Commun. Korean Math. Soc. **33** (2018), No. 4, pp. 1083–1096
https://doi.org/10.4134/CKMS.c170409
pISSN: 1225-1763 / eISSN: 2234-3024

THE SOURCE OF SEMIPRIMENESS OF RINGS

Neşet Aydin, Çağri Demir, and Didem Karalarlioğlu Camci

Abstract. Let R be an associative ring. We define a subset S_R of R as $S_R = \{a \in R \mid aRa = (0)\}$ and call it the *source of semiprimeness of* R. We first examine some basic properties of the subset S_R in any ring R, and then define the notions such as R being a $|S_R|$-reduced ring, a $|S_R|$-domain and a $|S_R|$-division ring which are slight generalizations of their classical versions. Beside others, we for instance prove that a finite $|S_R|$-domain is necessarily unitary, and is in fact a $|S_R|$-division ring. However, we provide an example showing that a finite $|S_R|$-division ring does not need to be commutative. All possible values for characteristics of unitary $|S_R|$-reduced rings and $|S_R|$-domains are also determined.

1. Introduction

Our primary purpose in this work is to define three types of rings, which to the best of our knowledge, have not appeared in literature before. They are originally motivated by their existing concepts in ring theory, and can be viewed as slight generalizations of their corresponding notions such as reduced rings, domains and division rings, respectively (see Definition 3). To define these new notions of rings, we will first introduce a particular subset of a ring which we call the *source of semiprimeness* of the ring in question. Before getting down into the subject matter, let us first outline the terminology that we will use throughout the paper.

We will mean by a ring an associative nontrivial ring (not necessarily commutative or with identity), and rings possessing a multiplicative identity will be called unitary. Even this would be the case, subrings are not presumed to contain the same identity of the base ring. The term ideal will refer to a two-sided ideal unless it is adorned with the adjective left or right, and a homomorphism from a ring R into a ring T will not be imposed to preserve units even though R and T happen to be unitary.

Received October 2, 2017; Accepted January 10, 2018.
2010 *Mathematics Subject Classification.* Primary 16N60; Secondary 16U80, 16W25.
Key words and phrases. prime ideal, semiprime ideal, prime ring and semiprime ring.

The material in this work is a part of third author's Ph. Dissertation under the supervision of Professor Neşet Aydin.

An element in a unitary ring with a right (*resp.* left) multiplicative inverse will be called a right (*resp.* left) unit, and accordingly it will be meant by a unit a two-sided unit. An element a of a ring R is called a right (*resp.* left) zero-divisor if there exists a nonzero element $b \in R$ such that $ba = 0$ (*resp.* $ab = 0$). An element which is neither a left nor a right zero-divisor is called a nonzero-divisor. A ring which has no nonzero right or left zero-divisors is called a domain, and a ring whose nonzero elements are all units is called a division ring. An element a of a ring R is called a nilpotent element of index n if n is the least positive integer such that $a^n = 0$. A ring with no nonzero nilpotent elements is called a reduced ring. An idempotent element $e = e^2 \in R$ is called central if it commutes with every element of R, that is to say e is contained in the center of R.

Following [3], we define a ring R to be a prime (*resp.* semiprime) ring if the zero ideal is a prime (*resp.* semiprime) ideal of R. Equivalently, R is called a prime ring if $aRb = (0)$ with $a, b \in R$ implies $a = 0$ or $b = 0$; and R is called a semiprime ring if $aRa = (0)$ with $a \in R$ implies $a = 0$. As it is well-known, the class of semiprime rings constitutes a huge class of rings containing, for instance, prime rings (and thus all domains, simple rings and primitive rings), reduced rings and Jacobson semisimple rings (and thus von Neumann regular rings, and in particular, semisimple rings). But this class still excludes many of the important types of other rings (*e.g.* most of the local rings and rings of triangular matrices even over fields). We refer the reader to [1] and [2] for the terminology mentioned so far.

It is now convenient to introduce our main instrument what we focus our attention on throughout the paper. For a ring R, we call the subset

$$S_R = \{a \in R \mid aRa = (0)\} \tag{1}$$

of R as *the source of semiprimeness of* R. It is always a nonempty set as it contains 0, and every element in S_R is nilpotent of index at most 3. At one extreme, S_R may consist only of 0 in which case we say S_R is trivial, and at another extreme, S_R may contain whole of R. Clearly triviality of S_R is only possible when R is a semiprime ring. In the case of 2-torsionfree rings (*i.e.*, rings in which $2x = 0$ implies $x = 0$), it is also possible to describe those rings with $S_R = R$. They are the rings with the property that the so-called Jordan triple product vanishes identically on R, that is to say

$$abc + cba = 0$$

for all $a, b, c \in R$ (see Remark 2.1). Putting these both aside, our general concern will be substantially the cases between these two extremes. A rigorous reader should have already noticed that S_R is always contained in the prime radical of R (see Proposition 2.5). So we can say S_R is not that large a subset to miss out the chance of examining the structure of R by taking a closer look at the elements in $R - S_R$. Let us also say a few words about the name we proposed for S_R. We prefer the name "the source of semiprimeness of R" for

S_R because the elements in $R - S_R$ behave exactly the same way that any nonzero element does in any semiprime ring: $aRa \neq (0)$ for every $a \in R - S_R$, explaining where the "semiprimeness" part comes from.

In Section 2, we investigate basic algebraic properties of S_R for any ring R, and most of the results in this section will be of elementary type. For instance, we shall show that S_R is a semigroup ideal of R (see Proposition 2.4). We will then compare the source of semiprimeness of R with that of $n \times n$ full matrix ring over R and of the corner subrings in R (Proposition 2.6). Another result worth mentioning here is that the source of semiprimeness is preserved under ring isomorphisms (Proposition 2.7).

In Section 3, we will define three new types of rings which we call $|S_R|$-reduced rings, $|S_R|$-domains and $|S_R|$-division rings. They are slight generalizations of their originating notions of a reduced ring, a domain and of a division ring, respectively (see Definition 3). Our main prospect in defining these notions is to restrict defining algebraic conditions for reduced rings, domains and division rings to relatively fewer elements of the ring. As we have previously mentioned, the elements of the subset S_R in any ring R and the zero element of a semiprime ring play analogous roles in some sense. Our presumption is that S_R already contains an adequate amount of "bad" elements of the ring R so that there is enough place out of S_R (*i.e.*, in $R - S_R$) to acquire a reasonable information about the global structure of R.

Section 3 is entirely devoted to the study of basic ring theoretic properties of these rings. A prominent result of this section is that every finite $|S_R|$-domain R is necessarily unitary, and is in fact, a $|S_R|$-division ring (Theorem 3.12). But, in contrast to the classical case, Wedderburn's Little Theorem stating that every finite division ring is commutative, is not valid for finite $|S_R|$-division rings (see Example 3.14). Beside others, we will also determine all possible values that unitary $|S_R|$-domains and $|S_R|$-reduced rings may possess as characteristics (Theorems 3.15 and 3.17). At the end of the paper, we will give two classification theorems (Corollaries 3.18 and 3.16) for the ring $\mathbb{Z}_n$ of integers modulo n to be a $|S_{\mathbb{Z}_n}|$-reduced ring and a $|S_{\mathbb{Z}_n}|$-integral domain (or, equivalently, a $|S_{\mathbb{Z}_n}|$-field).

2. Basic properties of the source of semiprimeness

We start by noting that a more comprehensive version of (1) can also be defined for any nonempty subset A of a ring R as the source of semiprimeness of A in R. We thereby define this more general version of "source", and immediately afterwards, continue examining its basic properties within the present section.

Definition. Let R be a ring and A be a nonempty subset of R. The set $S_R(A) = \{a \in R \mid aAa = (0)\}$ is called the *source of semiprimeness of the subset A in R*.

If the context is clear, we will write S_R in place of $S_R(R)$ for a ring R. It should also be clear now that $S_A = S_R(A) \cap A$ for any subring A of R.

Remark 2.1. As we mentioned earlier, there are two extreme cases for S_R: One is $S_R = (0)$ and the other $S_R = R$. Obviously first one defines semiprime rings. But the case $S_R = R$ should be treated carefully. In this case since $aba = 0$ for all $a, b \in R$, by linearizing this last identity at a, it follows that

$$abc + cba = 0 \tag{2}$$

for all $a, b, c \in R$. The product $\{a, b, c\} := abc + cba$ for $a, b, c \in R$ is called Jordan triple product in literature. What we have shown is that if $S_R = R$, then Jordan triple product vanishes identically in R. Conversely, we assume that (2) holds in R and that R is a 2-torsionfree ring. Then, in particular, one has $2aba = 0$ for all $a, b \in R$ from which $S_R = R$ follows.

We should remark that the torsionfreeness assumption in the above argument is essential for the converse implication work. For instance, consider the subring $R = 3\mathbb{Z}_{18}$ of the ring $\mathbb{Z}_{18}$ of integers modulo 18. R has a nonzero 2-torsion element, namely 9. Moreover, (2) holds in R but $S_R = \{0, 6, 12\} \neq R$.

Since we are not interested in classifying such rings in the present work, we leave this discussion at this level and continue with our principle objective.

Proposition 2.2. *Let A and B be nonempty subsets of R.*

(i) *If $A \subseteq B$, then $S_R(B) \subseteq S_R(A)$.*
(ii) *$S_{R\times R}(A \times B) = S_R(A) \times S_R(B)$.*

Proof. (i) If $b \in S_R(B)$, then $bAb \subseteq bBb = (0)$. Thus $b \in S_R(A)$.

(ii) Now $(a, b) \in S_{R\times R}(A \times B)$ if and only if

$$(0, 0) = (a, b)(x, y)(a, b) = (axa, byb)$$

for all $x \in A$ and $y \in B$. Equivalently, $(a, b) \in S_R(A) \times S_R(B)$. □

The following is an immediate consequence of (ii) of Proposition 2.2.

Corollary 2.3. *If R_1 and R_2 are rings and $A_1 \subseteq R_1$ and $A_2 \subseteq R_2$ are nonempty subsets, then $S_{R_1\times R_2}(A_1 \times A_2) = S_{R_1}(A_1) \times S_{R_2}(A_2)$.* □

Recall that a subset A of the semigroup $(R, \cdot)$ is called a semigroup ideal if $ax, xa \in A$ for all $a \in A$ and $x \in R$. The following proposition proves that S_R is a semigroup ideal in R. Nonetheless, we have no obvious reason to expect S_R to be an additively closed subset, yet alone an ideal of R. However, in some certain circumstances, such as the case when S_R is a nilpotent subset of nilpotency index 2, S_R turns out to be an ideal in R.

Proposition 2.4. *For an ideal I of a ring R, the following holds true*:

(i) *$S_R(I)$ is a semigroup ideal of R. In particular, $S_R(I)$ is a multiplicatively closed subset of R.*
(ii) *If $(S_R(I))^2 = (0)$, then $S_R(I)$ is an ideal of R.*

Proof. (i) Let $a \in S_R(I)$ and $x \in R$ be arbitrary elements. Then $ax, xa \in S_R(I)$, that is $S_R(I)$ is a semigroup ideal of R. The rest is now obvious.

(ii) By (i), $S_R(I)$ is a semigroup ideal of R. Now for any $a, b \in S_R(I)$, we have

$$(a+b)x(a+b) = axb + bxa = 0$$

for all $x \in I$, since $ax, xa \in S_R(I)$ and $(S_R(I))^2 = (0)$ by hypothesis. Hence $a + b \in S_R(I)$. By combining with (i), we conclude that $S_R(I)$ is an ideal of R. □

Prime radical $\mathcal{P}(R)$ of a ring R is defined to be the intersection of all prime ideals of R. It is well-known that every semiprime ideal Q of R is the intersection of prime ideals containing Q.

Proposition 2.5. *If Q is a semiprime ideal of R, then $S_R \subseteq Q$. Consequently, if $\{Q_\lambda\}_{\lambda\in\Lambda}$ is a family of semiprime ideals of R, then $S_R \subseteq \cap_{\lambda\in\Lambda} Q_\lambda$. In particular, S_R is contained in the prime radical $\mathcal{P}(R)$ of R.*

Proof. For all $a \in S_R$, we have $aRa = (0) \subseteq Q$, and thus $a \in Q$ by the semiprimeness of Q. Therefore $S_R \subseteq Q$. The rest is obvious. □

For a subset S of R we denote by $S^{n\times n}$ the set of all $n \times n$ matrices with entries in S. By $M_n(R)$, we will denote the ring of all $n \times n$ matrices over R.

Proposition 2.6. *For a ring R, the following holds true*:

(i) *If $e = e^2 \in R$ is an idempotent, then $eS_R(eRe)e = S_{eRe} = eS_Re$.*
(ii) $S_{M_n(R)} \subseteq (S_R)^{n\times n}$.
(iii) *If S_R is a principal ideal of R, then $S_{M_n(R)} = (S_R)^{n\times n}$.*

Proof. (i) If $a \in S_R(eRe)$, then $aeRea = (0)$ and hence $eaeReae = (0)$ implying $eae \in S_{eRe}$. Therefore $eS_R(eRe)e \subseteq S_{eRe}$. Conversely, if $a \in S_{eRe}$, then one has $eae = a$ and $aeRea = (0)$. This means that $a \in S_R(eRe)$, and since $a = eae$, we get $a \in eS_R(eRe)e$.

If $eae \in S_{eRe}$, then $eaeReae = (0)$. Therefore $eae \in S_R$ which in turn implies $eae = e^2ae^2 \in eS_Re$. Thus $S_{eRe} \subseteq eS_Re$. Conversely, let $a \in S_R$ be any element. Then $aRa = (0)$, and so $eaeReae \subseteq eaRae = (0)$. This means $eae \in S_{eRe}$ and thus we get $eS_Re \subseteq S_{eRe}$.

(ii) Let $a \in S_{M_n(R)}$. For any $1 \leq i, j \leq n$, we denote by e_{ij}'s (formally) the usual matric units, that is e_{ij} is the matrix 1 in the (i, j) position and zero elsewhere. Now for any $x \in R$,

$$a(xe_{ji})a = 0.$$

Left and right multiplying this with e_{ji} yields

$$(a_{ij}xa_{ij})e_{ji} = 0.$$

Hence $a_{ij} \in S_R$ for any $1 \leq i, j \leq n$. So we get $S_{M_n(R)} \subseteq (S_R)^{n\times n}$.

(iii) Assume that $S_R = (\alpha)$ is a principal ideal generated by $\alpha \in R$. Let $a \in (S_R)^{n\times n}$ be any element. For any $b \in M_n(R)$ and $1 \le i, j \le n$, we have

$$(aba)_{ij} = \sum_{k=1}^{n}\sum_{t=1}^{n}(a_{it}b_{tk}a_{kj}).$$

Since $a_{it}, a_{kj} \in S_R = (\alpha)$ for all $1 \le t, k \le n$, it follows that $(aba)_{ij} = 0$ for all $1 \le i, j \le n$. Hence $aba = 0$, that is $a \in S_{M_n(R)}$. Thus in view of (ii), the equality $S_{M_n(R)} = (S_R)^{n\times n}$ holds. □

Proposition 2.7. *Let R and T be rings and $f : R \to T$ a ring homomorphism. Then $f(S_R) \subseteq S_{f(R)}$. Moreover, if f is injective, then the equality holds.*

Proof. Let $a \in S_R$ be any element. Then $f(a)f(R)f(a) = f(aRa) = f(0) = (0)$, and thus $f(a) \in S_{f(R)}$. Therefore $f(S_R) \subseteq S_{f(R)}$, proving the first part. We assume next that f is injective and $f(a) \in S_{f(R)}$. Then $(0) = f(a)f(R)f(a) = f(aRa)$, and since f is injective we get $aRa = (0)$. Hence $a \in S_R$, and so we see that $f(a) \in f(S_R)$ proving the inverse inclusion $S_{f(R)} \subseteq f(S_R)$. □

Lemma 2.8. *Let R be a ring and $a \in S_R$. If $Ra \neq (0) \neq aR$, then a is a zero-divisor. Consequently, an element of R which is a nonzero-divisor is contained in $R - S_R$.*

Proof. Let $a \in S_R$ be any element and assume that $Ra \neq (0) \neq aR$. Then there exist $x, y \in R$ such that $xa \neq 0 \neq ay$. Since $a(xa) = 0$, we conclude that a is a left zero-divisor. On the other hand, since $(ay)a = 0$ we see that a is a right zero-divisor. Hence a is a zero-divisor as desired.

Now let $b \in R$ be a nonzero-divisor. Then $Rb \neq (0) \neq bR$. By the previous argument b cannot be in S_R. So it is in $R - S_R$. □

3. $|S_R|$-reduced rings, $|S_R|$-domains, and $|S_R|$-division rings

We will define in this section three new notions; namely the $|S_R|$-reduced rings, $|S_R|$-domains, and $|S_R|$-division rings. Our main objective will be to give some basic ring theoretic properties of these classes of rings. In the sequel we will show, for instance, that every finite $|S_R|$-domain is necessarily unitary, and is in fact, a $|S_R|$-division ring. So we first give the following.

Definition. Let R be a ring such that $R \neq S_R$.

(i) R is called a $|S_R|$-*reduced ring* if $R - S_R$ has no nilpotent elements.

(ii) R is called a $|S_R|$-*domain* if $R - S_R$ has neither a left nor a right zero-divisor. Accordingly, we call a commutative and unitary $|S_R|$-domain a $|S_R|$-*integral domain.*

(iii) R is called a $|S_R|$-*division ring* if $1 \in R$ and every element in $R - S_R$ is a unit in R. In accordance with the classical ring theory, we shall call a commutative $|S_R|$-division ring a $|S_R|$-*field.*

We shall start with some simple observations about these rings we just defined above, and then we will give an adequate number of examples in due course to get a reasonable insight into what they are and are not.

Observations. We will point out below some easy but worthwhile facts about those classes of rings we want to treat. We might leave the proofs of some of them to the reader for brevity.

1. First, as expected, we note that any reduced ring (*resp.* a domain, a division ring) R is a $|S_R|$-reduced ring (*resp.* a $|S_R|$-domain, a $|S_R|$-division ring). Notice further that a $|S_R|$-division ring R is a $|S_R|$-domain, and that a $|S_R|$-domain R is a $|S_R|$-reduced ring. □

2. If R_i is a $|S_{R_i}|$-domain for $i = 1, 2$, then the direct product $R_1 \times R_2$ is a $|S_{R_1} \times S_{R_2}|$-reduced ring by Proposition 2.2. Moreover, direct product of $|S_{R_i}|$-reduced rings R_i's with $1 \le i \le n$ for some positive integer n is a $|S_{R_1} \times \cdots \times S_{R_n}|$-reduced ring. □

3. Prime radical $\mathcal{P}(R)$ of a $|S_R|$-reduced ring R contains every nilpotent element $a \in R$ since $a \in S_R$ by definition and $S_R \subseteq \mathcal{P}(R)$ by Proposition 2.5. Although we are not going to bother in this work to interrelate our rings with the ones in the atlas of ring theory, we may at least emphasize that such rings, *i.e.*, the rings in which every nilpotent element is contained in the prime radical, are called 2-*primal* in literature. □

Before we proceed we briefly outline some illustrative examples and nonexamples of notions given in Definition 3, some of which we believe will be monitory to avoid misconception or will be useful to perceive the differences between these three notions.

Example 3.1. In the above definition it is substantially necessary to assume that $R \neq S_R$. For instance, we consider the subring $R = \{0, 3, 6\}$ of the ring $\mathbb{Z}_9$ of integers modulo 9. Since $x^2 = 0$ for all $x \in R$, it follows at once that $S_R = R$. Therefore the definitions would be meaningless without the assumption $R \neq S_R$.

Example 3.2. Let $R = T_2(\mathbb{Z})$ be the ring of all 2×2 upper triangular matrices over the ring $\mathbb{Z}$ of integers. It is easy to see that

$$S_R = \begin{pmatrix} 0 & \mathbb{Z} \\ 0 & 0 \end{pmatrix}.$$

Then the set

$$R - S_R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a \neq 0 \text{ or } c \neq 0 \right\}$$

contains zero divisors but no nilpotent elements. So it is a $|S_R|$-reduced ring but not a $|S_R|$-domain.

Example 3.3. Consider the commutative and unitary ring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}.$$

Now it turns out that

$$S_R = \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix},$$

and thus

$$R - S_R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}.$$

Since every element in $R - S_R$ is a unit in R, R is a $|S_R|$-field.

We note also that if we take the entries of matrices in R from an arbitrary division ring instead of $\mathbb{Q}$, R becomes a $|S_R|$-division ring, and if the entries are taken from a domain, R becomes a $|S_R|$-domain. Moreover, the entries are taken from a reduced ring, then R turns out to be a $|S_R|$-reduced ring.

Example 3.4. Consider the commutative and unitary ring

$$R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in F \right\},$$

where F is a field of characteristic 2. By direct computation we can easily see that

$$S_R = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in F \right\}.$$

Consequently

$$R - S_R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a \neq b \right\}.$$

Since the determinants of matrices in $R - S_R$ are all nonzero, R is another example of a $|S_R|$-field.

In the following proposition we will prove two equivalent characterizations of $|S_R|$-reduced rings.

Proposition 3.5. *For a ring R with $R \neq S_R$, the following are equivalent:*

(1) *R is a $|S_R|$-reduced ring.*
(2) *$a^2 \in S_R$ in R implies $a \in S_R$.*
(3) *$a^n \in S_R$ in R implies $a \in S_R$ for any integer $n \geq 1$.*

Proof. (1) $\Rightarrow$ (2). Let R be a $|S_R|$-reduced ring and $a \in R$ be any element such that $a^2 \in S_R$. It then follows that $a^5 = a^2 a a^2 = 0$, and so a must be contained in S_R by the very definition of a $|S_R|$-reduced ring.

(2) $\Rightarrow$ (3). Assume (2) and let $a \in R$ be such that $a^n \in S_R$ where n is the least such positive integer. Since now there exists an integer $k \geq 1$ such that $n \leq 2k \leq n + 1$, we once see that $(a^k)^2 \in S_R$ either by our assumption or by

Proposition 2.4. Therefore we must have $a^k \in S_R$ by (2). We are of course done if $k = 1$. So we may further assume that $k > 1$. Since now $k \leq n - k + 1 < n$, a^k being in S_R contradicts to the choice of n. Therefore n cannot exceed 2, and thus the required result directly follows from our assumptions.

(3) $\Rightarrow$ (1). Let $a \in R$ be any nilpotent element. Then there is an integer $n \geq 1$ such that $a^n = 0 \in S_R$, and hence $a \in S_R$ by our assumption (3). $\square$

Corollary 3.6. *Let R be a $|S_R|$-reduced ring. Then $S_R = \{a \in R \mid a^3 = 0\}$.*

Proof. The inclusion $S_R \subseteq \{a \in R \mid a^3 = 0\}$ is always true for any ring R. So we assume that R is a $|S_R|$-reduced ring and proceed to show that the reverse inclusion also holds. Hence suppose $a \in R$ is such that $a^3 = 0$. Then of course $a^3 \in S_R$, and thus we conclude $a \in S_R$ from the equivalent conditions in Proposition 3.5. $\square$

In the following proposition we will prove that the source of semiprimeness of any nonzero subring of a $|S_R|$-domain R coincides with the source of semiprimeness of R.

Proposition 3.7. *If R is a $|S_R|$-domain, then $S_R(A) = S_R$ for any nonzero subring A of R. Consequently, a nonzero subring A is a $|S_R|$-subdomain of R. Furthermore, A itself is a $|S_A|$-domain.*

Proof. Let A be a nonzero subring of R. Then the inclusion $S_R \subseteq S_R(A)$ follows from Proposition 2.2. To prove the converse inclusion, we suppose on the contrary that there is an element $a \in S_R(A)$ such that $a \notin S_R$. Then $a \in R - S_R$, and so a is a nonzero-divisor in R. In the present case, we get $aA = (0) = Aa$ since $aAa = (0)$ which, in turn, leads us to the contradiction $A = (0)$. Hence the equality $S_R(A) = S_R$ follows. This observation essentially proves also that A is a $|S_R|$-subdomain of R.

It remains to prove the last part. So we assume that $a \in A$ is a zero-divisor. Then a must be in $S_R = S_R(A)$ by what we have shown above. But then having $aAa = (0)$ in hand implies $a \in S_A$. Therefore A is also a $|S_A|$-domain. $\square$

However, for a $|S_R|$-reduced ring R and a nonzero subring A of R, S_R and $S_R(A)$ does not need to coincide (see Example 3.8 below). Nevertheless, as we shall prove in the sequel, a nonzero subring A of a $|S_R|$-reduced ring R is still a $|S_A|$-reduced ring.

Example 3.8. Let T be a unitary reduced ring and $0, 1 \neq e \in T$ be a nontrivial idempotent. We consider the ring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in T \right\}.$$

It is not hard to see that $S_R = \{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in T\}$, and thus

$$R - S_R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in T \text{ and } a \neq 0 \right\}.$$

Notice that $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \in R$ is nilpotent if and only if $a = 0$. Therefore $R - S_R$ has no nilpotent elements, in other words R is a $|S_R|$-reduced ring.

Now we compute $S_R(A)$ for the subring $A = \{\left(\begin{smallmatrix} ea & eb \\ 0 & ea \end{smallmatrix}\right) \mid a, b \in T\}$ of R. Let $\left(\begin{smallmatrix} x & y \\ 0 & x \end{smallmatrix}\right) \in S_R(A)$ be an arbitrary element. Then for any $\left(\begin{smallmatrix} ea & eb \\ 0 & ea \end{smallmatrix}\right) \in A$, one has

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \begin{pmatrix} ea & eb \\ 0 & ea \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} = 0.$$

Since every idempotent in a reduced ring is central, by direct computation, we see that $ex \in S_T = \{0\}$. This means that $x \in Ann(e) = (1-e)T$, the annihilator of e in T. So we get

$$S_R(A) = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \mid x \in (1-e)T, y \in T \right\}.$$

Since $e \neq 1$, $(1-e)T \neq (0)$ and thus $S_R \neq S_R(A)$.

$Ann(e) = (1-e)T$: Clearly $(1-e)T \subseteq Ann(e)$. Conversely, notice that $x = ex + (1-e)x$ for all $x \in T$. If, in particular, $x \in Ann(e)$, then $x = ex + (1-e)x = (1-e)x \in (1-e)T$.

Proposition 3.9. *If R is a $|S_R|$-reduced ring and A is a nonzero subring of R, then A itself is a $|S_A|$-reduced ring.*

Proof. This is almost clear. For if $a \in A$ is a nilpotent element, then a must be in $S_R \subseteq S_R(A)$ since R is a $|S_R|$-reduced ring. Hence we get $a \in A \cap S_R(A) = S_A$ which implies that A is a $|S_A|$-reduced ring. □

At this point we should also remark that S_A and $S_R(A)$ may not be equal even though R is a $|S_R|$-domain. The following is such an example illustrating this situation.

Example 3.10. Let $R = \mathbb{Z}_4[t]\,/P$, where $P = (t^2 + t + 1)$ is the principle ideal generated by the polynomial $t^2 + t + 1$. We note that $\mathbb{Z}_4$ can be viewed as a subring of R via the monomorphism $i : \mathbb{Z}_4 \ni a \mapsto a + P \in R$. Since $S_{\mathbb{Z}_4} = \{0, 2\}$, $\mathbb{Z}_4$ itself is a 2-field. On the other hand, as it can be easily seen that

$$S_R(\mathbb{Z}_4) = \{0 + P, 2 + P, 2x + P, 2 + 2x + P\} = S_R.$$

It is also not hard to verify that every element in $R - S_R$ is a unit in R implying that R is a 4-field.

We continue with the following lemma which will be used in the sequel.

Lemma 3.11. *If R is a $|S_R|$-domain, then $R - S_R$ is a multiplicative set.*

Proof. Assume that $a, b \in R - S_R$. Since by definition a and b are nonzero-divisors, so is their product ab. From Lemma 2.8, we get $ab \in R - S_R$ and hence $R - S_R$ is a multiplicatively closed set. □

Now we are in a position to prove:

Theorem 3.12. *If R is a finite $|S_R|$-domain, then it is a $|S_R|$-division ring.*

Proof. Assume that R is a finite $|S_R|$-domain. We first show that R has an identity element. Now $T = R - S_R$ is a finite set, say with n elements, and thus let $T = \{a_1, \ldots, a_n\}$. Pick any $a \in T$. Since T is multiplicatively closed by Lemma 3.11 and a is neither a left nor a right zero-divisor, both of the maps $x \mapsto ax$ and $x \mapsto xa$ from T into T are injective. Now because of the finite cardinality, these maps must also be surjective, and thus bijective. Therefore there exist $1 \leq i, j \leq n$ (depending on the choice of a) such that $aa_i = a = a_j a$. Then

$$aa_i a = a^2 = aa_j a,$$

and so

$$a_i = a_j$$

since a is a nonzero-divisor. Now we have in hand the following equalities:

$$aa_i = a = a_i a.$$

Take any other $b \in T$. As above, there is an element $a_i^{'} \in T$ such that

$$ba_i^{'} = b = a_i^{'} b.$$

Accordingly, one has

$$(ab)a_i^{'} = a(ba_i^{'}) = ab,$$
$$a_i(ab) = (a_i a)b = ab.$$

By comparison we get

$$(ab)a_i^{'} = ab = a_i(ab),$$

and by the same argument we used in the very beginning, since $ab \in T$, it follows that $a_i^{'} = a_i$. Set $e = a_i$ and notice that e acts as the multiplicative identity in the sub-semigroup T. Notice also that we particularly have $e^2 = e$.

Now let $x \in R$ be arbitrary. Then we either have $x \in T$ or $x \in S_R$. If $x \in T$, then $xe = x = ex$ as we have already proved. So we may assume that $x \in S_R$. We claim first that $e - ex \in T$. Suppose on the contrary that $e - ex \in S_R$. Then

$$0 = (e - ex)e(e - ex) = e - ex - exe + exex = e - ex - exe.$$

Right multiplying $e - ex - exe = 0$ with x results in $ex = ex^2$. Now since $x^3 = 0$ (because $xRx = (0)$), right multiplying the identity $ex = ex^2$ with x yields $ex = ex^2 = ex^3 = 0$. But this implies $e = e - ex - exe = 0$, a contradiction because $e \in T$. Similarly one can prove that $e - xe \in T$. Since e acts as the identity element in the semigroup T, we must have

$$(e - ex)e = e - ex$$

and

$$e(e - xe) = e - xe.$$

By comparing these last two equations we once see that $ex = exe = xe$. Finally, since $(xe - x)e = 0$ and e is not a right zero-divisor, we conclude that $xe = x$. Therefore e is in fact the multiplicative identity of R. We rename e as 1.

We have shown up to now that R is unitary. Turning back to the bijections $x \mapsto ax$ and $x \mapsto xa$ again from T onto T, we conclude that there exist $x, y \in T$ such that $ax = 1 = ya$, that is a is a unit in R. Hence R is in fact a $|S_R|$-division ring. □

We immediately have the following corollary of the above theorem.

Corollary 3.13. *Every finite $|S_R|$-integral domain is a $|S_R|$-field.*

Now, one may of course wonder whether Wedderburn's Little Theorem is valid for a finite $|S_D|$-division ring D. More precisely, is every finite $|S_D|$-division ring D is commutative? The answer to this question is negative as the following example shows.

Example 3.14. Let F be a field and ϕ be a nonidentity monomorphism of F. Then the ring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & \phi(a) \end{pmatrix} \mid a, b \in F \right\}$$

is a noncommutative unital ring. It is not hard to see that $S_R = \left(\begin{smallmatrix} 0 & F \\ 0 & 0 \end{smallmatrix}\right)$, and thus every element in

$$R - S_R = \left\{ \begin{pmatrix} a & b \\ 0 & \phi(a) \end{pmatrix} \mid a \neq 0 \right\}$$

is invertible. Hence R is a $|S_R|$-division ring. When we take F to be a finite field, R turns out to be a finite $|S_R|$-division ring which is noncommutative.

This example also shows that the multiplicative group $R - S_R$ need not be cyclic even if the field F is finite. Indeed, if it was true that the group $R - S_R$ is cyclic, then it would be abelian which is obviously not the case. We can actually bring a more tangible example into being as follows: Take $F = GF(4)$ to be the Galois field of 4 elements and ϕ to be the Frobenius automorphism sending each element of F to its square. Then by direct computation it can be verified that any nonidentity element in the group $R - S_R$ is either of order 2 or of order 3 while the order of $R - S_R$ is 12.

The following theorem puts forward all possibilities for values of characteristics that a unitary $|S_R|$-domain R may possess.

Theorem 3.15. *If R is a unitary $|S_R|$-domain, then the characteristic of R is either 0, or a prime p, or square of a prime p.*

Proof. We assume that $\mathrm{char}(R) = n > 1$ and that p is a prime dividing n, say $n = pk$ for some integer $1 \leq k < n$. We then see that

$$0 = n \cdot 1 = (p \cdot 1)(k \cdot 1),$$

that is, $p \cdot 1$ is a zero-divisor, and so it must be in S_R. Therefore we get

$$0 = (p \cdot 1)x(p \cdot 1) = p^2 \cdot x$$

for all $x \in R$ implying that n divides p^2. But p divides n, and hence $n \in \{p, p^2\}$, proving the claim. □

We note that easy-to-verify examples for each case are $\mathbb{Z}$, $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ for a prime p. In fact, in view of the above theorem it is possible to classify $|S_{\mathbb{Z}_n}|$-integral domains (as well as $|S_{\mathbb{Z}_n}|$-fields by Corollary 3.13) among the rings $\mathbb{Z}_n$ of integers modulo n.

Corollary 3.16. *Let $n > 1$ be an integer. Then $\mathbb{Z}_n$ is a $|S_{\mathbb{Z}_n}|$-integral domain* (*and hence a $|S_{\mathbb{Z}_n}|$-field*) *if and only if n is either a prime p or p^2.*

Proof. If $\mathbb{Z}_n$ is a $|S_{\mathbb{Z}_n}|$-integral domain, then n, the characteristic of $\mathbb{Z}_n$, is either p or p^2 for some prime p by Theorem 3.15. The converse is clear as we have already mentioned above. □

Theorem 3.17. *If R is a unitary $|S_R|$-reduced ring, then the characteristic of R is a cube-free integer n, i.e., there is no prime p such that p^3 divides n.*

Proof. Assume that $\mathrm{char}(R) = n > 1$ and that p is prime dividing n, say $n = p^\alpha t_0$ for some $\alpha \geq 1$ and $1 \leq t_0 < n$ with p coprime to t_0. Then

$$(pt_0 \cdot 1)^\alpha = t_0^{\alpha-1} \cdot (n \cdot 1) = 0,$$

and thus $pt_0 \cdot 1 \in S_R$. Therefore, $p^2 t_0^2 \cdot x = (pt_0 \cdot 1)x(pt_0 \cdot 1) = 0$ for all $x \in R$. Hence n divides $p^2 t_0^2$, that is, there is an integer $t_1 \geq 1$ such that $p^\alpha t_0 t_1 = p^2 t_0^2$. Suppose for the moment that $\alpha \geq 3$. We thence get $t_0 = p^{\alpha-2} t_1$ leading us to the contradiction p divides t_0. Hence n must be a cube-free integer. □

As for the classification of $|S_{\mathbb{Z}_n}|$-integral domains, we have the following.

Corollary 3.18. *Let $n > 1$ be an integer. Then $\mathbb{Z}_n$ is a $|S_{\mathbb{Z}_n}|$-reduced ring if and only if n is a cube-free integer.*

Proof. Assume that $\mathbb{Z}_n$ is a $|S_{\mathbb{Z}_n}|$-reduced ring. Since now the characteristic of $\mathbb{Z}_n$ is n, n is a cube-free integer by Theorem 3.17.

Conversely, assume that n is a cube-free integer. Then there exist distinct primes $p_1, \ldots, p_r$ and integers $\alpha_1, \ldots, \alpha_r$ with $1 \leq \alpha_i \leq 2$ for each $i \in \{1, \ldots, r\}$ such that $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. It is quite easy to observe that

$$S_{\mathbb{Z}_n} = \{\bar{a} \in \mathbb{Z}_n \mid \bar{a}^2 = \bar{0}\} = (\overline{p_1 \cdots p_r}).$$

Let now $\bar{a} \in \mathbb{Z}_n$ be any element such that $\bar{a}^2 \in S_{\mathbb{Z}_n}$. Then one gets

$$a^2 = p_1 \cdots p_r k + nt$$

for some integers k and t. Therefore each p_i divides a since they all divide a^2. This means that $a = p_1 \cdots p_r q$ for some $q \in \mathbb{Z}$. Accordingly $\bar{a} = \overline{p_1 \cdots p_r q} \in S_{\mathbb{Z}_n}$. Now we can apply Proposition 3.5 to be able to conclude that $\mathbb{Z}_n$ is a $|S_{\mathbb{Z}_n}|$-reduced ring. □

Conclusion 3.19. *In the light of Proposition 2.5 it can be seen that S_R coincides with the prime radical under some conditions. This issue will be discussed in our next study.*

Acknowledgement. The authors are very thankful to Dr. Çetin Camcı for his valuable suggestions and comments.

References

[1] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, **131**, Springer-Verlag, New York, 1991.

[2] ———, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, **189**, Springer-Verlag, New York, 1999.

[3] N. H. McCoy, *The Theory of Rings*, The Macmillan Co., New York, 1964.

Neşet Aydin
Department of Mathematics
Çanakkale Onsekİz Mart University
Çanakkale 17020, Turkey
Email address: neseta@comu.edu.tr

Çağri Demir
Department of Mathematics
Ege University
İzmir, Turkey
Email address: cagri.demir@ege.edu.tr

Didem Karalarlioğlu Camci
Department of Mathematics
Çanakkale Onsekİz Mart University
Çanakkale 17020, Turkey
Email address: didemk@comu.edu.tr