local commutative ring with $\mathrm{U}(R) = \{1\}$*;*
(6) $\mathrm{U}(R) = \{1\}$ *and R is either a left Artinian ring or a right Artinian ring;*
(7) R is a semisimple ring with $\mathrm{U}(R) = \{1\}$.

Proof. (6) $\Rightarrow$ (7): A one-sided Artinian ring with trivial Jacobson radical must be a (left and right) semisimple ring (cf. [15, Proposition 2, page 68]), and so the desired implication follows from the first assertion in Proposition 2.4.

(7) $\Rightarrow$ (3): Without loss of generality, $R \neq 0$. Assume (7). By Artin-Wedderburn Theory (cf. [15, Proposition 6, page 65]), $R \cong \prod_{i=1}^{k} \mathrm{M}_{n_i}(\Delta_i)$, a finite direct product of matrix rings over division rings Δ_i, with the i^{th} direct factor pertaining to $n_i \times n_i$ matrices for some positive integer n_i. As $\mathrm{U}(R) = \{1\}$, we get that $\mathrm{U}(\mathrm{M}_{n_i}(\Delta_i)) = \{1\}$ for each i. Thus, it suffices to prove that if $\mathrm{U}(\mathrm{M}_n(\Delta)) = \{1\}$ for some positive integer n and some division ring Δ, then $\Delta \cong \mathbb{Z}_2$ and $n = 1$. Now, if $0 \neq \delta \in \Delta$, then $\delta \in \mathrm{U}(\Delta)$, so that the diagonal matrix $B := \mathrm{diag}(\delta \ldots, \delta)$ is in $\mathrm{U}(\mathrm{M}_n(\Delta))$, whence B is the identity matrix. Thus $\delta = 1$ and so $\Delta = \{0, 1\} \cong \mathbb{Z}_2$. Finally, to see that $n = 1$, note that if $n \geq 2$, then the number of units in $\mathrm{M}_n(\Delta) \cong \mathrm{M}_n(\mathbb{Z}_2)$ (that is, the number of invertible $\mathbb{F}_2$-linear endomorphisms of an n-dimensional vector space over $\mathbb{F}_2$) is at least $2^n - 1 \geq 3 > 1$, contrary to hypothesis.

(3) $\Rightarrow$ (2): Clear.

(2) $\Rightarrow$ (1): Apply Proposition 2.3.

(1) $\Rightarrow$ (6): This implication follows from the fact that any finite ring is both left and right Artinian.

(4) $\Rightarrow$ (2): For the sake of completeness, we include the rather well known proof of this implication. Assume (4). As any Boolean ring is commutative, the "semi-quasi-local" hypothesis has a standard meaning (cf. [7]), namely, that R has finitely many maximal ideals. Let these be $M_1, , \dots , M_n$ (with $M_j \neq M_k$ if $j \neq k$). By the first assertion in Proposition 2.4, $\cap_{i=1}^n M_i = \mathrm{J}(R) = 0$. Hence, by the Chinese Remainder Theorem (cf. [11, Theorem 2.25, page 131]), $R \cong R/0 \cong \prod_{i=1}^n R/M_i$. As each R/M_i is a field that inherits the "Boolean ring" property from R, each $R/M_i \cong \mathbb{F}_2$, by the comment following the proof of Proposition 2.3. Then (3) and (2) follow at once.

(2) $\Rightarrow$ (4): This implication follows from the fact that any finite ring has only finitely many maximal ideals.

We have now shown that conditions (1), (2), (3), (4), (6) and (7) are equivalent. It remains to treat condition (5). By Proposition 2.3, (4) $\Rightarrow$ (5). It now suffices to prove that (5) $\Rightarrow$ (3). Assume (5). Then, as in the above proof that (4) $\Rightarrow$ (2), we get that $R \cong \prod_{i=1}^n R/M_i$, where the M_i are the n maximal ideals of R. As $\mathrm{U}(R) = \{1\}$, it follows that for each i, R/M_i is a field whose only unit is 1; that is, $R/M_i \cong \mathbb{F}_2$ for all i.

□

In Corollary 2.10, we will prove that the "$\mathrm{U}(R) = \{1\}$" condition can be used to characterize Boolean rings within the universe of (not necessarily commutative) von Neumann regular rings. If one assumes commutativity, a more accessible connection is easily exhibited: see Corollary 2.6 where, as usual, $\dim(R)$ denotes the Krull dimension of a commutative ring R.

Corollary 2.6. *Let R be a commutative ring such that* $\mathrm{U}(R) = \{1\}$. *Then R is a von Neumann regular ring if and only if* $\dim(R) = 0$.

Proof. It is well known that (a commutative ring) R is a von Neumann regular ring if and only if R is reduced and $\dim(R) = 0$ (cf. [14, Exercise 22, page 64]). Therefore, an application of the "reduced" assertion from Proposition 2.4 completes the proof.

□

Recall that an element a of a ring R is said to be (a) *von Neumann regular* (*element of* R) if there exists $x \in R$ such that $axa = a$. Of course, a ring R is a von Neumann regular ring if and only if each of its elements is a von Neumann regular element of R. For any ring R, it will be convenient to let $\mathrm{vnr}(R)$ denote the set of von Neumann regular elements of R, to let $\mathrm{Idem}(R)$ denote the set of idempotent elements of R, and to let $\mathrm{C}(R)$ denote the center of R. To prove one of our main results, Theorem 2.9, we will need the following two lemmas.

Lemma 2.7. *Let R be a reduced ring with $1 + 1 = 0$ in R. (For instance, let R be a ring such that* $\mathrm{U}(R) = \{1\}$.) *If $a, b \in R$ such that $ab \in$* $\mathrm{Idem}(R)$, *then $ab = ba$.*

Proof. The parenthetical assertion follows from Proposition 2.4. Next, without loss of generality, $R \neq 0$. As $ab \in \mathrm{Idem}(R)$, we have $(ab)^2 = ab$. Hence, $(ba)^3 = bababa = b(ab)^2a = b(ab)a = (ba)^2$. Thus $(ba)^4 = (ba)^3 = (ba)^2$. Since $\mathrm{char}(R) = 2$, it follows that $[(ba)^2 - ba]^2 = 0$. Then $(ba)^2 = ba$ since R is reduced. Thus $ba \in \mathrm{Idem}(R)$. Next, let $r \in R$. Then it is straightforward to check that $(bar - barba)^2 = 0$ and $(rba - barba)^2 = 0$. As R is reduced, it follows that $bar = barba$ and $rba = barba$. Thus $bar = rba$. Hence $ba \in \mathrm{C}(R)$. Similarly, $ab \in \mathrm{C}(R)$. Then

$$(ba - ab)^2 = (ba)^2 - (ba)ab - ab(ba) + (ab)^2 = (ba)^2 - a(ba)b - b(ab)a + (ab)^2$$

$$= (ba)^2 - (ab)^2 - (ba)^2 + (ab)^2 = 0.$$

As R is reduced, we get $ba = ab$, as desired.

□

The method of proof of the next lemma is widely known. The first-named author learned of it in the context of von Neumann regular rings during a conversation with Dick Bumby and Barbara Osofsky in 1971. This method was also used in the proof of a result of Raphael [19, Lemma 4] shortly afterwards. We include a sketch of the proof of Lemma 2.8 for the sake of completeness.

Lemma 2.8. *Let R be a ring and $a \in R$. Then $a \in \mathrm{vnr}(R)$ if and only if there exists $x \in R$ such that $a = axa$ and $x = xax$.*

Proof. The "if" assertion is trivial. For the "only if" assertion, assume that $a \in \mathrm{vnr}(R)$. Then there exists an element $y \in R$ satisfying $a = aya$. It is straightforward to verify that the element $x := yay$ satisfies $axa = a$ and $xax = x$, as desired.

□

Theorem 2.9. *Let R be a (not necessarily commutative) ring such that $\mathrm{U}(R) = \{1\}$. Then:*

(a) $\mathrm{vnr}(R) \subseteq \mathrm{Idem}(R) \subseteq \mathrm{C}(R)$.

(b) If $R \neq 0$ and $a \in R$, then a is algebraic over $\mathbb{Z}_2$ if and only if $a \in \mathrm{Idem}(R)$.

(c) Let $R \neq 0$. Then the algebraic closure of $\mathbb{Z}_2$ in R (that is, the set of all the elements of R which are algebraic over $\mathbb{Z}_2$) is a Boolean ring.

Proof. (a) Let $a \in \mathrm{vnr}(R)$. By Lemma 2.8, there exists $x \in R$ such that $axa = a$ and $xax = x$. It is clear that ax and xa are each idempotent elements. Also, Lemma 2.7 guarantees that $ax = xa$. As $R \neq 0$ without loss of generality, $\mathrm{char}(R) = 2$ by Proposition 2.4. Then one checks easily that $(1-ax+a)(1-ax+x) = 1$. As $\mathrm{U}(R) = \{1\}$, it follows that $1-ax+a = 1 = 1-ax+x$. Thus $a = ax \in \mathrm{Idem}(R)$. This completes the proof that $\mathrm{vnr}(R) \subseteq \mathrm{Idem}(R)$.

Now, let $x \in \mathrm{Idem}(R)$. We need to show that $x \in \mathrm{C}(R)$. To this end, let $r \in R$. One checks easily that $(xr - xrx)^2 = 0$ and $(rx - xrx)^2 = 0$. Since R is reduced, we get $xr = xrx$ and $rx = xrx$. Hence $xr = rx$. Thus $x \in \mathrm{C}(R)$. This completes the proof that $\mathrm{Idem}(R) \subseteq \mathrm{C}(R)$.

(b) As $R \neq 0$, the final assertion of Proposition 2.4 allows us to view $\mathbb{Z}_2 \subseteq R$. As the "if" assertion is clear, we turn to the "only if" assertion. Let $a \in R$ be algebraic over $\mathbb{Z}_2$. If $a \in \mathbb{Z}_2$, then $a \in \mathrm{Idem}(R)$. So, without loss of generality, $a \notin \mathbb{Z}_2$. Let

$$m(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in \mathbb{Z}_2[X]$$

be the minimal polynomial of a over $\mathbb{Z}_2$. Notice that $\deg(m(X)) = n \geq 2$ since $a \notin \mathbb{Z}_2$. There are now two cases to consider.

Case 1: $c_0 = 1$. Then $0 = m(a) = a^n + c_{n-1}a^{n-1} + \cdots + c_1a + 1$. It follows that $\alpha := -a^{n-1} - c_{n-1}a^{n-2} - \cdots - c_1 \in \mathbb{Z}_2[a] \subseteq R$ satisfies $a\alpha = 1 = \alpha a$, and so $a \in \mathrm{U}(R)$. Hence $a = 1 \in \mathrm{Idem}(R)$.

Case 2: $c_0 = 0$. Then $m(X) = X^kf(X)$, for some positive integer k and some $f(X) \in \mathbb{Z}_2[X]$ such that $f(0) = 1$. We claim that $k = 1$. Assume, for the sake of argument, that this claim fails. Then $(af(a))^k = (a^kf(a))f(a)^{k-1} = m(a)f(a)^{k-1} = 0$. Since Proposition 2.4 ensures that R is reduced, we get $af(a) = 0$. Thus a is a root of the monic polynomial $Xf(X) \in \mathbb{Z}_2[X]$. But this contradicts the minimality of $\deg(m(X))$, since $\deg(Xf(X)) < \deg(X^kf(X)) = \deg(m(X))$. This proves the above claim that $k = 1$, and so $m(X) = Xf(X)$. Now, since $f(0) = 1$ and $n \geq 2$, the fact that $\mathrm{char}(R) = 2$ yields a polynomial $g(X) \in \mathbb{Z}_2[X]$ such that $f(X) + 1 = Xg(X)$. Thus $X^2g(X) = Xf(X) + X = m(X) + X$, and so

$$ag(a)a = a^2g(a) = m(a) + a = 0 + a = a.$$

Thus $a \in \mathrm{vnr}(R)$, since $g(a) \in \mathbb{Z}_2[a] \subseteq R$. Therefore, the first part of assertion (a) yields that $a \in \mathrm{Idem}(R)$, as desired.

(c) Of course, both 0 and 1 are idempotent and, hence, algebraic over $\mathbb{Z}_2$. Hence, by (b), it suffices to prove that if $a, b \in \mathrm{Idem}(R)$, then $ab, a \pm b \in \mathrm{Idem}(R)$. By (a), both a and b are elements of $\mathrm{C}(R)$. It follows that $ab \in \mathrm{Idem}(R)$, since $(ab)^2 = a(ba)b = a(ab)b = a^2b^2 = ab$. Moreover, since $\mathrm{char}(R) = 2$ by Proposition 2.4, $a + b = a - b$ satisfies $(a+b)^2 = a^2 + (ab + ba) + b^2 = a + 2ab + b = a + b$, thus completing the proof.

□

We can now give the promised strengthening of Corollary 2.6. The case of Corollary 2.10 in which R is a commutative ring was observed by D. F. Anderson and Badawi [1, page 5].

Corollary 2.10. *Let R be a (not necessarily commutative) ring. Then the following two conditions are equivalent:*
(*1*) *R is Boolean;*
(*2*) *R is a von Neumann regular ring with* $\mathrm{U}(R) = \{1\}$.
If R is a commutative ring, then the above equivalent conditions (1) and (2) are also equivalent to the following condition:
(*3*) $\mathrm{U}(R) = \{1\}$ *and* $\dim(R) = 0$.

Proof. (1) $\Rightarrow$ (2): Apply Proposition 2.3 and the fact that each Boolean ring is von Neumann regular.
(2) $\Rightarrow$ (1): This implication follows from the first inclusion stated in Theorem 2.9 (a).
Finally, assume also that R is commutative. Then (3) $\Rightarrow$ (2) by Corollary 2.6; and (1) $\Rightarrow$ (3) (resp., (2) $\Rightarrow$ (3)) by Proposition 2.3 and the fact that any Boolean ring is zero-dimensional (resp., since any commutative von Neumann regular ring is zero-dimensional).
□

Parts (b) and (c) of Theorem 2.9 (b) each readily yield the following far-reaching generalization of the implication (1) $\Rightarrow$ (2) in Corollary 2.5.

Corollary 2.11. *Let R be a nonzero (not necessarily commutative) ring such that* $\mathrm{U}(R) = \{1\}$. *Then the ring extension $\mathbb{Z}_2 \subseteq R$ is algebraic if and only if R is a Boolean ring.*

The next corollary characterizes the nonzero ring R of smallest cardinality with the property that $\mathrm{U}(R) = \{1\}$. First, we must address the fact that there are some inequivalent definitions of "valuation ring" in the literature, even in the commutative case. In this regard, we will follow the usage of, for instance, [13, page 176]. So, for our purposes, a ring V is said to be a *valuation ring* if V is a nonzero commutative ring such that V is quasi-local and each finitely generated ideal of V is principal.

Corollary 2.12. *Let R be a nonzero commutative ring such that* $\mathrm{U}(R) = \{1\}$. *Then the following conditions are equivalent:*
(*1*) *R is a field;*
(*2*) *R is a valuation ring;*
(*3*) *R is quasi-local;*
(*4*) $R \cong \mathbb{Z}_2$.

Proof. It is clear that (1) $\Rightarrow$ (2) $\Rightarrow$ (3); and that (4) $\Rightarrow$ (1). It remains only to prove that (3) $\Rightarrow$ (4).
Assume (3). Then by Corollary 2.5, R is isomorphic to a direct product of finitely many, say n, copies of $\mathbb{Z}_2$. This direct product has exactly n maximal ideals. As R is (nonzero and) quasi-local, $n = 1$, whence $R \cong \mathbb{Z}_2$, as desired.
□

We next use Proposition 2.4 to obtain new families of examples of commutative rings R such that $\mathrm{U}(R) = \{1\}$. In choosing an appropriate context that may lead to examples with a non-Boolean flavor, we are motivated by Corollary 2.11 to consider rings that are *not* algebraic over their prime rings. Of course, the simplest examples of such rings are polynomial rings (over nonzero coefficient rings). Theorem 2.12 shows that in the commutative case, the "$\mathrm{U}(R) = \{1\}$" property transfers between (that is, to and from) a ring and its polynomial ring (in arbitrarily many variables).

Theorem 2.13. *For any commutative ring R, the following conditions are equivalent:*
(*1*) $\mathrm{U}(R) = \{1\}$*;*

(2) *For each nonempty (possibly infinite) set $\{X_i\}$ of commuting, algebraically independent indeterminates over R, the ring $R[\{X_i\}]$ has only 1 as a unit;*

(3) *There exists $\{X_i\}$ as in (2) such that the ring $R[\{X_i\}]$ has only 1 as a unit.*

Proof. Without loss of generality we can assume that $R \neq \{0\}$. It is trivial that (2) $\Rightarrow$ (3). Also, it is clear that (3) $\Rightarrow$ (1), since $\{1\} \subseteq \mathrm{U}(R) \subseteq \mathrm{U}(R[\{X_i\}])$. Finally, assume (1). To prove (2), let $\Lambda = \{X_i \mid i \in I\}$ be a set of commuting, algebraically independent indeterminates over R and let $A = R[\Lambda]$. It suffices to prove that if $f \in \mathrm{U}(A)$, then $f = 1$. By restricting attention to the indeterminates that actually appear in f or its multiplicative inverse, it is then clear that there exists a finite subset J of I such that f is a unit of $R[\{X_j \mid j \in J\}]$. Thus, by replacing I with J, we may assume, without loss of generality, that I is finite. Then, by induction on the cardinal number of I, we may assume that $\Lambda = \{X\}$, a singleton set, with f a unit of $A = R[X]$. As $A \cong \mathbb{Z}_2\langle\{X\}\rangle$, the proof can be finished by applying Theorem 2.1. For readers wishing to avoid considerations involving noncommutative rings, the preceding sentence can be replaced by the next paragraph.

We have $f \neq 0$ (since $R \neq \{0\}$ ensures that $0 \neq 1$ in A), and so we can write $f = r_nX^n + r_{n-1}X^{n-1} + \cdots + r_0$ for some non-negative integer n and some finite set of elements $r_k \in R$ with $r_n \neq 0$. The nature of the units of a polynomial ring over a commutative ring is well known: cf. [10, Lemma 6.1.2]. Therefore, $r_0 \in \mathrm{U}(R)$ and each of the elements $r_1, r_2, \ldots, r_n$ is nilpotent. Consequently, $r_0 = 1$ by hypothesis; and $0 = r_1 = r_2 = \ldots = r_n$ by Proposition 2.4. Thus $f = 1$, as desired.

□

The most immediate way to build some examples by applying Theorem 2.13 would be to take R in it to be any of the principal ideal domains satisfying $\mathrm{U}(R) = \{1\}$ that were found in [9]. Many additional families of examples will be given below. But, first, the proof of Theorem 2.13 raises some important questions.

Question 2.14. Our interest in studying the rings R such that $\mathrm{U}(R) = \{1\}$ in a context going beyond the setting of principal ideal domains from [9] has included some arguments involving possibly noncommutative rings. As the above alternate way to finish the proof of Theorem 2.13 illustrated, some arguments are technically easier for the context of commutative rings. In view of the care that was needed in proving Theorem 2.1, one must ask: besides the examples issuing from Theorem 2.1, what are some other accessible families of noncommutative rings R such that $\mathrm{U}(R) = \{1\}$?

Question 2.15. Commutativity of R was used in the proof of Theorem 2.13 in two ways: the commutativity of R was inherited by rings of polynomials over R in arbitrarily many variables, and $\mathrm{U}(R[X])$ is well understood in case R is commutative. However, for an arbitrary noncommutative ring, we are not aware of any characterization of the units of $R[X]$. It is easy to use Proposition 2.4 in conjunction with some classical results of Amitsur and McCoy on radicals to show that if R is a ring such that $\mathrm{U}(R) = \{1\}$ and X is an indeterminate over R, then $R[X]$ is a reduced ring and $\mathrm{J}(R[X]) = 0$ (and $\mathrm{char}(R[X]) = 2$ if $R \neq 0$). But we do not know how to characterize the units of $R[X]$ under these conditions. This raises the question: can one characterize the units of $R[X]$ for noncommutative rings R, at least in the case where $R[X]$ is a reduced ring and $\mathrm{J}(R[X]) = 0$?

Remark 2.16. The assumption "R is semi-quasi-local" cannot be deleted from conditions (4) and (5) in the statement of Corollary 2.5. Indeed, consider the polynomial ring $R = \mathbb{Z}_2[X]$. By Theorem 2.13, $\mathrm{U}(R) = \mathrm{U}(\mathbb{Z}_2) = \{1\}$, but R is not a Boolean ring (and R is not semi-quasi-local or finite or one-sided Artinian or semisimple).

We next use Theorem 2.13 to build some new examples of commutative rings R such that $\mathrm{U}(R) = \{1\}$. By "new", we mean that the following examples cannot be explained by appealing to Corollary 2.5, Corollary 2.10 or Corollary 2.12.

Example 2.17. (a) The polynomial ring $A := \mathbb{Z}_2[X]$ is a (commutative) integral domain, but not a field, satisfying $\mathrm{U}(A) = \{1\}$; also, A is not a Boolean ring and A is not semi-quasi-local. The polynomial ring $B := (\mathbb{Z}_2 \times \mathbb{Z}_2)[X]$ is a commutative ring, but not an integral domain, satisfying $\mathrm{U}(B) = \{1\}$; also, B is not a Boolean ring and B is not semi-quasi-local.

(b) For each non-negative integer n, there exists an integral domain (resp., a commutative ring that is not an integral domain) R that is n-dimensional and Noetherian such that $\mathrm{U}(R) = \{1\}$.

(c) There exists an integral domain (resp., a commutative ring that is not an integral domain) R that is a coherent ring such that $\dim(R) = \infty$ and $\mathrm{U}(R) = \{1\}$.

Proof. (a) Since $\mathrm{U}(\mathbb{Z}_2) = \{1\}$ and $\mathrm{U}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{1\}$, Theorem 2.13 ensures that $\mathrm{U}(A) = \{1\}$ and $\mathrm{U}(B) = \{1\}$. Also, the conclusions that neither A nor B is semi-quasi-local come from the general fact that if Λ is any nonzero commutative ring, then the polynomial ring $\Lambda[X]$ has infinitely many maximal ideals (cf. [14, page 25]). The other assertions are clear.

(b) Take R to be the polynomial ring $A[X_1, \dots, X_n]$ in n commuting algebraically independent indeterminates over the ring $A := \mathbb{F}_2$ (resp., over the ring $A := \mathbb{F}_2 \times \mathbb{F}_2$). As in the proof of (a), Theorem 2.13 ensures that $\mathrm{U}(R) = \{1\}$. As A is a zero-dimensional Noetherian ring, R is n-dimensional by [7, Theorem 30.5] (cf. [14, Theorem 39]) and R is a Noetherian ring by the Hilbert Basis Theorem.

(c) Take R to be the polynomial ring $A[X_1, \dots, X_n, \dots]$ in denumerably many commuting algebraically independent indeterminates over the ring $A := \mathbb{F}_2$ (resp., over the ring $A := \mathbb{F}_2 \times \mathbb{F}_2$). Once again, as in the proof of (a), Theorem 2.13 ensures that $\mathrm{U}(R) = \{1\}$. Also, since $A \neq 0$, it is clear that $\dim(R) = \infty$. (Of course, this is due to the chain $\{(X_1, \dots, X_n) \mid n = 1, 2, \dots\}$ of prime ideals of R.) Since A is a Noetherian ring, the fact that R is a coherent ring follows from a result about direct limits of suitable directed systems whose transition maps are flat: cf. [8, Corollary 2.3.4 and Theorem 2.3.3]. The other assertions are clear. This completes the proof.

□

The next result collects some other ways to build some relevant rings. Proposition 2.18 (a) is motivated by Theorem 2.13. (Indeed, the latter result ensures that $R := \mathbb{Z}_2[X_1, ..., X_n, ...]$ satisfies $\mathrm{U}(R) = \{1\}$. This example is of special interest because this ring R is not finitely generated as an algebra over its prime ring $\mathbb{Z}_2$.) Our motivation for Proposition 2.18 (b) comes from the possible vanishing of the nilradical of a direct product of commutative rings or the Jacobson radical of a finite direct product of rings. One motivation for Proposition 2.18 (c) comes from the fact that any ultraproduct (for instance, any direct product) of Boolean rings is a Boolean ring. As ultraproducts may be less familiar to some readers than direct limits or direct products, the proof of Proposition 2.18 (c) includes the definition of an ultraproduct, while Remark 2.19 (a) indicates an alternate approach to Proposition 2.18 (c) via some relevant model theory.

Proposition 2.18. *(a) If $\{R_i\}$ is a directed system of commutative rings such that $\mathrm{U}(R_i) = \{1\}$ for all i, then the direct limit $R := \varinjlim_i R_i$ also satisfies $\mathrm{U}(R) = \{1\}$.*

(b) If R is the direct product of a (possibly infinite) multiset $\{R_i\}$ of rings, then $\mathrm{U}(R) = \{1\}$ if and only if $\mathrm{U}(R_i) = \{1\}$ for each i.

(c) Let J be a (possibly infinite) index set and let $\mathcal{F}$ be an ultrafilter on J. Let $\{R_\alpha \mid \alpha \in J\}$ be a multiset of rings (possibly with $R_\beta = R_\gamma$ for some $\beta \neq \gamma$) such that $\mathcal{V} := \{\alpha \in J \mid \mathrm{U}(R_\alpha) = \{1\}\} \in \mathcal{F}$. Then the ultraproduct $R := \prod R_\alpha/\mathcal{F}$ satisfies $\mathrm{U}(R) = \{1\}$.

Proof. Part (b) is easy (and has already been used implicitly). As for (a), we assume familiarity with direct limits of commutative rings, as in [2, Exercises 14, 15 and 21, pages 32-34]. Suppose $\xi \in \mathrm{U}(R)$. Then ξ can be viewed as an equivalence class $[\xi_i]$, with $\xi_i \in R_i$ for all i, for which there exists an equivalence class $\eta = [\eta_i]$, with $\eta_i \in R_i$ for all i, such that $\xi\eta = 1 \in R$. It follows from the above-mentioned exercises in [2] that there exists an index j such that $\xi_i\eta_i = 1 \in R_i$ for all $i \geq j$. Thus, if $i \geq j$, then $\xi_i \in \mathrm{U}(R_i)$. Then $\xi_i = 1 \in R_i$ for all $i \geq j$. It follows that $\xi = [\xi_i] = 1 \in R$, as desired.

(c) Recall (cf. [10, page 180]) the following straightforward construction of the ring R. Consider the direct product $P := \prod_{\alpha\in J} R_\alpha$. Since $\mathcal{F}$ is an ultrafilter on J, it is easy to see that

$$I := \{f = (f_\alpha) \in P \mid \{\alpha \in J \mid f_\alpha = 0\} \in \mathcal{F}\}$$

is an ideal of P. Then the ultraproduct $R = \prod R_\alpha/\mathcal{F}$ is defined to be the factor ring P/I. We will show that if $u \in P$ is such that $\overline{u} := u + I \in \mathrm{U}(R)$, then $\overline{u} = 1 \in R$, that is, that

$$\mathcal{T} := \{\alpha \in J \mid u(\alpha) - 1 = 0 \in R_\alpha\}$$

satisfies $\mathcal{T} \in \mathcal{F}$. Pick $v \in P$ such that $\overline{v} := v + I = \overline{u}^{-1} \in R$. Then $uv - 1 \in I$; that is,

$$\mathcal{S} := \{\alpha \in J \mid u(\alpha)v(\alpha) = 1\}$$

satisfies $\mathcal{S} \in \mathcal{F}$. Observe that $\mathcal{S} \cap \mathcal{V} \subseteq \mathcal{T}$. Since $\mathcal{S}$ and $\mathcal{V}$ are each elements of $\mathcal{F}$ and $\mathcal{F}$ is a filter, it follows that $\mathcal{T}$ is also an element of $\mathcal{F}$, as desired.

□

Remark 2.19. (a) A deeper perspective on Proposition 2.18 (c) is provided by Loś's Theorem (also known as the Fundamental Theorem of Ultraproducts, as in [3, Theorem 5.1.0.1]) and some of its immediate consequences. For instance, since the axioms for rings constitute a first-order theory, an application of [3, Corollary 5.1.0.3] gives another proof that any ultraproduct of rings is a ring. Then, since the statement that $\mathrm{U}(R) = \{1\}$ can easily be expressed as a sentence in first-order logic in the language of rings, Proposition 2.18 (c) follows at once from the reformulation of Loś's Theorem in [3, Corollary 5.1.0.3].

(b) Ultraproducts can be used to produce examples of integral domains R such that $\mathrm{U}(R) = \{1\}$ and R is more complicated than the integral domains that were considered in Example 2.17. For instance, consider an ultraproduct $R := \prod R_\alpha/\mathcal{F}$ such that R_α is a polynomial ring $\mathbb{Z}_2[X_1, \dots, X_n]$ (where the positive integer n can depend on α) for $\mathcal{F}$-many α (that is, such that the set of indexes α for which R_α is such a polynomial ring is an element of $\mathcal{F}$). Then R is an integral domain (cf. [17, item 1.1.7]) and $\mathrm{U}(R) = \{1\}$ by Theorem 2.13 and Proposition 2.18 (c). In case each R_α is a polynomial ring of the above form (hence, a Krull domain and a Cohen-Macaulay ring, hence universally catenarian), the prime spectrum of R can be studied to some extent (cf. [18, page 783]) but is extremely complicated (cf. [18, especially page 793]).

(c) Consider the special case of Proposition 2.18 (c) in which $\mathrm{U}(R_\alpha) = \{1\}$ for each $\alpha \in J$. As above, take $P := \prod_{\alpha\in J} R_\alpha$. Hence, by Proposition 2.18 (b), $\mathrm{U}(P) = \{1\}$. Since the ring R in Proposition 2.18 (c) takes the form $R = P/I$, we wish to stress that the property that a ring has only the trivial unit is not preserved by arbitrary homomorphic images. To establish this fact, it suffices to produce a $\mathbb{Z}_2$-algebra A such that $\mathrm{U}(A) \neq \{1\}$. (Indeed, let A be any $\mathbb{Z}_2$-algebra that properly contains $\mathbb{Z}_2$. Pick any generating set S of A as a $\mathbb{Z}_2$-algebra. Necessarily, S is nonempty. Take $\mathbf{X}$ to be any set such that $|\mathbf{X}| = |S|$. Then A is a $\mathbb{Z}_2$-algebra homomorphic image of the free $\mathbb{Z}_2$-algebra $B := \mathbb{Z}_2\langle\mathbf{X}\rangle$, and so $A \cong B/\mathcal{I}$ for some ideal $\mathcal{I}$ of B. As $\mathrm{U}(B) = \{1\}$ by Theorem 2.1, it follows that every $\mathbb{Z}_2$-algebra is isomorphic to a factor algebra of a $\mathbb{Z}_2$-algebra that has only the trivial unit.) Notice that the $\mathbb{Z}_2$-algebra $\mathbb{Z}_2[X]/(X^2)$ has a (in fact, exactly one) nontrivial unit, namely, $1 + X + (X^2)$. This algebra will make another brief (but necessary) appearance in the proof of Proposition 2.20 (b).

Recall from the first paragraph of the Introduction that the study of the rings R such that $\mathrm{U}(R) = \{1\}$ can be reduced in theory (by studying the units of suitable subrings) to the context of rings R that are n-generated over the prime ring Γ, for $n = 0, 1, 2$. In case n is 0 (resp., 1), such rings R are classified up to isomorphism in part (a) (resp., part (b)) of Proposition 2.20. These results identify pertinent roles for the rings 0, $\mathbb{Z}_2$, $\mathbb{Z}_2[X]$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Part (c) of Proposition 2.20 identifies a different kind of behavior, for which $\mathbb{Z}_2 \times \mathbb{Z}_2$ is, up to isomorphism, the sole example. This has to do with minimal ring extensions (cf. [6]), a concept that plays a role in parts (b) and (c) of Proposition 2.20. (Recall that if $A \subset B$ are rings, then $A \subset B$ is said to be a *minimal ring extension* if there does not exist any ring C

such that $A \subset C \subset B$.) The first classification result on minimal ring extensions was due to Ferrand-Olivier [6, 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) a minimal field extension of k, $k \times k$ or $k[X]/(X^2)$. (A detailed proof of this result was recently given in Section 2 of the survey article [4].) Although [6] introduced the notion of a "minimal ring extension" only in the context of commutative rings, the literature has also considered this notion for ring extensions involving (possibly) noncommutative rings (cf. [5] and its bibliography). This level of generality is needed in Proposition 2.20 (c).

Proposition 2.20. (*a*) *Let R be a* 0*-generated ring. Then R satisfies* $\mathrm{U}(R) = \{1\}$ *if and only if either $R = 0$ or $R \cong \mathbb{Z}_2$.*

(*b*) *Let R be a* 1*-generated ring. Then R satisfies* $\mathrm{U}(R) = \{1\}$ *if and only if R is isomorphic to* (*exactly one of*) $\mathbb{Z}_2[X]$ *or* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(*c*) *Up to isomorphism,* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *is the only* (*possibly noncommutative*) *ring R such that* $\mathrm{U}(R) = \{1\}$ *and R is a minimal ring extension of its prime ring.*

Proof. (a) The "if" assertion is clear, and we will now prove the "only if" assertion. Suppose that $R \neq 0$ is a 0-generated ring such that $\mathrm{U}(R) = \{1\}$. Then R is a prime ring and, by Proposition 2.4, of characteristic 2, hence isomorphic to $\mathbb{Z}_2$, which completes the proof of (a).

(b) The "if" assertion follows from Theorem 2.13 and Proposition 2.18 (b). We will now prove the "only if" assertion. As R is a 1-generated ring, $R \neq 0$ and R properly contains its prime ring, Γ. Since $\mathrm{U}(R) = \{1\}$, Proposition 2.4 allows us to identify $\Gamma = \mathbb{Z}_2$. Thus $R = \mathbb{Z}_2[u]$, for some $u \in R \setminus \Gamma$. If u is transcendental over $\mathbb{Z}_2$, then $R \cong \mathbb{Z}_2[X]$. In the remaining case, u is algebraic over $\mathbb{Z}_2$. Hence, by Theorem 2.9 (b), $u^2 = u$. Then

$$\mathbb{Z}_2 \subset \mathbb{Z}_2 + \mathbb{Z}_2 u = \mathbb{Z}_2[u] = R.$$

It follows that R is a 2-dimensional vector space over $\mathbb{Z}_2$, and so $\mathbb{Z}_2 \subset R$ must be a minimal ring extension. Moreover, R must be a commutative ring.

Consider the field $k := \mathbb{F}_2$ $(= \mathbb{Z}_2)$. It is clear that if A and B are k-algebras, then any ring isomorphism $A \to B$ is also a k-algebra isomorphism $A \to B$. We next consider the alternatives provided by the classification result of Ferrand-Olivier [6, Lemme 1.2] which was mentioned above. First, observe that if $k \subset L$ is a minimal field extension, then $\mathrm{U}(L) \neq \{1\}$ (the point being that $|\mathrm{U}(L)| \geq |k|^2 - 1 = 3 > 1$). Next, since $x := X + (X^2)$ is a nonzero nilpotent element of $R_1 := k[X]/(X^2)$, it follows from the "reduced" assertion of Proposition 2.4 that $\mathrm{U}(R_1) \neq \{1\}$. (It can be seen directly that $|\mathrm{U}(R_1)| = 2$ since $\mathrm{U}(R_1) = \{1, 1 + x\}$; on the other hand, Proposition 2.18 (b) ensures that $\mathrm{U}(k \times k) = \{1\}$.) Therefore, [6, Lemme 1.2] ensures that $R \cong k \times k$, which completes the proof of (b).

For an alternate end for the proof of (b), one can begin at the point where one has shown "u is algebraic over $\mathbb{Z}_2$" and argue as follows. Then $R = \mathbb{Z}_2[u]$ is a commutative ring and a finite-dimensional vector space over $\mathbb{Z}_2$. Hence R is a finite ring and also an algebraic extension of $\mathbb{Z}_2$. Thus by Theorem 2.9 (b), R is a finite Boolean ring. So (cf. Corollary 2.5), R is isomorphic to a finite direct product of n copies of $\mathbb{F}_2$, for some integer $n \geq 2$. As this ring isomorphism is also an isomorphism of vector spaces over $k := \mathbb{F}_2$, we have $n = \dim_k(R) = 2$, thus completing the alternate proof of (b).

(c) It is clear that any ring R which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ must satisfy $\mathrm{U}(R) = \{1\}$ and must be a minimal ring extension of its prime ring. Conversely, suppose that R is a ring such that $\mathrm{U}(R) = \{1\}$ and R is a minimal ring extension of its prime ring. To prove that $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, one need only rework the proof of (b), bearing in mind also that $\mathbb{Z}_2 \subset \mathbb{Z}_2[X]$ is not a minimal ring extension (thanks to the existence of, for instance, $\mathbb{Z}_2[X^2]$). This completes the proof. □

From the above point of view of studying the behavior of the n-generated subrings, it is apparent from parts (a) and (b) of Proposition 2.20 that the key to understanding the rings R such that $\mathrm{U}(R) = \{1\}$ is to understand the case $n = 2$. Thanks to Theorem 2.13, we know that $\mathbb{Z}_2[X, Y]$ is one such ring. While we will not solve the general "$n = 2$" problem here, we will say more about it in Theorem 2.21. First, we will devote a paragraph to two results of Heinzer-Roitman, the second of which falls under the "$n = 2$" umbrella.

Recall that Proposition 2.20 (a), (b) identified special roles that are played in the theory by the rings 0, $\mathbb{Z}_2$, $\mathbb{Z}_2[X]$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Those roles should be contrasted with the following result of Heinzer-Roitman [9, Theorem 3.5]: a ring R is a finitely generated Euclidean domain such that $\mathrm{U}(R) = \{1\}$ (if and) only if R is isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2[X]$. (It is interesting that the "Euclidean" context would lead, for rings that are 0- or 1-generated, to an answer that consists of uniting half of the above answer from Proposition 2.20 (a) with half of the answer from Proposition 2.20 (b); notice that the Boolean rings 0 and $\mathbb{Z}_2 \times \mathbb{Z}_2$ would not fit into the domain-theoretic context.) Perhaps more to the/our "$n = 2$" point is the following result of Heinzer-Roitman [9, Example 2.3]: the ring

$$R := \mathbb{F}_2[X, Y]/(Y^2 + Y + X^3 + X^2 + 1)$$

is a non-Euclidean principal ideal domain such that $\mathrm{U}(R) = \{1\}$. As noted in [9], this ring R is the coordinate ring of an affine curve of genus 1 over $\mathbb{Z}_2$. In particular, $\dim(R) = 1$.

For convenience, some of Proposition 2.20 will be restated in the next result. Theorem 2.21 will also say more about the case $n = 2$ (and, more generally, the n-generated case) for commutative rings, while also delving into attempts to characterize the examples of "low" Krull dimension. (As noted in the penultimate sentence of the preceding paragraph, there are good algebro-geometric reasons for focusing on the one-dimensional examples that are integral domains, but our approach to them in Theorem 2.21 will use standard tools from multiplicative ideal theory.) Those attempts will lead to a final list of open questions, some of which are reminiscent of some open questions that were identified in [9].

Theorem 2.21. *Let R be a ring. Then:*

(a) $\mathrm{U}(R) = \{1\} \Leftrightarrow \mathrm{U}(A) = \{1\}$ *for every finitely generated subring A of R* $\Leftrightarrow \mathrm{U}(A) = \{1\}$ *for every 0-generated, 1-generated, or 2-generated subring A of R.*

(b) R is a 0-generated ring satisfying $\mathrm{U}(R) = \{1\}$ *if and only if R is either 0 or isomorphic to $\mathbb{Z}_2$.*

(c) R is a 1-generated ring satisfying $\mathrm{U}(R) = \{1\}$ *if and only if R is isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_2[X]$ (for some element X that is transcendental over $\mathbb{Z}_2$).*

(d) If R is an n-generated commutative ring for some positive integer n and if $\mathrm{U}(R) = \{1\}$, *then* $\dim(R) \leq n$.

(e) If R is a 2-generated commutative ring and $\mathrm{U}(R) = \{1\}$, *then either $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or* $\dim(R)$ *is either 1 or 2. (All four possibilities can arise.)*

(f) If R is a 2-generated (commutative) integral domain and $\mathrm{U}(R) = \{1\}$, *then either there exists $X \in R$ which is transcendental over $\mathbb{Z}_2$ such that $\mathbb{Z}_2[X] \subset R$ is an integral ring extension or $R = \mathbb{Z}_2[X, Y]$ for some pair X, Y of algebraically independent indeterminates over $\mathbb{Z}_2$.*

Proof. The assertion in (a) was proved in the first paragraph of the Introduction. The assertions in (b) and (c) were proved in parts (a) and (b), respectively, of Proposition 2.20.

(d) As $n \neq 0$, it follows that R is nonzero (and R is not a prime ring). So, by the final assertion of Proposition 2.4, the prime ring of R can be identified with $\mathbb{Z}_2$. Since R is an n-generated ring, there is an ideal I of the polynomial ring $B := \mathbb{Z}_2[X_1, \ldots, X_n]$ such that $B/I \cong R$. Since $\mathbb{Z}_2$ is a 0-dimensional Noetherian ring, we have $\dim(B) = n$ (cf. [7, Theorem 30.5], [14, Theorem 39]). Hence $\dim(R) \leq n$.

(e) Suppose the assertion fails. Then, by (d), $\dim(R) = 0$. As R is also reduced (by Proposition 2.4), R is a von Neumann regular ring (cf. Corollary 2.6). Since $\mathrm{U}(R) = \{1\}$ as well, R is a Boolean ring [1, page 5]. By Proposition 2.4, the prime ring of R can be identified with $\mathbb{Z}_2$. Since R is a finite-type algebra that is integral (that is, algebraic) and hence module-finite over its (finite) prime ring $\mathbb{Z}_2$, R is a finite (Boolean) ring. Therefore (cf. Corollary 2.5), R is isomorphic to a direct product of n copies of $\mathbb{Z}_2$ for some non-negative integer n. As R is an 2-generated ring, n cannot be 0, 1 or 2, since 0 and $\mathbb{Z}_2$ are each 0-generated and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is 1-generated. To obtain the desired contradiction, it suffices to show that $n \leq 4$. This inequality will be established in the next paragraph.

By the "2-generated" hypothesis, $R = \mathbb{Z}_2[a, b]$ for some $a, b \in R$. As R is a Boolean ring, $a^2 = a$ and $b^2 = b$. It is now easy to verify that the $\mathbb{Z}_2$-vector space

$$E := \mathbb{Z}_2 + \mathbb{Z}_2 a + \mathbb{Z}_2 b + \mathbb{Z}_2 ab$$

is closed under products. It follows that E is a ring, necessarily coinciding with R. As $|E| \leq 2^4$ and $|R| = 2^n$, we have $2^n \leq 2^4$, whence $n \leq 4$, as desired.

Finally, for the parenthetical assertion, it suffices to observe the following four facts: the coordinate ring example of Heinzer-Roitman [9, Example 2.3] that was discussed above is one-dimensional; the polynomial ring $\mathbb{Z}_2[X, Y]$ (whose only unit is 1, by Theorem 2.13) is two-dimensional; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is 2-generated (after all, it is generated by $\{(1, 0, 0), (0, 1, 0)\}$ and the only potential singleton generator, $(1, 1, 1)$, fails to generate $(1, 0, 0)$); and $\mathcal{E} := \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is 2-generated. This fourth fact can be verified as follows. Since $\mathcal{E}$ is neither 0-generated nor 1-generated and $\mathcal{E}$ is a $\mathbb{Z}_2$-vector space of cardinality 2^4 (as $\dim_{\mathbb{Z}_2}(\mathcal{E}) = 4$), one need only produce elements $a, b \in \mathcal{E}$ such that the $\mathbb{Z}_2$-span of $\{0, 1, a, b\}$ has cardinality exceeding 2^3. We leave to the reader the calculational verification that if one chooses $a := (1, 1, 0, 0)$ and $b := (1, 0, 1, 0)$, then the elements $0, 1, a, b, ab, 1 + a, 1 + b, 1 + ab$ and $a + b$ in $\mathcal{E}$ are pairwise distinct.

(f) Since Proposition 2.4 allows us to view R as a finite-type algebra over $\mathbb{Z}_2$, it follows that $\dim(R)$ coincides with the transcendence degree of (the quotient field of) R over $\mathbb{Z}_2$ (cf. [7, Theorem 31.16]). Also, by (e), $\dim(R)$ is either 1 or 2. Therefore, since the partners in an integral ring extension have the same Krull dimension (cf. [14, Theorem 44]), an application of a fundamental normalization theorem [16, Theorem 14.4] reduces our task to proving the following: if ($\dim(R) = 2$ and) R contains a pair X, Y of algebraically independent indeterminates over $\mathbb{Z}_2$ such that $\mathbb{Z}_2[X, Y] \subset R$ is an integral ring extension, then $R \cong \mathbb{Z}_2[X, Y]$.

Let K denote the quotient field of R. Now, since R is assumed to be 2-generated, $R = \mathbb{Z}_2[u, v]$ for some $u, v \in R$. It cannot be the case that both u and v are algebraic (that is, integral) over $\mathbb{Z}_2$ since R (being of Krull dimension 2) cannot be a field. By relabeling if necessary, we can assume, without loss of generality, that u is transcendental over $\mathbb{Z}_2$. It will suffice to show that u and v are algebraically independent over $\mathbb{Z}_2$ (for then $R = \mathbb{Z}_2[u, v] \cong \mathbb{Z}_2[X, Y]$, as desired). Note first that $v \notin \mathbb{Z}_2(u)$ (for, otherwise, $K = \mathbb{Z}_2(u, v) = \mathbb{Z}_2(u)$ and $2 = \dim(R) = \text{td}_{\mathbb{Z}_2}(K) = \text{td}_{\mathbb{Z}_2}(\mathbb{Z}_2(u)) = 1$, a contradiction). Therefore, by [11, Theorem 1.5, page 313], it is enough to prove that v is transcendental over $\mathbb{Z}_2(u)$. Suppose, on the contrary, that v is algebraic over $\mathbb{Z}_2(u)$. Then, since transcendence degree is additive in towers [11, Theorem 1.11, page 316], we get

$$2 = \dim(R) = \text{td}_{\mathbb{Z}_2}(K) = \text{td}_{\mathbb{Z}_2}(\mathbb{Z}_2(u)) + \text{td}_{\mathbb{Z}_2(u)}(K) = 1 + 0 = 1,$$

the desired contradiction, thus completing the proof.

□

Remark 2.22. (a) It may be helpful to reformulate part of Theorem 2.21 (c)-(f) in terms of dimension, as follows. Each 2-generated integral domain R such that $\text{U}(R) = \{1\}$ has dimension either 1 or 2. The only 2-generated two-dimensional integral domain R such that $\text{U}(R) = \{1\}$ is, up to isomorphism, the polynomial ring $\mathbb{Z}_2[X, Y]$. The 2-generated one-dimensional integral domains R such that $\text{U}(R) = \{1\}$ consist of certain rings of characteristic 2 (such as the ring in [9, Example 2.3]) for which there exists $X \in R$ which is transcendental over $\mathbb{Z}_2$ and $\mathbb{Z}_2[X] \subset R$ is an integral ring extension.

(b) It seems natural to ask what one can say about the last kind of integral domain mentioned in (a), namely, the 2-generated integral domains R such that $\text{U}(R) = \{1\}$ and there exists $X \in R$ which is transcendental over $\mathbb{Z}_2$ with $\mathbb{Z}_2[X] \subset R$ being an integral ring extension. (Necessarily, any such R is one-dimensional and of characteristic 2.) One obvious conclusion, thanks to the Krull-Akizuki Theorem, is that (even if “2-generated" is replaced by ‘finitely-generated" and one ignores the “$\text{U}(R) = \{1\}$" hypothesis) the integral closure of R (in its quotient field) is a Dedekind domain. Under certain conditions, one can conclude more. For instance, a result of Heinzer-Roitman [9, Theorem 3.4] implies that if such an R is a Euclidean domain, then $R \cong \mathbb{Z}_2[X]$. A relevant class of domains was given by Heinzer-Roitman [9, Theorem 2.1], a special case of which states the following: if $f(X, Y) = Y^2 + Y + p(X)$ where the polynomial $p(X) \in \mathbb{Z}_2[X]$ has odd degree, then $R := \mathbb{Z}_2[X, Y]/(f)$ is a Dedekind domain such that $\text{U}(R) = \{1\}$. This result was followed by Heinzer-Roitman [9, Theorem 2.2], giving a necessary and sufficient condition for an R that has been constructed in this manner to be a principal ideal domain. The above-mentioned example from [9, Example 2.3] is such a principal ideal domain which is a 2-generated ring, necessarily one-dimensional, and happens not to be a Euclidean domain. Question 2.23 will essentially ask for a characterization of the kinds of R satisfying $\mathrm{U}(R) = \{1\}$ that we have been discussing here in (b).

(c) If we take the coefficient ring to be $R := \mathbb{Z}_2 \times \mathbb{Z}_2$ and form the polynomial ring over it in infinitely many variables, Theorem 2.13 produces examples of commutative non-domain rings E such that $\mathrm{U}(E) = \{1\}$ and E is not finitely generated over R. The "smallest" such E is $R[X_1, X_2, \ldots, X_n, \ldots]$, which is isomorphic to

$$\mathbb{Z}_2[X_1, X_2, \ldots, X_n, \ldots] \times \mathbb{Z}_2[X_1, X_2, \ldots, X_n, \ldots].$$

One may be tempted to say that this E has "infinite transcendence degree over R." We will refrain from any such assertion because of the subtleties exposed by E. Hamann during 1986-1992 in a series of papers concerning various inequivalent notions of "finite transcendence degree" for algebras over commutative rings that are not integral domains. In any case, the above example E (and similar polynomial rings over R that are built by using uncountably infinite sets of indeterminates) should be contrasted with the examples of integral domains D in [9, Section 4] such that $\mathrm{U}(D) = \{1\}$ and D is of infinite transcendence degree over $\mathbb{Z}_2$. This completes the Remark.

Rather than asking the trite question of whether one can develop methods for arbitrary commutative rings that could produce results rivaling what was done for integral domains in Theorem 2.21, we will focus the next question on trying to further what was accomplished in Theorem 2.21.

Question 2.23. The approach in Theorem 2.21 to the problem of characterizing the integral domains R such that $\mathrm{U}(R) = \{1\}$ reduces to finding a tractable answer to the following question. If R is a (necessarily one-dimensional) 2-generated integral domain of characteristic 2 such that there exists an integral ring extension $\mathbb{Z}_2[X] \subset R$ (with X transcendental over $\mathbb{Z}_2$), can one find necessary and sufficient conditions on this integral ring extension so that $\mathrm{U}(R) = \{1\}$? (Note that [9, Example 2.3] shows that an integral domain R satisfying these conditions need not be isomorphic to the polynomial ring $\mathbb{Z}_2[X]$. Indeed, this example of Heinzer and Roitman shows that the integral extension mentioned in Theorem 2.21 (f) cannot be ignored in general.)

As a practical matter, "knowing" a ring R does not ensure that one "knows" the set of subrings of R. As a result, there are a number of attractive examples and attractive questions that do not fit into our subring-focused program that is based on Theorem 2.21. For instance, in [9, Section 4], Heinzer and Roitman construct a (necessarily infinitely generated) principal ideal domain R, with quotient field K, such that $\mathrm{U}(R) = \{1\}$ and $\mathrm{td}_{\mathbb{Z}_2}(K) = \infty$. We close by raising one of the "attractive questions" that were alluded to above.

Question 2.24. For some positive integer n, does there exist an n-generated two-dimensional integral domain R such that $\mathrm{U}(R) = \{1\}$ and R is not isomorphic to the polynomial ring $\mathbb{Z}_2[X, Y]$? (By parts (b), (c) and (f) of Theorem 2.21, an affirmative answer would have to feature $n \geq 3$.)

3 Appendix

Proposition 2.20 and Theorem 2.21 may lead one to ask if there are any connections between the "n-generated ring" and "minimal ring extension" concepts that are not cast in the "$\mathrm{U}(R) = 1$" setting. In that regard, Remark 3.1 (a) presents one such connection which, although quite easy, stimulates the examination in parts (b)-(g) of Remark 3.1 of the possible validity of a number of putative generalizations and analogues of the result in part (a).

Remark 3.1. (a) If $\Gamma \subset B$ is a minimal ring extension and Γ is a prime ring, then B is a 1-generated ring. To see this, pick $u \in B \setminus \Gamma$. Then the "minimal ring extension" hypothesis ensures that $B = \Gamma[u]$. As Γ is the prime ring of B and $B \neq 0$, the assertion follows.

(b) The "prime ring" hypothesis in (a) cannot be deleted. In fact, there exists a minimal ring extension $A \subset B$ such that B is not an n-generated ring for any non-negative integer n.

Moreover, there is such an example in which both A and B are fields. To see this, it suffices to take $A := \mathbb{Q}$ and $B := \mathbb{Q}(\sqrt{2})$. While $A \subset B$ is a minimal ring extension (since $\dim_A(B) = 2$), there do not exist $b_1, \ldots, b_n \in B$ such that $B = \mathbb{Z}[b_1, \ldots, b_n]$. Indeed, if such b_i existed, necessarily with $b_i = m_i + s_i\sqrt{2}$ for some rational numbers m_i and s_i, then

$$\mathbb{Q} = A \subseteq \mathbb{Z}[\{m_i + s_i\sqrt{2} \mid 1 \leq i \leq n\}] \cap \mathbb{Q},$$

whence $\mathbb{Q} = \mathbb{Z}[\{m_i, 2s_is_j \mid 1 \leq i, j \leq n\}]$ (by the irrationality of $\sqrt{2}$), which is a contradiction since $\mathbb{Q}$ is not a finite-type $\mathbb{Z}$-algebra.

(c) Despite (b), we do have the following result in positive characteristic. Let $k \subset B$ be finite fields, not necessarily with k a prime ring/field. (For instance, let k be a finite field and let $k \subset B$ be a minimal field extension.). Then B is a 1-generated ring. For a proof, recall that the multiplicative group of nonzero elements of B is cyclic (since B is a finite field), say generated as a group by some element $y \in B$. Thus $B = \mathbb{Z}_p[y]$ where $p :=$ char(B). As $\mathbb{Z}_p$ is the prime ring of B and $B \neq 0$, the assertion follows.

(d) The "1-generated ring" conclusion in (c) can fail in arbitrary positive (prime) characteristic p if the base field k is not assumed to be finite. Indeed, if X and Y are commuting algebraically independent indeterminates over $\mathbb{Z}_p$, then the field extension $A := \mathbb{Z}_p(X, Y^2) \subset B := \mathbb{Z}_p(X, Y)$ is a minimal ring extension (since $\dim_A(B) = 2$), but there does not exist $u \in B$ such that $B = \mathbb{Z}_p[u]$, for otherwise, consideration of transcendence degree would give $2 = \text{td}_{\mathbb{Z}_p}(B) = \text{td}_{\mathbb{Z}_p}(\mathbb{Z}_p[u]) \leq 1$, which is a contradiction.

(e) Returning to the context of characteristic 0, we next give a result that serves as a counterpoint to the assertion in (a). If A is an algebraic number field and $A \subset B$ is a minimal field extension (or, more generally, a finite-dimensional algebraic field extension), then B is 2-generated *as a* $\mathbb{Q}$*-algebra*. For a proof, one need only use the Primitive Element Theorem of classical field theory (for finite-dimensional field extensions of characteristic 0) to get $u \in A$ such that $A = \mathbb{Q}(u) = \mathbb{Q}[u[$ and $v \in B$ such that $B = A[v]$, as one then has $B = \mathbb{Q}[u, v]$.

(f) In closing, we show that the "algebraic number field" type of condition on the base fields in (a) and (e) cannot be deleted. In fact, if F is any countable field (of unspecified characteristic) and κ is any infinite cardinal number, then there exists a minimal field extension $A \subset B$ of fields containing F such that B cannot be generated as an F-algebra by a set of cardinality at most κ. To see this, note first that if a set S of cardinality at most κ generates a commutative F-algebra $\mathcal{E}$, it follows from the usual rules of arithmetic with infinite cardinal numbers (which hold because we are assuming the Zermelo-Fraenkel foundations of set theory and the Axiom of Choice) that

$$|\mathcal{E}| \leq \aleph_0 2^\kappa = \max(\aleph_0, 2^\kappa) = 2^\kappa < \gamma := 2^{(2^\kappa)}.$$

Then take $S = \{X_i\}$ to be a set of commuting algebraically independent indeterminates over F such that $|S| = \gamma$, pick $X_j \in S$, and put $A := F(\{X_i^2\})$ and $B := A(X_j)$. Note that $A \subset B$ is a minimal ring extension (since $\dim_A(B) = 2$). Moreover, B cannot be generated as an F-algebra by a set of cardinality at most κ, since $|B| = |A| \geq \gamma > 2^\kappa$.

References

[1] D. F. Anderson and A. Badawi, Von Neumann regular and related elements in commutative rings, *Algebra Colloq.* **19** (2012), Special Issue no. 1, 1017-1040.

[2] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, *Addison-Wesley, Reading (MA),* 1969.

[3] M. J. Chimes, Ultraproducts and Loś's Theorem: a Category-Theoretic Analysis, *M.S. dissertation, Stellenbosch Univ., Stellenbosch, South Africa,* 2017.

[4] D. E. Dobbs, The Ferrand-Olivier classification of the minimal ring extensions of a field: a proof and a survey of its influence, *JP J. Algebra, Number Theory Appl.* **40** (2018), no. 4, 605-662; dx.doi.org/10.17654/NT040040605.

[5] T. J. Dorsey and Z. Mesyan, On minimal extensions of rings, *Comm. Algebra* **37** (2009), 3463-3486.

[6] D. Ferrand and J.-P. Olivier, Homomorphismes minimaux d'anneaux, *J. Algebra* **16** (1970), 461–471.

[7] R. Gilmer, Multiplicative Ideal Theory, *Dekker, New York,* 1972.

[8] S. Glaz, Commutative Coherent Rings, *Lecture Notes in Math.* 1371, Springer-Verlag, Berlin, 1989.

[9] W. Heinzer and M. Roitman, Principal ideal domains and Euclidean domains having 1 as the only unit, *Comm. Algebra* **29** (2001), no. 11, 5197-5208.

[10] I. N. Herstein, Noncommutative Rings, *Carus Math. Monographs 15, Math. Assoc. America, distributed by Wiley, New York,* 1968.

[11] T. W. Hungerford, Algebra, *Graduate Texts in Math. 73, Springer-Verlag, New York/Heidelberg/Berlin,* 1974.

[12] N. Jacobson, Basic Algebra I, *W. H. Freeman and Co., San Francisco,* 1974.

[13] M. Kabbour and N. Mahdou, On valuation rings, *Comm. Algebra* **39** (2011), no. 1, 176–183.

[14] I. Kaplansky, Commutative Rings, *rev. ed., Univ. Chicago Press, Chicago,* 1974.

[15] J. Lambek, Lectures on Rings and Modules, *Blaisdell, Waltham (MA),* 1966.

[16] M. Nagata, Local Rings, *Wiley-Interscience, New York-London-Sydney,* 1962.

[17] B. Olberding, S. Saydam and J. Shapiro, Completions, valuations and ultrapowers of Noetherian domains, *J. Pure Appl. Algebra* 197 (2005), 213–237.

[18] B. Olberding and J. Shapiro, Prime ideals in ultraproducts of commutative rings, *J. Algebra* **285** (2005), no. 2, 768–794.

[19] R. Raphael, Some remarks on regular and strongly regular rings, *Canad. Math. Bull.* **17** (1974/75), no. 5, 709-712.

Author information

David E. Dobbs, Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1320, U. S. A..
E-mail: ddobbs1@utk.edu

Noômen Jarboui, Department of Mathematics and Statistics, King Faisal University, College of Science, P. O. Box 400, Al-Ahsa 31982, Saudi Arabia.
E-mail: njarboui@kfu.edu.sa

Received: November 11, 2019.
Accepted: March 15, 2020.