# RINGS WHOSE SUBRINGS HAVE AN IDENTITY

GREG OMAN AND JOHN STROUD

Abstract. Let $R$ be a ring. A nonempty subset $S$ of $R$ is a *subring* of $R$ if $S$ is closed under negatives, addition, and multiplication. In this paper, we determine the rings $R$ for which every subring $S$ of $R$ has a multiplicative identity (which need not be the identity of $R$).

## 1. Introduction

Let $R$ be a ring (assumed only to be associative, not necessarily commutative or with 1). Recall that a nonempty subset $S$ of $R$ is a *subring* of $R$ if $S$ is closed under negatives, addition, and multiplication.[1] Suppose now that $R$ has a 1. It is easy to see that a subring $S$ of $R$ need not have an identity. For instance, the subring $2\mathbb{Z}$ of $\mathbb{Z}$ consisting of the even integers has no multiplicative identity. In fact, it is easy to see that the only subrings of $\mathbb{Z}$ which have an identity are $\{0\}$ and $\mathbb{Z}$.

On the other extreme, consider the seemingly uninteresting ring $\mathbb{Z}/6\mathbb{Z}$. The subrings of $\mathbb{Z}/6\mathbb{Z}$ are as follows:

(1) $S_1 := \{\overline{0}\}$,
(2) $S_2 := \{\overline{0}, \overline{3}\}$,
(3) $S_3 := \{\overline{0}, \overline{2}, \overline{4}\}$, and
(4) $S_4 := \mathbb{Z}/6\mathbb{Z}$.

One easily verifies that $\overline{0}$ is the identity of $S_1$, $\overline{3}$ is the identity of $S_2$, $\overline{4}$ is the identity of $S_3$, and $\overline{1}$ is the identity of $S_4$. Hence every subring of $\mathbb{Z}/6\mathbb{Z}$ has an identity.

The purpose of this note is to classify the rings with the above property enjoyed by $\mathbb{Z}/6\mathbb{Z}$. That is, we shall find all rings $R$ up to isomorphism with the property that every subring of $R$ has an identity. This work is related to results in the literature. For example, in [2], the authors study commutative rings with identity with the property that every proper unital subring is Artinian; they show that such rings are precisely the Artinian rings for which every unital subring is Artinian. Now suppose that $X$ is an infinite set and $R$ is a binary relation on $X$. For $2 \leq \kappa \leq |X|$, say that $(X, R)$ is $\kappa$-homogeneous if any two subsets of size $\kappa$ are isomorphic (with the order induced by $R$). Such structures were classified by Droste in [1]. The first author has conducted related research in universal and commutative algebra; see [5] - [8].

*2010 Mathematics Subject Classification.* Primary:16B99; Secondary:13A99, 12E99.

*Key Words and Phrases. absolutely algebraic field, Jacobson's Theorem, reduced ring.*

[1]Some authors define a subring $S$ of a ring $R$ with identity $1_R$ to be *unital* if $1_R \in S$. In fact, it is commonplace for many authors to consider only rings with identity and only subrings which are unital.

## 2. Results

To streamline terminology, let us agree to call a nonzero ring $R$ with the property that every subring of $R$ has an identity *strongly unital*. As the example in the introduction shows, the identities of the subrings need not all be the same, in stark contrast to the fact that the additive identity of a subring coincides with the additive identity of the ambient ring.

We begin by recalling that an element $\alpha$ of a ring $R$ is *nilpotent* if there is a positive integer $n$ such that $\alpha^n = 0$. If $R$ has no nonzero nilpotent elements, then $R$ is said to be *reduced*.

**Proposition 1.** *Every strongly unital ring is reduced.*

*Proof.* Suppose that $R$ be a strongly unital ring and let $\alpha \in R$. As is well-known, it suffices to prove that if $\alpha^2 = 0$, then $\alpha = 0$. Thus suppose $\alpha^2 = 0$ and set $S := \{n\alpha \colon n \in \mathbb{Z}\}$. One checks at once that $S$ is a subring of $R$ with trivial multiplication. But $S$ has an identity, and therefore $S = \{0\}$. We deduce that $\alpha = 0$, as desired. $\square$

Recall next that if $R$ is a ring with identity, then the so-called *prime subring* $P(R)$ of $R$ is the subring of $R$ generated by $1_R$. Since $P(R)$ is a homomorphic image of $\mathbb{Z}$, it is clear that $P(R) \cong \mathbb{Z}$ or $P(R) \cong \mathbb{Z}/n\mathbb{Z}$ for some positive integer $n$. We now record a trivial but useful observation and then prove several lemmas.

**Observation 1.** *Suppose that a ring $R$ is strongly unital. Then so is every nontrivial subring of $R$.*

**Lemma 1.** *Let $R$ be a strongly unital ring. Then $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ for some square-free integer $m > 1$.*

*Proof.* Let $R$ be strongly unital. Now, $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ for some integer $m \geq 0$. Since $2\mathbb{Z}$ is a nonunital subring of $\mathbb{Z}$, we see that $m \neq 0$. As $R$ is a nontrivial ring, $m \neq 1$. This shows that $m > 1$. Invoking Proposition 1, we deduce that $P(R)$ is reduced, and hence $m$ is square-free. $\square$

The following lemma is a well-known result in elementary field theory, but since its proof is short, we include it.

**Lemma 2.** *Let $F$ be a finite field and let $f(X) \in F[X]$ be a nonzero polynomial. Then $F[X]/\langle f(X)\rangle$ is finite.*

*Proof.* Suppose that $F$ is a finite field, and fix some nonzero polynomial $f(X) \in F[X]$ of degree $n \geq 0$. As is well-known, the polynomial ring $F[X]$ is a Euclidean domain. Thus via the Division Algorithm, every member of the quotient ring $F[X]/\langle f(X)\rangle$ can be expressed in the form $\langle f(X)\rangle + r(X)$, where $r(X) \in F[X]$ is zero or of degree less than $n$. It follows that $|F[X]/\langle f(X)\rangle| \leq |F|^n$, and therefore $F[X]/\langle f(X)\rangle$ is finite. $\square$

**Lemma 3.** *Suppose that $R$ is a ring with identity. The polynomial ring $R[X]$ is not strongly unital.*

*Proof.* If $R$ is the trivial ring, then $R[X]$ is also trivial, thus by definition is not strongly unital. Now suppose that $R$ is nontrivial. Then it is easy to see that the subring $XR[X]$ (the subring of polynomials with constant term 0) does not have an identity: if $f(X) \in XR[X]$, then $X \cdot f(X) \neq X$. $\square$

We are almost equipped to prove our next proposition; first we comment on notation. Let $R$ be a ring with identity and let $S$ be a subring of $R$ contained in $Z(R)$, the center of $R$. Further, let $a \in R$. Then we define $S[a]$ as follows:

$$S[a] = \{s_0 + s_1 a + \cdots + s_n a^n : n \in \mathbb{N}, s_i \in S\} = \{f(a) : f(X) \in S[X]\}. \tag{2.1}$$

Observe that $S[a]$ is a subring of $R$ containing $S$ but need *not* contain $a$. However, if $R$ is unital with identity $1_R$ and $1_R \in S$, then $S[a]$ contains $a$ and, moreover, $S[a]$ is the smallest subring of $R$ containing $S$ and $a$.

**Proposition 2.** *Suppose $R$ is a strongly unital ring. Then for every $\alpha \in R$, there exists a positive integer $n$ (depending on $\alpha$) such that $\alpha^n = \alpha$. Therefore, $R$ is commutative.*

*Proof.* Let $R$ be a strongly unital ring and let $\alpha \in R$ be arbitrary. Recall from Lemma 1 that $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ for some integer $m > 1$ which is square-free; say $m = p_1 \cdots p_k$, where the $p_i$s are distinct primes. It follows that $P(R)$ is the internal direct sum of rings $S_1, \ldots, S_k$, where each $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$. Clearly $P(R) \subseteq Z(R)$, and hence each $S_i \subseteq Z(R)$. It is straightforward to check that

$$P(R)[\alpha] = (S_1 + \cdots + S_k)[\alpha] = S_1[\alpha] + \cdots + S_k[\alpha]. \tag{2.2}$$

Fix $i$ with $1 \leq i \leq k$. Recall that $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$. Thus there are ring surjections $f : \mathbb{Z}/p_i\mathbb{Z}[X] \to S_i[X]$ and (by 2.1) $g : S_i[X] \to S_i[\alpha]$. Letting $K$ be the kernel of the composition, we have $S_i[\alpha] \cong \mathbb{Z}/p_i\mathbb{Z}[X]/K$. If $K$ is trivial, then $S_i[\alpha] \cong \mathbb{Z}/p_i\mathbb{Z}[X]$. But then by Observation 1, $\mathbb{Z}/p_i\mathbb{Z}[X]$ is strongly unital, contradicting Lemma 3. We conclude that $K$ is nontrivial. Invoking Lemma 2 (and using the fact that $\mathbb{Z}/p\mathbb{Z}[X]$ is a PID), $S_i[\alpha]$ is finite. As $1 \leq i \leq k$ was arbitrary, it follows from (2.2) above that

$$P(R)[\alpha] \text{ is a finite ring.} \tag{2.3}$$

Note that Proposition 1 implies that $P(R)[\alpha]$ is reduced. Thus as is well-known (and an easy consequence of the Chinese Remainder Theorem),

$$P(R)[\alpha] \cong F_1 \times \cdots \times F_j \text{ for some finite fields } F_1, \ldots, F_j. \tag{2.4}$$

Now, for any $a \in F_i^\times$, $1 \leq i \leq j$, we have $a^{|F_i|-1} = 1$. We deduce that for any $\beta \in F_1 \times \cdots \times F_j$, $\beta^{(|F_1|-1)\cdots(|F_j|-1)+1} = \beta$. But then there is a positive integer $n$ such that $\beta^n = \beta$. Applying (2.4), we see that there is a positive integer $m$ such that $\alpha^m = \alpha$. That $R$ is commutative is now immediate from Jacobson's Theorem (see [3], p. 367). $\square$

**Remark 1.** *The fact that the integer $m$ in the above proof is square-free is essential to our proof of (2.3). Indeed, suppose that $n > 1$ is an integer which is not square-free, and let $N$ be the nilradical of $\mathbb{Z}/n\mathbb{Z}$. Then $N$ is nontrivial and proper. Therefore, $\mathbb{Z}/n\mathbb{Z}[X]/N[X] \cong ((\mathbb{Z}/n\mathbb{Z})/N)[X]$ is infinite. Hence it is not the case that $\mathbb{Z}/n\mathbb{Z}[X]/K$ is finite for every nonzero ideal $K$ of $\mathbb{Z}/n\mathbb{Z}[X]$.*

We pause now to recall more terminology. If $R$ is a ring and $I$ is an (two-sided) ideal of $R$, then $I$ is *indecomposable* if there do not exist nonzero ideals $I_1$ and $I_2$ of $R$ such that $I = I_1 \oplus I_2$. A ring $R$ is indecomposable if it is indecomposable as an ideal of itself. Our next lemma may be in the literature, but we could not locate a source. Therefore, we present a self-contained proof.

**Lemma 4.** *Let $R$ be a ring, and suppose that $R$ does not contain an ideal which is an infinite internal direct sum of nonzero ideals of $R$. Then $R = I_1 \oplus \cdots \oplus I_n$ for some indecomposable ideals $I_1, \ldots, I_n$ of $R$.*

*Proof.* We proceed by contraposition. Thus let $R$ be a ring, and suppose that $R$ is not a finite direct sum of indecomposable ideals. Then $R$ is not indecomposable as an ideal, and hence $R = I_1 \oplus J_1$ for some nonzero ideals $I_1$ and $J_1$. Since $R$ is not a finite direct sum of indecomposable ideals, we may assume without loss of generality that $J_1$ is not indecomposable. Hence $J_1 = I_2 \oplus J_2$ for some nonzero ideals $I_2$ and $J_2$. Now, $R = I_1 \oplus I_2 \oplus J_2$. Again, $R$ is not a finite direct sum of indecomposable ideals, and so we may assume without loss of generality that $J_2$ is not indecomposable. Thus $J_2 = I_3 \oplus J_3$ for some nonzero ideals $I_3$ and $J_3$. Thus $R = I_1 \oplus I_2 \oplus I_3 \oplus J_3$. Proceeding recursively, we see that $R$ contains an ideal which is an infinite internal direct sum of nonzero ideals of $R$, and the proof is complete. $\square$

We are almost ready to classify the strongly unital rings. First, we establish a final lemma and recall a couple of definitions. The lemma is a special case of a more general result in the literature; on p. 22 of [4], the author establishes that a left Artinian ring with no nonzero nilpotent left ideals is a semisimple ring with identity. Our next lemma is an immediate consequence of this fact.

**Lemma 5.** *Every finite reduced commutative ring has an identity.*

Before stating our main theorem, we remind the reader that if $F$ is a field, then the *prime subfield* of $F$ is the subfield of $F$ generated by 1. It is easy to see that if $F$ has characteristic $p$, then the prime subfield of $F$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$; if $F$ has characteristic 0, then the prime subfield of $F$ is isomorphic to $\mathbb{Q}$. Finally, $F$ is called *absolutely algebraic* if $F$ is algebraic over its prime subfield. Our main result and its proof conclude this note.

**Theorem 1.** *Let $R$ be a ring. Then $R$ is strongly unital if and only if there is a positive integer $n$ such that $R \cong F_1 \times \cdots \times F_n$, where each $F_i$ is an absolutely algebraic field of prime characteristic.*

*Proof.* Assume first that $R$ is a ring which is strongly unital. We claim that

(2.5) there is no ideal of $R$ which is an infinite internal direct sum of nonzero ideals of $R$.

Suppose not, and let $X$ be an infinite index set and $\{I_x \colon x \in X\}$ an enumeration of nonzero ideals of $R$ which generate a direct sum. Because $X$ is infinite, it is clear that $\bigoplus_{x \in X} I_x$ does not have a multiplicative identity. However, $\bigoplus_{x \in X} I_x$ is an ideal of $R$, hence also a subring of $R$. This contradicts the assumption that $R$ is strongly unital, and (2.5) is verified. It now follows from Lemma 4 (and the fact that by definition, $R$ is nontrivial) that there exist nonzero indecomposable ideals $I_1, \ldots, I_n$ of $R$ such that $R = I_1 \oplus \cdots \oplus I_n$. Observe that the map $(i_1, \ldots, i_n) \mapsto i_1 + \cdots + i_n$

is a ring isomorphism between the external direct product $I_1 \times \cdots \times I_n$ of the rings $I_1, \ldots, I_n$ and $R$. We record this below:

$$R \cong I_1 \times \cdots \times I_n \text{ (as rings).} \tag{2.6}$$

To finish proving the first implication of the theorem, it remains only to show that

$$I_k \text{ is an absolutely algebraic field of prime characteristic for every } k, 1 \leq k \leq n. \tag{2.7}$$

Clearly it suffices to prove the assertion for $I := I_1$. Toward this end, since $I$ is a subring of $R$ and $R$ is strongly unital, there is some $1_I \in I$ which is a multiplicative identity for $I$. We claim that

$$\text{the only idempotents of } I \text{ are } 0 \text{ and } 1_I. \tag{2.8}$$

Indeed, if $e \neq 0, 1_I$ is an idempotent of $I$, then $I$ decomposes as $I = Ie \oplus I(1_I - e)$. Now observe that both $Ie$ and $I(1_I - e)$ are nonzero ideals of $R$, and we have contradicted the fact that $I$ is indecomposable. We now easily show that $I$ is a field. Recall from Proposition 2 that $R$ is commutative. Next, let $r \in I$ be nonzero. Then clearly $Ir \subseteq I$ is a nonzero ideal of $R$, hence has an identity element $e^*$. Because $e^*$ is idempotent, we deduce from (2.8) that $e^* = 0$ or $e^* = 1_I$. $e^* \neq 0$, lest $Ir = \{0\}$. We conclude that $e^* = 1_I$, and thus $1_I \in Ir$. But this means that $r$ is invertible, and $I$ is a field, as claimed. Finally, Proposition 2 implies that $I$ is absolutely algebraic of prime characteristic.

Conversely, suppose that $R \cong F_1 \times \cdots \times F_n$, where each $F_k$ is an absolutely algebraic field of prime characteristic, and let $S$ be a subring of $R$. We shall prove that $S$ has an identity. We may of course assume that $S$ is nontrivial. For $1 \leq i \leq n$, let $\pi_i \colon R \to F_i$ be the projection map onto the $i$th coordinate. Further, set $\pi(S) := \{1 \leq i \leq n \colon \pi_i(S) \text{ is nontrivial}\}$. Without loss of generality, we may suppose that $\pi(S) = \{1, 2, \ldots, r\}$ for some $r$ with $1 \leq r \leq n$. For $1 \leq i \leq r$, let $x_i \in S$ be such that

$$\pi_i(x_i) \neq 0. \tag{2.9}$$

Now let $S'$ be the subring of $S$ generated by $x_1, \ldots, x_r$. Further, for each $i$ with $1 \leq i \leq n$, let $K_i$ be the prime subfield of $F_i$. It is clear that up to isomorphism,

$$S' \text{ is a subring of } K_1(\pi_1(x_1), \pi_1(x_2), \ldots, \pi_1(x_r)) \times \cdots \times K_n(\pi_n(x_1), \pi_n(x_2), \ldots, \pi_n(x_r)). \tag{2.10}$$

Recall that each $K_i$ is finite and each $\pi_i(x_j)$ is algebraic over $K_i$. But then it follows that each $K_i(\pi_i(x_1), \pi_i(x_2), \ldots, \pi_i(x_r))$ is a finite field, and we conclude from (2.10) that $S'$ is finite. Applying Lemma 5, we see that $S'$ has a multiplicative identity $1_{S'} := (e_1, \ldots, e_r, 0, \ldots, 0)$. We claim that $1_{S'}$ is also an identity for $S$. Toward this end, it clearly suffices to prove that $e_i = 1$ for $1 \leq i \leq r$ (here, 1 is the multiplicative identity of $F_i$). To see this, simply note that $1_{S'} \cdot x_i = x_i$. Therefore, $\pi_i(1_{S'}) \cdot \pi_i(x_i) = \pi_i(x_i)$. Applying (2.9) and the fact that $F_i$ is a field, we deduce that $e_i = \pi_i(1_{S'}) = 1$, and the proof is complete. $\square$

**Acknowledgment.** The authors thank the anonymous referees, whose comments improved the exposition of this note.

## References

[1] M. Droste, *$k$-homogeneous relations and tournaments.* Quart. J. Math. Oxford Ser. (2) **40** (1989), no. 157, 1–11.

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

[3] I.N. Herstein, *Topics in Algebra.* Blaisdell Publishing Co., New York-Toronto-London, 1964.

[4] J. Jans, *Rings and Homology.* Holt, Rinehart, and Winston Inc., New York-Chicago-San Francisco-Toronto-London, 1964.

[5] G. Oman, *Elementarily $\lambda$-homogeneous binary functions.* Algebra Universalis **78** (2017), no. 2, 147–157.

[6] G. Oman, *More results on congruent modules.* J. Pure Appl. Algebra **213** (2009), no. 11, 2145–2155.

[7] G. Oman, *On elementarily $\kappa$-homogeneous unary structures.* Forum Math. **23** (2011), no. 4, 791–802.

[8] G. Oman, *On modules $M$ for which $N \cong M$ for every submodule $N$ of size $|M|$.* J. Commut. Algebra **1** (2009), no. 4, 679–699.

(Greg Oman) Department of Mathematics, University of Colorado, Colorado Springs, Colorado Springs, CO 80918, USA

*Email address*: goman@uccs.edu

(John Stroud) Department of Physics, University of Colorado, Colorado Springs, Colorado Springs, CO 80918, USA

*Email address*: jstroud@uccs.edu