UNITAL RINGS WITH CARDINALITY RESTRICTIONS ON UNITAL SUBRINGS

GREG OMAN[†]

Abstract. It is well-known that an associative ring R (which may not be unital) is finite if and only if R has but finitely many subrings (again, not assumed to be unital even if R has an identity). A consequence of a theorem of Dobbs, Mullins, and Picavet L'Hermite is that a commutative unital ring R with but finitely many unital subrings is finite if and only if R has positive characteristic. In this note, we extend this result to noncommutative rings. We also extend a result of Laffey to determine the infinite unital rings with the property that every proper unital subring is finite. We conclude by discussing natural extensions of these results to uncountable rings.

Statements and Declarations

(1) The author has no competing interests to disclose.
(2) All data generated or analysed during this study are included in this published article.

1. Introduction

It is a textbook exercise to show that a group G is finite if and only if G has but finitely many subgroups. The ring-theoretic analog is true as well: an associative ring R is finite if and only if R has but finitely many subrings (which are not assumed to be unital even if R has an identity). This theorem appears to be originally due to Szele ([18]), but was also proven (independently) by Belkin ([1]) and Rosenfeld ([17]) in the case where R is unital. Bell gave a more elementary proof of this result in [2]. Then, in 1973, Robert Gilmer extended this theorem to rings not assumed to have an identity ([10]).[1]

In light of the above results, a natural question arises: is a unital ring with but finitely many unital subrings necessarily finite? It is immediate that the answer to this question is a resounding *no*, as the ring $\mathbb{Z}$ of integers witnesses. However, the commutative unital rings with but finitely many unital subrings were classified by Dobbs, Mullins, and Picavet L'Hermitte.

Fact 1 ([5])**.** A commutative unital ring R has but finitely many unital subrings if and only if R is finite or $R = \mathbb{Z}[t_1, \ldots, t_n]$, where each $t_i \in R$, and the rings $\mathbb{Z}[t_i]$ have but finitely many unital subrings.

2010 Mathematics Subject Classification Primary: 16P10, 16P20; Secondary: 13A70, 16N20, 16N40.

Key Words and Phrases. Artinian ring, division ring, transcendence base, Wedderburn-Artin theorem.

(†) *Department of Mathematics, University of Colorado, Colorado Springs, CO 80918, USA,* goman@uccs.edu.

[1] It appears that these authors were not aware of Szele's result from 1954, which establishes a bit more: every ring which satisfies ACC and DCC on subrings is finite.

As the authors had previously classified the singly generated unital rings (that is, rings generated by 1 and some other element) with only finitely many unital subrings in [6], this provides a complete description of the commutative unital rings with but finitely many unital subrings.

As mentioned above, a unital ring with but finitely many unital subrings need not be finite, in contrast to the non-unital situation. However, Fact 1 immediately yields a necessary and sufficient condition for a commutative unital ring with but finitely many unital subrings to be finite: R simply must have positive characteristic. We extend this result to noncommutative unital rings. In addition, we classify the infinite unital rings for which every proper unital subring is finite, extending a result of Laffey ([14]). We also consider some natural extensions of these results to uncountable rings, generalizing some other theorems in the literature. In addition to esstablishing some new results, one of our main objectives is to make stronger use of the cardinality assumptions in order to give more elegant proofs of some classical results in the literature.

2. Main Results

2.1. **Rings with but finitely many subrings.** As mentioned in the Introduction, it is a textbook exercise to prove that a group G is finite if and only if G has but finitely many subgroups. In fact, this claim holds when one replaces "group" with "semigroup", and the former result follows as a corollary from the latter.

Proposition 1. *Let S be a semigroup. Then S is finite if and only if S has but finitely many subsemigroups.*

Proof. It is patent that a finite semigroup has but finitely many subsemigroups. Conversely, assume that a semigroup S has but finitely many subsemigroups. We shall prove that S is finite. To wit, let $s \in S$ be arbitrary. Then the powers $s, s^2, s^3, \dots$ cannot all be distinct, lest $\langle s\rangle := \{s^n \colon n \in \mathbb{Z}^+\} \cong (\mathbb{Z}^+, +)$, which clearly has infinitely many subsemigroups, a contradiction. Hence for every $s \in S$, there are integers $0 < m < n$ such that $s^n = s^m$, from which it follows that $\langle s\rangle$ is finite. As $S = \bigcup_{s\in S}\langle s\rangle$, S is a finite union (since S has but finitely many subsemigroups) of finite subsemigroups, S is finite. □

Corollary 1. *Let G be a group. Then G is finite if and only if G has but finitely many subgroups.*

Proof. Let G be a group with but finitely many subgroups. Since $(\mathbb{Z}, +)$ has infinitely many subgroups, G cannot contain an element of infinite order. Hence every subsemigroup of G is a subgroup of G, and the result follows from the previous proposition. □

We now transition to rings. Perhaps not surprisingly, the fact that a ring R is finite if and only if R has but finitely many subrings is a bit more difficult to prove. We provide a short, elementary proof. We first establish two lemmas which will be useful throughout this note.

Lemma 1. *Let D be a division ring. If D has but finitely many unital subrings, then D is finite. Thus if D has but finitely many subrings, D is also finite.*

Proof. Let D be a division ring with but finitely many unital subrings. Observe that for primes $q_1 \neq q_2$, the rings $\mathbb{Z}[\frac{1}{q_1}]$ and $\mathbb{Z}[\frac{1}{q_2}]$ are distinct unital subrings of $\mathbb{Q}$, and so it follows that D has prime characteristic p. We claim that D is algebraic over its prime subfield $\mathbb{F}_p$. If not, then up to isomorphism, the polynomial ring $\mathbb{F}_p[X]$ in the variable X is a unital subring of D. For every positive integer n, let R_n be the subring of $\mathbb{F}_p[X]$ generated by 1_D and X^n. It is clear that $R_n \neq R_m$ for $m \neq n$, and this is a contradiction to the fact that D has but finitely many unital subrings. It follows that for every $\alpha \in D$, $\mathbb{F}_p[\alpha]$ is a finite field. Now by Lagrange, for every $\alpha \in D$, there is $n(\alpha) > 1$ such that $\alpha^{n(\alpha)} = \alpha$. The commutativity of D now follows by Jacobson's Theorem. Suppose by way of contradiction that D is infinite. Choose $\alpha_1 \in D$. Then $\mathbb{F}_p(\alpha_1)$ is finite, so there is $\alpha_2 \in D \backslash \mathbb{F}_p(\alpha_1)$. Also $\mathbb{F}_p(\alpha_1, \alpha_2)$ is finite, so there is $\alpha_3 \in D \backslash \mathbb{F}_p(\alpha_1, \alpha_2)$. Continuing recursively, we obtain a strictly increasing tower of subfields, and this is a contradiction to the assumption that D has but finitely many unital subrings. □

Lemma 2. *Let R be a ring and I be an infinite two-sided ideal of R. Suppose that every proper one-sided ideal of R contained in I has smaller cardinality than I. Then the following hold:*

(1) *If R has an identity, then $\operatorname{Ann}(I_R) := \{r \in R \colon Ir = \{0\}\}$ is a prime ideal of R.*
(2) *Either I is a division ring or $xy = 0$ for all $x, y \in I$.*
(3) *If $xy = 0$ for all $x, y \in R$, then as rings, $I \cong C(p^\infty)(0)$ for some prime number p (the ring with additive group the quasi-cyclic group $C(p^\infty)$ and with zero multiplication).*

Proof. Let R be a ring with an infinite ideal I such that every proper one-sided ideal of R contained in I has smaller cardinality than I. Let $r \in R$ be arbitrary, and consider the function $\varphi \colon I \to Ir$ defined by $\varphi(x) := xr$. Then φ is easily seen to be a surjective homomorphism of left R-modules; let K be the kernel of this map. Then $I/K \cong Ir$, and we deduce that $|I| = |Ir||K|$. As I is infinite, elementary cardinal arithmetic yields that either $|Ir| = |I|$ or $|K| = |I|$. The condition on I implies $Ir = I$ or $K = I$. So we have shown that

$$Ir = I \text{ or } Ir = \{0\} \text{ for every } r \in R\text{; symmetrically,} \tag{2.1}$$

$$rI = I \text{ or } rI = \{0\} \text{ for every } r \in R. \tag{2.2}$$

Our next claim is that

$$\text{for all } x \in I,\ Ix = \{0\} \text{ if and only if } xI = \{0\}. \tag{2.3}$$

To see this, let $x \in I$ be arbitrary, and assume that $Ix = \{0\}$. Suppose by way of contradiction that $xI \neq \{0\}$. By (2.2), $xI = I$. But then $x^2 I = xI = I$ as well, and we deduce that $x^2 \neq 0$. But $Ix = \{0\}$ implies that $x^2 = 0$, a contradiction. Thus $xI = \{0\}$. Similarly, if $xI = \{0\}$, then $Ix = \{0\}$, and (2.3) is verified.

(1) Suppose that R has an identity. Then $\operatorname{Ann}(I_R) \neq R$. Suppose $x, y \in R \backslash \operatorname{Ann}(I_R)$. Then by (2.1), we see that $Ix = I = Iy$. Thus $Ixy = Iy = I$, and $xy \notin \operatorname{Ann}(I_R)$. This proves (1).

(2) Next, suppose there exist $x, y \in I$ such that $xy \neq 0$. We will show that I is a division ring. First, we establish that $\operatorname{Ann}(I_I) := \{x \in I \colon Ix = \{0\}\} = \{0\}$. Let $b \in I$ and suppose that

$Ib = \{0\}$; we will show that $b = 0$.. Since $xy \neq 0$, we deduce from (2.1) that $Iy = I$. Thus $b = ay$ for some $a \in I$. If $aI = \{0\}$, then $b = 0$ and we are done. Now suppose that $aI \neq \{0\}$. By (2.1) and (2.3), $Ia = I$. Thus $Ib = Iay = Iy = I$, contradicting that $Ib = \{0\}$. We have proven that $\text{Ann}(I_I) := \{i \in I \colon Ii = \{0\}\} = \{0\}$, and so from (2.1)–(2.3), we deduce that $Ii = iI = I$ for every nonzero $i \in I$. It now follows that I is a division ring, and (2) is verified.

(3) Finally, suppose that $xy = 0$ for all $x, y \in R$. Then every additive subgroup of I is an ideal of R contained in I, so by the condition on I, every proper additive subgroup of I has smaller cardinality than I. It is well-known that the only infinite abelian groups with this property are the quasi-cyclic groups (see [7] for more details), and thus $I \cong C(p^\infty)(0)$ for some prime p in this case. □

We are now equipped to give an elementary proof of the fact that a ring with but finitely many subrings is finite.

Theorem 1 ([1], [2], [10], [17])**.** *A ring with but finitely many subrings is finite.*

Proof. We proceed by strong induction. Let n be a positive integer, and suppose that for every positive integer $m < n$, any ring with exactly m subrings is finite. Now let R be a ring with n subrings (we include the trivial subring and R in this collection). Suppose by way of contradiction that R is infinite. Then if S is a proper subring of R, then S has fewer subrings than R does (since every subring of S is a subring of R but R is not a subring of S). We deduce from the inductive hypothesis that S is finite. It follows that every proper one-sided ideal of R is finite, so by Lemma 2, either $R \cong C(p^\infty)(0)$ for some prime p or R is a division ring. The former is impossible as $C(p^\infty)$ has infinitely many subgroups, whence $C(p^\infty)(0)$ has infinitely many subrings, and the latter is precluded by Lemma 1. The proof is complete. □

2.2. **Unital rings with but finitely many unital subrings.** Next, we extend Theorem 1 to unital rings and unital subrings. As noted previously, $\mathbb{Z}$ is a unital ring with but one unital subring yet is infinite. So we must change the statement to be proved in the unital case. Note trivially that a necessary condition for a ring to be finite is that it have positive characteristic. We will show that this condition is also sufficient in order for a unital ring with only finitely many unital subrings to be finite. Again, we require two preliminary lemmas.

Our next lemma is a generalization of one of the main results of [8] (Corollary 2), where the authors use the theory of Jónsson ω-generated modules to show that if T is a commutative unital ring which admits a proper unital subring, and if every proper unital subring of T is Artinian, then T is Artinian. We present a generalization of this result to noncommutative rings using only basic principles.

Lemma 3. *Let T be a unital ring with a proper unital subring. Suppose that every proper unital subring of T is left* (*right*) *Artinian. Then T is left* (*right*) *Artinian.*

Proof. Let T be as stated, and suppose by way of contradiction that T is not left Artinian. Then there exists an infinite strictly decreasing sequence

$$\cdots \subsetneq I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1 \tag{2.4}$$

of left ideals of T. Now, since T admits a proper unital subring, we see that $P(R)$, the prime subring of R generated by 1, must be proper, and thus left Artinian. As $\mathbb{Z}$ is not Artinain, it follows that

$$P(R) \text{ is a finite ring, say of cardinality } n. \tag{2.5}$$

For every positive integer k, let $R_k := I_k + P(R)$. It is easy to see that each R_k is a unital subring of T. Moreover, for every $k \in \mathbb{Z}^+$, $\cdots \subsetneq I_{k+2} \subsetneq I_{k+1} \subsetneq I_k$ is an infinite, strictly decreasing sequence of left ideals of R_k. Because every proper unital subring of T is left Artinian, we deduce that

$$R_k = T \text{ for every positive integer } k. \tag{2.6}$$

Next, observe from the fundamental theorem on modules homomorphisms that

$$(T/I_{k+1})/(I_k/I_{k+1}) \cong T/I_k, \tag{2.7}$$

and thus $|T/I_{k+1}| = |T/I_k| \cdot |I_k/I_{k+1}| \geq 2|T/I_k|$. It follows that

$$\text{there is no finite upper bound on the sizes of } T/I_k, \text{ where } k \text{ ranges over } \mathbb{Z}^+. \tag{2.8}$$

Next, let $k \in \mathbb{Z}^+$. Recall from (2.5) that $|P(R)| = n$. Thus, trivially,

$$|\{I_k + r \colon r \in P(R)\}| \leq n. \tag{2.9}$$

Finally, recall from (2.6) that $R_k = T$. Hence $T/I_k = R_k/I_k = (I_k + P(R))/I_k = P(R)/I_k$, and thus $|T/I_k| = |P(R)/I_k| \leq n$ (from (2.9) above). This contradicts (2.8). By considering the opposite ring R^{op}, one obtains the symmetric result for the right Artinian condition, and the proof is complete. □

The previous lemma yields a nice corollary.

Corollary 2. *Let R be a unital ring of positive characteristic with but finitely many unital subrings. Then R is* (*left and right*) *Artinian.*

Proof. Again, we proceed by strong induction. Let n be a positive integer and suppose that any unital ring of positive characteristic with fewer than n unital subrings is Artinian. Now let R be a unital ring of positive characteristic with n unital subrings. If R has no proper, unital subrings, then $R \cong \mathbb{Z}/\langle n \rangle$ for some positive integer n and so is clearly Artinian. Now suppose that R has a proper, unital subring, and let S be such a subring. Then S has fewer than n unital subrings and hence is Artinian by the inductive hypothesis. Invoking Lemma 3, R is Artinian, and the proof is complete. □

We need one final lemma, and then we establish the main result of this subsection. Our proof will make use of standard results on Artinian rings without explicit references to the literature; we refer the reader to Lam's text [15] for details.

Lemma 4 ([16], Corollary 4)**.** *Let R be an infinite unital ring which satisfies the ascending chain condition on two-sided ideals. There exists a prime ideal P of R such that $|R/P| = |R|$.*

Theorem 2. *Let R be a unital ring with but finitely many unital subrings. The following are equivalent.*

(1) *R is finite.*
(2) *R has positive characteristic.*
(3) *R is Artinian.*

Proof. Let R be a unital ring with only finitely many unital subrings.

(1)⇒(2): trivial.

(2)⇒(3): immediate from Corollary 2.

(3)⇒(1): assume that R is Artinian, and let P be an arbitrary prime ideal of R. Then P is also a maximal ideal, and hence R/P is a simple Artinian ring. By the Wedderburn-Artin Theorem, $R/P \cong M_n(D)$ for some division ring D and positive integer n. Because R has but finitely many unital subrings, the same is true of R/P; therefore, $M_n(D)$ has but finitely many unital subrings. One checks easily that if R is a unital subring of D, then $M_n(R)$ is a unital subring of $M_n(D)$. It follows that D has but finitely many unital subrings, hence is finite by Lemma 1. We deduce that $M_n(D)$, and thus R/P, is finite. As R is Artinian, R is also Noetherian and thus satisfies ACC on two-sided ideals. Since R/P is finite for every prime ideal P, Lemma 4 implies that R is finite, and the proof is complete. □

In [13], Laffey proved that if a ring S (not assumed to be commutative or unital) has a maximal, finite subring R, then S itself is finite. This extends Theorem 8 of [3], where the authors prove the result for commutative such S. We close this subsection by establishing the commutative result for unital rings and subrings.

Corollary 3. *Let S be a commutative unital ring with a finite, unital maximal subring R (meaning R is a proper unital subring of S and there is no unital subring of S properly between R and S). Then S is finite.*

Proof. Suppose that S and R are as stated, and assume by way of contradiction that S is infinite. We claim that S is Artinian. Suppose that $\cdots \subsetneq I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1$ is a strictly decreasing chain of ideals of S. Because R is finite, there is $k \in \mathbb{Z}^+$ such that $I_n \nsubseteq R$ for all $n \geq k$. So without loss of generality, we may assume that $I_n \nsubseteq R$ for all positive integers n. By maximality of R, it follows that $I_n + R = S$ for all n, and we obtain the same contradiction we obtained in the proof of Lemma 3. Thus S is Artinian and hence Noetherian. Applying Lemma 4, there is a prime ideal P of S such that $|S/P| = |S|$. But P is also maximal in S; furthermore, $P \cap R$ is maximal in R, as R is finite. We deduce that the field $F := R/(P \cap R)$ is a maximal unital subring of the field $K := S/P$. It follows immediately by maximality that K is algebraic over F and for any $\alpha \in K \backslash F$, we see that $F \subsetneq F(\alpha) \subsetneq K$, a contradiction. □

2.3. **A classification of the infinite unital rings for which every proper unital subring has smaller cardinality.** In [14], Laffey classified the infinite rings for which every proper subring is finite. We pause to recall his classification.

Lemma 5 ([14], Theorem 1)**.** *Let R be an infinite ring. Then every proper subring of R is finite if and only if one of the following holds.*

(1) *R is isomorphic to $C(p^\infty)(0)$ for some prime p, or*
(2) *R is isomorphic to $\bigcup_{n\in\mathbb{Z}^+}\mathbb{F}_{p^{q^n}}$ for some primes p and q (where $\mathbb{F}_m$ denotes the field with m elements).*

We now extend Laffey's result to characterize the infinite unital rings for which every proper unital subring has smaller cardinality than the ambient ring.

Theorem 3. *Let R be an infinite unital ring. Then every proper unital subring of R has smaller cardinality than R if and only if one of the following holds.*

(1) *$R \cong \mathbb{Z}$,*
(2) *$R \cong (\bigcup_{n\in\mathbb{Z}^+}\mathbb{F}_{p^{q^n}}) \times \mathbb{Z}/m\mathbb{Z}$ for some integer $m > 0$ and some primes p and q, or*
(3) *$R \cong D \times \mathbb{Z}/m\mathbb{Z}$ for some integer $m \geq 0$ and uncountable, noncommutative division ring for which every proper unital subring of D has smaller cardinality than D.*

Proof. We first verify that the rings in (1)–(3) above have the desired property. As $\mathbb{Z}$ has no proper unital subrings, every proper unital subring of $\mathbb{Z}$ is of smaller cardinality vacuously. As for the rings in (2) and (3), we can take care of both simultaneously. Consider a ring $R := D \times \mathbb{Z}/m\mathbb{Z}$ where D is an infinite division ring, and every proper unital subring of D has smaller cardinality than D. Assume also that if D is countable, then $m > 0$ and if D is uncountable, then $m \geq 0$. Let S be a unital subring of R of the same cardinality as R. It suffices to show that $S = R$. Letting $\pi_1(S)$ be the projection function onto the first coordinate, it is clear that $\pi_1(S)$ is a unital subring of D. If $\pi_1(S) \neq D$, then $\pi_1(S)$ has smaller cardinality than D. But thn S has smaller cardinality than R, a contradiction. So we have shown that

$$\pi_1(S) = D. \tag{2.10}$$

Now choose $\alpha \in D\backslash P(D)$. Then $\alpha \in \pi_1(S)$, and thus there is $k \in \mathbb{Z}$ such that $(\alpha, k) \in S$ (and k is taken modulo m). Because S is unital, $(k, k) \in S$. Subtracting, $(\alpha - k, 0) \in S$. As $\alpha \notin P(D)$, $\alpha - k \neq 0$, and is thus invertible in D. Also, $((\alpha - k)^{-1}, l) \in S$ for some integer l by (2.10). Multiplying, we get $(1, 0) \in S$. We deduce from (2.10) that $D \times \{0\} \subseteq S$. Now, also $(1, 1) \in S$ as S is unital, and so $(0, 1) \in S$. This proves that $\{0\} \times \mathbb{Z}/m\mathbb{Z} \subseteq S$, and we deduce that $S = R$.

Conversely, suppose that R is an infinite unital ring and that all proper unital subrings of R are of smaller cardinality. First, we verify that

(2.11) if R is commutative and $|R| > \omega$, then for all primes P of R, $|R/P| < |R|$; thus $|P| = |R|$.

Indeed, if there is a prime ideal P of R for which $|R/P| = |R|$, then $R/P := D$ is an uncountable integral domain. So we may choose a subset $\beta \subseteq D$ which is maximal with respect to being algebraically independent over the prime subring $P(D)$. Since $P(D)$ is countable but D is uncountable, it follows that $|\beta| = |D|$. Now choose any $b \in \beta$. Then $P(D)[\beta \backslash \{b\}]$ is a proper unital subring of D of the same cardinality as D. Pulling back to R, we obtain a proper unital subring of R of the same cardinality as R, a contradiction. Since $|R| = |R/P||P|$ and $|R/P| < |R|$, basic cardinal arithmetic yields that $|P| = |R|$.

If $R \cong \mathbb{Z}$, then R belongs to group (1) and we are done. Thus we assume that

$$R \ncong \mathbb{Z}. \tag{2.12}$$

We claim that

$$\text{every one-sided ideal of } R \text{ of the same cardinality as } R \text{ is two-sided.} \tag{2.13}$$

Indeed, suppose that I is a left ideal of R with $|I| = |R|$. Then $I + P(R)$ is a unital subring of R of the same size as R, so coincides with R. Now let $i \in I$ and $r \in R$. Then $r = i_0 + m$ for some $i_0 \in I$ and integer m. Hence $ir = ii_0 + im \in I$, and I is two-sided. Analogously, every right ideal of R of the same cardinality as R is two-sided.

Next, we show that

(2.14) There is an ideal I of R cardinality $|R|$ such that $|J| < |I|$ for every one-sided ideal $J \subsetneq I$.

We consider two cases.

Case 1: R has positive characteristic. Suppose that there is a chain $\cdots \subsetneq I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1$ of ideals of R, each of size $|R|$. Then for each k, we see that $I_k + P(R) = R$. It follows that $|R/I_k| \leq |P(R)|$ for every k, and we obtain a contradiction as in the proof of Lemma 3. It follows from this that there is an ideal I of R which is minimal with respect to having cardinality $|R|$. Suppose that $J \subsetneq I$ is a one-sided ideal of R. If $|J| = |I| = |R|$, then from (2.13), J is two-sided, and this contradicts the minimality of I.

Case 2: R has characteristic 0. We identity the prime subring of R with $\mathbb{Z}$. Since $\mathbb{Z}$ is a unital subring of R and since $R \ncong \mathbb{Z}$, it follows that R is uncountable. Let I_1 be an ideal of R of size $|R|$. If I_1 is minimal in this respect, then since every one-sided ideal of size R is two-sided, we see that for every one-sided ideal J of R such that $J \subsetneq I_1$, we have $|J| < |I|$.Otherwise, there is an ideal I_2 of R of size $|R|$ for which $I_2 \subsetneq I_1$. If I_2 is minimal with respect to having size $|R|$, then we are done as above. Hence we may assume that

$$\cdots \subsetneq I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1 \text{ is a chain of ideals of } R \text{ each of size } |R|. \tag{2.15}$$

Next, we establish that

(2.16) there is a prime ideal P of R such that $|P| = |R|$ and $P \cap \mathbb{Z} = \{0\}$.

Suppose first that R is commutative. Noting that the set of nonzero integers is a multiplicatively closed subset of R, there is a prime ideal P of R such that $P \cap \mathbb{Z} = \{0\}$. From (2.11), we see that $|P| = |R|$, establishing (2.16) in case R is commutative. Now let us drop the assumption that R is commutative. We consider two cases.

Case 2A: $|I_1 \cap I_2 \cap \cdots| < |R|$. For every positive integer n, we see that $I_n + \mathbb{Z} = R$, and so $R/I_n \cong \mathbb{Z}/I_n$ is a commutative unital ring. Since $S := R/(I_1 \cap I_2 \cdots)$ embeds into $R/I_1 \times R/I_2 \times \cdots$, it follows that S is commutative. Because $|I_1 \cap I_2 \cap \cdots| < |R|$, we see that $|S| = |R|$, and it follows that every proper unital subring of S has smaller cardinality than S. As the I_n strictly descend, there is no finite bound on the size of the residues R/I_n. Recalling above that $R/I_n \cong \mathbb{Z}/I_n$, we deduce that for every positive integer n, we have $n \notin I_1 \cap I_2 \cap \cdots$.This shows that S has characteristic 0. From what we just proved above, there is a prime ideal P' of S such that $|P'| = |S|$ and $P' \cap \mathbb{Z} = \{0\}$. Note that $P' = P/(I_1 \cap I_2 \cap \cdots)$ for some prime ideal P of R containing $I_1 \cap I_2 \cap \cdots$. It is easy to see that $|P| = |R|$ and $P \cap \mathbb{Z} = \{0\}$.

Case 2B: $I := \bigcap_{n \in \mathbb{Z}^+} I_n$ satisfies $|I| = |R|$. Then $I + \mathbb{Z} = R$. Clearly R/I is infinite, since the I_k properly descend, and so we have $I \cap \mathbb{Z} = \{0\}$, implying that $R/I \cong \mathbb{Z}$. Hence I is prime, and we have verified (2.16).

Suppose that $I_1 \subsetneq I_2 \subsetneq I_3$ are ideals of R of cardinality $|R|$ that intersect $\mathbb{Z}$ trivially. Then as noted above, $R/I_1 \cong R/I_2 \cong R/I_3 \cong \mathbb{Z}$, hence each I_k is prime. But then I_3/I_1 is a prime ideal of $R/I_1 \cong \mathbb{Z}$ of height at least two, which is absurd. It follows that we may choose an ideal I of R which is minimal with respect to having cardinality $|R|$ and intersecting $\mathbb{Z}$ trivially. Suppose that J is a one-sided ideal properly contained in I. We claim that $|J| < |I|$. For suppose that $|J| = |I|$. Then J is two-sided (2.13), and so by minimality of I, J intersects $\mathbb{Z}$ nontrivially. Because $J + \mathbb{Z} = R$, R/J is finite. But $(R/J)/(I/J) \cong R/I \cong \mathbb{Z}$ is infinite, which is absurd. This establishes (2.14).

Let I be an ideal furnished by (2.14). By Lemma 2(1),

(2.17) $\mathrm{Ann}(I_R)$ is a prime ideal of R.

We claim that

(2.18) $|\mathrm{Ann}(I_R)| < |R|$; thus $|R/\mathrm{Ann}(I_R)| = |R|$.

Note that I is naturally a right $R/\mathrm{Ann}(I_R)$-module. Moreover,

(2.19) the set of right ideals of R contained in I is the set of $R/\mathrm{Ann}(I_R)$-submodules of I.

Suppose by way of contradiction that $\mathrm{Ann}(I_R)$ has the same cardinality as R. Then $\mathrm{Ann}(I_R) + P(R) = R$. As $\mathrm{Ann}(I_R)$ is a prime ideal of R, either $R/\mathrm{Ann}(I_R)$ is a finite field, or $R/\mathrm{Ann}(I_R) \cong \mathbb{Z}$.

In the former case, we obtain a proper subspace of I as an $R/\mathrm{Ann}(I_R)$-vector space of size $|I|$ by taking the span of a basis minus one element, contradicting (2.14) and (2.19). In the latter case, R has characteristic 0. Because we have assumed $R \not\cong \mathbb{Z}$, we deduce that R, and hence I, is uncountable. Since $R/\mathrm{Ann}(I_R) \cong \mathbb{Z}$, every additive subgroup of I is a right ideal of R contained in I, and so every proper additive subgroup of I has smaller cardinality than I. But then $(I,+) \cong C(p^\infty)$, contradicting that I is uncountable. This proves (2.18).

Our next claim is that

$$\text{there exist } x, y \in I \text{ such that } xy \neq 0. \tag{2.20}$$

If not, then $I \subseteq \mathrm{Ann}(I_R)$, which is impossible since $|I| = |R|$ but $|\mathrm{Ann}(I_R)| < |R|$. We deduce from Lemma 2(2) that I is a division ring. It follows from this fact that

$$I \text{ is a simple left (right) } R\text{-module, and } R/\mathrm{Ann}(I_R) \text{ is a division ring.} \tag{2.21}$$

Finally, we complete the argument. We consider two cases.

Case 1: $\mathrm{Ann}(I_R) = \{0\}$. Then R is a division ring. Let's suppose first that R is countable. Then R is an infinite division ring with the property that every proper unital subring is finite. Let $\alpha \in R\backslash\{0\}$. If α is transcendental over $P(R)$, then up to isomorphism, $P(R)[\alpha] \cong P(R)[X]$ is a proper, infinite unital subring of R, a contradiction. Thus α is algebraic over $P(R)$ and so $P(R)[\alpha]$ is a finite field. We conclude that there is a positive integer n such that $\alpha^n = 1$. It follows that every nonzero subring of R is unital, and thus every proper subring of R is finite. Invoking Lemma 5, we see that $R \cong \bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}}$ for some prime q, and so R belongs to family (2). Now suppose that R is uncountable. Then (2.11), (2.17), and (2.18) imply that R is noncommutative, and hence belongs to family (3).

Case 2: $\mathrm{Ann}(I_R)$ is nonzero. If $I \cap \mathrm{Ann}(I_R) \neq \{0\}$, then the simplicity of I implies that $I \subseteq I \cap \mathrm{Ann}(I_R) \subseteq \mathrm{Ann}(I_R)$, which is impossible since $|\mathrm{Ann}(I_R)| < |I|$. Thus $I \cap \mathrm{Ann}(I_R) = \{0\}$. Since $\mathrm{Ann}(I_R)$ is a maximal (two-sided) ideal and I is a nonzero (two-sided) ideal which intersects $\mathrm{Ann}(I_R)$ trivially, $\mathrm{Ann}(I_R) + I = R$. Applying the Chinese remainder theorem, $R \cong R/\mathrm{Ann}(I_R) \times R/I$. Now, $R/\mathrm{Ann}(I_R)$ inherits the property that all proper unital subrings are of smaller cardinality, and so as above, either $R/\mathrm{Ann}(I_R)$ is an uncountable noncommutative division ring, or $R/\mathrm{Ann}(I_R) \cong \bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}}$ for some primes p and q. It remains only to show that $R/I \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \geq 0$. Toward this end, as $|I| = |R|$, we have $I + P(R) = R$, whence $R/I \cong P(R)/I$ and the result follows. □

Remark 1. It is not known if there exists an uncountable division ring with all proper subrings of smaller cardinality (see [12], [4]), and so at present, our classification above appears to be best possible.

We immediately obtain the following corollary due to Robert Gilmer and Bill Heinzer.

Corollary 4 ([9], Theorem 1.2)**.** *Let R be an uncountable unital commutative ring. Then R possesses a proper unital subring of the same cardinality as R.*

Now, if R is an uncountable unital ring, then it is easy to construct a strictly increasing chain of countable unital subrings. Thus any unital ring satisfying ACC on unital subrings is countable. It is not so obvious that if R satisfiess DCC on unital subrings, then R must be countable. But we obtain this as a simple corollary of the previous theorem.

Corollary 5. *Let R be a unital ring which satisfies DCC on unital subrings. Then R is countable.*

Proof. Suppose by way of contradiction that there exists an uncountable unital ring R which satisfies DCC on unital subrings. Pick a unital subring S of R which is minimal with respect to $|S| = |R|$. Then by Theorem 3, there is an uncountable division ring D which is a homomorphic image of S, thus also satisfies DCC on unital subrings. If D has characteristic 0, then $\mathbb{Q}$ is (up to isomorphism) a unital subring of D, but $\mathbb{Q}$ does not satisfy DCC on unital subrings. Thus $\mathbb{F}_p$ is the prime subring of D for some prime p. D is not algebraic over $\mathbb{F}_p$, lest D be countable. So $\mathbb{F}_p[X]$ is a unital subring of D up to isomorphism. However, if we let S_n be the subring of $\mathbb{F}_p[X]$ generated by 1 and X^{2^n}, then $\{S_n \colon n \in \mathbb{Z}^+\}$ is a strictly decreasing chain of unital subrings of D, a contradiction. □

We close the paper by generalizing Szele's result that a ring satisying ACC and DCC on subrings is finite ([18]), while also generalizing Theorem 2.

Corollary 6. *Let R be a unital ring which satisfies ACC and DCC on unital subrings. Then the following are equivalent.*

(1) *R is finite.*
(2) *R has positive characteristic.*
(3) *R is Artinian.*

Proof. Let R be unital and satisfy ACC and DCC on unital subrings.

(1)⇒(2): trivial.

(2)⇒(3): assume that R has positive characteristic. It suffices to show that R is finite. Suppose that R is infinite, and pick a unital subring S of R which is minimal with respect to being infinite. Clearly S inherits ACC and DCC on subrings. Theorem 3 shows that S is isomorphic to either $\bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}}$ or to $\bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}} \times \mathbb{Z}/m\mathbb{Z}$ for some primes p and q and positive integer m. But neither of these rings has ACC on unital subrings, a contradiction.

(3)⇒(1): assume that R is Artinian. It suffices by Lemma 4 to show that R/P is finite for every prime ideal P of R. Thus let P be a prime ideal of R. Then $R/P \cong M_n(D)$ for some division ring D and positive integer n. ACC and DCC on unital subrings clearly pass to R/P and then also to D. We claim that D has prime characteristic. This follows from the fact that $\mathbb{Z}[\frac{1}{p_1}] \subseteq \mathbb{Z}[\frac{1}{p_1p_2}] \subseteq \cdots$ is a strictly increasing chain of unital subrings of $\mathbb{Q}$, where $p_1, p_2, \ldots$ is an enumeration of the primes. It now suffices to prove that D is finite. Suppose not, and let S be a minimally infinite, unital subring of D. Again, S inherits ACC and DCC on unital subrings. As D has positive characteristic, so does S. As in the proof of the previous implication, S is isomorphic to either $\bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}}$ or to $\bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{q^n}} \times \mathbb{Z}/m\mathbb{Z}$ for some primes p and q and positive integer m. But neither of these rings has ACC on unital subrings, a contradiction. The proof is now complete. □

References

[1] V.P. Belkin, *Semigroups with additive endomorphisms*, Algebra i Logika Sem. **6** (1967), no. 1, 9–14.

[2] H.E. Bell, *Rings with finitely many subrings*, Math. Ann. **182** (1969), 314–318.

[3] H.E. Bell, F. Guerriero, *Some conditions for finiteness and commutativity of rings*, Internat. J. Math. Math. Sci. **13** (1990), no. 3, 535–544.

[4] E. Coleman, *Jónsson groups, rings and algebras*, Irish Math. Soc. Bull. **36** (1996), 34–45.

[5] D.E. Dobbs, B. Mullins, M. Picavet L'Hermitte, *A characterization of the commutative unital rings with only finitely many unital subrings*, J. Algebra Appl. **7** (2008), no. 5, 601–622.

[6] D.E. Dobbs, B. Mullins, M. Picavet L'Hermitte, *The singly generated unital rings with only finitely many unital subrings*, Comm. Algebra **36** (2008), no. 7, 2638–2653.

[7] L. Fuchs, *Abelian groups.* Publishing House of the Hungarian Academy of Sciences, Budapest 1958.

[8] R. Gilmer, W. Heinzer, *An application of Jónsson modules to some questions concerning proper subrings*, Math. Scand. **70** (1992), no. 1, 34–42.

[9] R. Gilmer, W. Heinzer, *On the cardinality of subrings of a commutative ring*, Canad. Math. Bull. **29** (1986), no. 1, 102–108.

[10] R. Gilmer, *A note on rings with only finitely many subrings*, Scripta Math. **29** (1973), 37–38.

[11] I.N. Herstein, *Topics in algebra. Second edition.* Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.

[12] A. Kostinsky, *Some problems for rings and lattices within the domain of general algebra.* Thesis (Ph.D.), University of California, Berkeley, 1969.

[13] T. Laffey, *A finiteness theorem for rings*, Proc. Roy. Irish Acad. Sect. A **92** (1992), no. 2, 285–288.

[14] T. Laffey, *Infinite rings with all proper subrings finite*, Amer. Math. Monthly **81** (1974), 270–272.

[15] T.Y. Lam, *A first course in noncommutative rings. Second edition.* Graduate Texts in Mathematics, 131. Springer-Verlag, New York, 2001.

[16] G. Oman *Small and large ideals of an associative ring*, J. Algebra Appl. **13** (2014), no. 5, 1350151, 20 pp.

[17] A. Rosenfeld, *A note on two special types of rings*, Scripta Math. **28** (1967), 51–54.

[18] T. Szele, *On a finiteness criterion for modules*, Publ. Math. Debrecen 3 (1954), 253–256 (1955).