involve
a journal of mathematics

Rings whose subrings have an identity

Greg Oman and John Stroud

msp

2020 vol. 13, no. 5

INVOLVE 13:5 (2020)
https://doi.org/10.2140/involve.2020.13.823

Rings whose subrings have an identity

Greg Oman and John Stroud

(Communicated by Kenneth S. Berenhaut)

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. 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

$$S_1 := \{\bar{0}\}, \quad S_2 := \{\bar{0}, \bar{3}\}, \quad S_3 := \{\bar{0}, \bar{2}, \bar{4}\} \quad \text{and} \quad S_4 := \mathbb{Z}/6\mathbb{Z}.$$

One easily verifies that $\bar{0}$ is the identity of S_1, $\bar{3}$ is the identity of S_2, $\bar{4}$ is the identity of S_3, and $\bar{1}$ 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 [Gilmer and Heinzer 1992], the authors studied 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 $2 \leq \kappa \leq |X|$, we say that (X, R) is κ-homogeneous if any two subsets of size κ are isomorphic (with the order induced by R). Such structures were classified in [Droste 1989]. The first author has conducted related research in universal and commutative algebra; see [Oman 2009a; 2009b; 2011; 2017].

MSC2010: primary 16B99; secondary 13A99, 12E99.

Keywords: 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 α 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 is 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 $S := \{n\alpha : n \in \mathbb{Z}\}$. 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. □

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 2. Suppose that a ring R is strongly unital. Then so is every nontrivial subring of R.

Lemma 3. *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. □

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

Lemma 4. *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 as $\langle f(X)\rangle + r(X)$, 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. □

Lemma 5. *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, and 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 $X \cdot f(X) \neq X$. □

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

$$S[a] = \{s_0 + s_1 a + \cdots + s_n a^n : n \in \mathbb{N}, s_i \in S\} = \{f(a) : f(X) \in S[X]\}. \quad (2\text{-}1)$$

Observe that $S[a]$ is a subring of R containing S, but it 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 6. *Suppose R is a strongly unital ring. Then for every $\alpha \in R$, there exists a positive integer n (depending on α) 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 3 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 are distinct primes. It follows that $P(R)$ is the internal direct sum of rings $S_1, \ldots, S_k$, where $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$ for $i = 1, \ldots, k$. Clearly $P(R) \subseteq Z(R)$, and hence $S_i \subseteq Z(R)$ for $i = 1, \ldots, k$. It is straightforward to check that

$$P(R)[\alpha] = (S_1 + \cdots + S_k)[\alpha] = S_1[\alpha] + \cdots + S_k[\alpha]. \quad (2\text{-}2)$$

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 2, $\mathbb{Z}/p_i\mathbb{Z}[X]$ is strongly unital, contradicting Lemma 5. We conclude that K is nontrivial. Invoking Lemma 4 (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

$$P(R)[\alpha] \text{ is a finite ring.} \quad (2\text{-}3)$$

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),

$$P(R)[\alpha] \cong F_1 \times \cdots \times F_j \quad \text{for some finite fields } F_1, \ldots, F_j. \quad (2\text{-}4)$$

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 $\beta \in F_1 \times \cdots \times F_j$, we have $\beta^{(|F_1|-1)\cdots(|F_j|-1)+1} = \beta$. 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 [Herstein 1964, p. 367]. □

Remark 7. 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 a (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 8. *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. □

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; in [Jans 1964, p. 22], 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 9. *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 10. *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

there is no ideal of R which is an infinite direct sum of nonzero ideals of R. (2-5)

Suppose not, and let X be an infinite index set and $\{I_x : x \in X\}$ 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, and 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 8 (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

$$I_k \text{ is an absolutely algebraic field of prime characteristic for } 1 \le k \le n. \tag{2-7}$$

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 6 that R is commutative. Next, let $r \in I$ be nonzero. Then clearly $Ir \subseteq I$ is a nonzero ideal of R, and hence has an identity element e^*. Because e^* is idempotent, we deduce from (2-8) that $e^* = 0$ or $e^* = 1_I$. Also $e^* \neq 0$, 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 6 implies that I is absolutely algebraic of prime characteristic.

Conversely, suppose $R \cong F_1 \times \cdots \times F_n$, 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 $1 \le i \le n$, let $\pi_i : R \to F_i$ be the projection map onto the i-th coordinate. Further, set $\pi(S) := \{1 \le i \le n : \pi_i(S) \text{ is nontrivial}\}$. Without loss of generality, we may suppose that

$\pi(S) = \{1, 2, \ldots, r\}$ for some r with $1 \le r \le n$. For $1 \le i \le r$, 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 $1 \le i \le n$, let K_i be the prime subfield of F_i. It is clear that, up to isomorphism, S' 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 9, 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 $1 \le i \le r$ (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. □

Acknowledgment

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

References

[Droste 1989] M. Droste, "k-homogeneous relations and tournaments", *Quart. J. Math. Oxford Ser.* (2) **40**:157 (1989), 1–11. MR Zbl

[Gilmer and Heinzer 1992] R. Gilmer and W. Heinzer, "An application of Jónsson modules to some questions concerning proper subrings", *Math. Scand.* **70**:1 (1992), 34–42. MR Zbl

[Herstein 1964] I. N. Herstein, *Topics in algebra*, Blaisdell, New York, 1964. MR Zbl

[Jans 1964] J. P. Jans, *Rings and homology*, Holt, Rinehart and Winston, New York, 1964. MR Zbl

[Oman 2009a] G. Oman, "More results on congruent modules", *J. Pure Appl. Algebra* **213**:11 (2009), 2147–2155. MR Zbl

[Oman 2009b] G. Oman, "On modules M for which $N \cong M$ for every submodule N of size $|M|$", *J. Commut. Algebra* **1**:4 (2009), 679–699. MR Zbl

[Oman 2011] G. Oman, "On elementarily κ-homogeneous unary structures", *Forum Math.* **23**:4 (2011), 791–802. MR Zbl

[Oman 2017] G. Oman, "Elementarily λ-homogeneous binary functions", *Algebra Universalis* **78**:2 (2017), 147–157. MR Zbl

Received: 2020-01-06 Revised: 2020-06-19 Accepted: 2020-08-06

goman@uccs.edu *Department of Mathematics, University of Colorado, Colorado Springs, CO, United States*

jstroud@uccs.edu *Department of Physics, University of Colorado, Colorado Springs, CO, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve
2020 vol. 13 no. 5

Set-valued domino tableaux and shifted set-valued domino tableaux 721
Florence Maas-Gariépy and Rebecca Patrias
The first digit of the discriminant of Eisenstein polynomials as an invariant of totally ramified extensions of p-adic fields 747
Chad Awtrey, Alexander Gaura, Sebastian Pauli, Sandi Rudzinski, Ariel Uy and Scott Zinzer
Counting pseudo progressions 759
Jay Cummings, Quin Darcy, Natalie Hobson, Drew Horton, Keith Rhodewalt, Morgan Throckmorton and Ry Ulmer-Strack
Growth series for graphs 781
Walter Liu and Richard Scott
Peg solitaire in three colors on graphs 791
Tara C. Davis, Alexxis De Lamere, Gustavo Sopena, Roberto C. Soto, Sonali Vyas and Melissa Wong
Disagreement networks 803
Florin Catrina and Brian Zilli
Rings whose subrings have an identity 823
Greg Oman and John Stroud
Simple graphs of order 12 and minimum degree 6 contain K_6 minors 829
Ryan Odeneal and Andrei Pavelescu
Mixed volume of small reaction networks 845
Nida Obatake, Anne Shiu and Dilruba Sofia
Counting profile strings from rectangular tilings 861
Anthony Petrosino, Alissa Schembor and Kathryn Haymaker
Isomorphisms of graded skew Clifford algebras 871
Richard G. Chandler and Nicholas Engel
Eta-quotients of prime or semiprime level and elliptic curves 879
Michael Allen, Nicholas Anderson, Asimina Hamakiotes, Ben Oltsik and Holly Swisher