involve
a journal of mathematics

Rings isomorphic to their nontrivial subrings

Jacob Lojewski and Greg Oman

msp

2018 vol. 11, no. 5

INVOLVE 11:5 (2018)
dx.doi.org/10.2140/involve.2018.11.877

Rings isomorphic to their nontrivial subrings

Jacob Lojewski and Greg Oman

(Communicated by Scott T. Chapman)

Let G be a nontrivial group, and assume that $G \cong H$ for every nontrivial subgroup H of G. It is a simple matter to prove that $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}/\langle p\rangle$ for some prime p. In this note, we address the analogous (though harder) question for rings; that is, we find all nontrivial rings R for which $R \cong S$ for every nontrivial subring S of R.

1. Introduction

The notion of "same structure" is ubiquitous in mathematics. Indeed, the concept appears as early as high school geometry, where congruence of angles and similarity of triangles are studied. One then learns the analogous concept for groups in a first course on modern algebra, where two groups G and H have the same structure if there is a bijection $f : G \to H$ with the property that $f(xy) = f(x)f(y)$ for all $x, y \in G$. Such an f is called an *isomorphism* from G to H; if such an f exists, then we say that G and H are *isomorphic*, and write $G \cong H$. There exist many groups which are isomorphic to a proper subgroup. For example, the group $(\mathbb{Z}, +)$ is isomorphic to $(E, +)$, where E is the subgroup of $\mathbb{Z}$ consisting of the even integers. More generally, since every nontrivial subgroup of an infinite cyclic group is also infinite cyclic, and since every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$, it follows that the group $(\mathbb{Z}, +)$ is inordinately homogeneous in the sense that all nontrivial subgroups are isomorphic.

More generally, a mathematical structure $\mathfrak{M}$ is called *κ-homogeneous* (κ an infinite cardinal of size at most $|\mathfrak{M}|$) provided any two substructures of cardinality κ are isomorphic [Droste 1989; Oman 2009; 2011]. A related mathematical object called a *Jónsson group* is an infinite group G such that every proper subgroup of G has smaller cardinality than G; in this case, note that G is $|G|$-homogeneous. It is well known, see [Scott 1952], that the only abelian Jónsson groups are the quasicyclic groups $\mathbb{Z}(p^\infty)$, p a prime, which is isomorphic to the subgroup of the factor group $\mathbb{Q}/\mathbb{Z}$ consisting of those elements whose order is a power of p.

MSC2010: primary 16B99; secondary 20K99.
Keywords: direct sum, integral domain, polynomial ring, quotient field, reduced ring, zero divisor.

If one does not assume G to be abelian, then the situation becomes much more complicated. Saharon Shelah was the first to construct an example of a *Kurosh monster*, which is a group of size $\aleph_1$ in which all proper subgroups are countable. It is still an open problem to determine whether a Jónsson group of size $\aleph_\omega$ can be shown to exist in Zermelo–Fraenkel set theory with choice (ZFC); we refer the reader to the excellent survey [Coleman 1996] for more details.

Laffey [1974] characterized the countably infinite rings R for which every proper subring of R is finite. An infinite ring R with the property that every proper subring of R has smaller cardinality than R is called a *Jónsson ring*. It is known that any uncountable Jónsson ring is necessarily a noncommutative division ring. The existence of such a ring has yet to be established [Coleman 1996]. It is apparently a very difficult problem to classify all rings R for which $R \cong S$ for every subring S of size $|R|$, since doing so would automatically classify the Jónsson rings. In view of these results, we take a more modest approach in this paper and consider the problem of classifying those nontrivial rings R for which $R \cong S$ for every nontrivial subring S of R.

2. Results

We begin by fixing terminology. First, all rings will be assumed to be associative, but not necessarily commutative or unital. Indeed, commutativity of the rings studied in this paper can be deduced rather quickly (so it need not be assumed), and many important and well-studied classes of rings do not contain an identity. For example, Leavitt path algebras on graphs with infinitely many vertices *never* contain an identity; see [Abrams et al. 2017, Lemma 1.2.12(iv)]. If R is a ring, then a *subring* of R is a nonempty subset S of R which is closed under addition, multiplication, and negatives. It is important to note that in this article, we do *not* require a subring of a unital ring to contain an identity. For the purposes of this note, say that a ring R (respectively, group G) is *homogeneous* if R is nontrivial and $R \cong S$ for all nontrivial subrings S of R (respectively, if G is nontrivial and $G \cong H$ for every nontrivial subgroup H of G).

We begin our investigation by first classifying the homogeneous groups.

Lemma 1. *Let G be a group. Then G is homogeneous if and only if $G \cong \mathbb{Z}/\langle p\rangle$ for some prime p or $G \cong \mathbb{Z}$.*

Proof. Because (by Lagrange's theorem) $\mathbb{Z}/\langle p\rangle$ has no proper, nontrivial subgroups (that is, $\mathbb{Z}/\langle p\rangle$ is *simple*), we see that $\mathbb{Z}/\langle p\rangle$ is trivially homogeneous. As for the additive group $\mathbb{Z}$ of integers, if H is a nontrivial subgroup of $\mathbb{Z}$, then H is an infinite cyclic group; hence $H \cong \mathbb{Z}$. We deduce that $\mathbb{Z}$ is a homogeneous group.

Conversely, suppose that G is a homogeneous group. Let g be a nonidentity element of G. Then $G \cong \langle g\rangle$, and thus G is cyclic. If G is infinite, then $G \cong \mathbb{Z}$.

Thus suppose that G is finite. If H is a proper subgroup of G, then $|H| < |G|$; thus $H \ncong G$. As G is homogeneous, it follows that G is simple. It is well known that the only nontrivial simple abelian groups are the groups $\mathbb{Z}/\langle p\rangle$ where p is a prime. To keep the paper self-contained, we give the argument. We have already noted above that for a prime p, the group $\mathbb{Z}/\langle p\rangle$ is simple. Conversely, suppose that G is simple, and let $g \in G\backslash\{e\}$ be arbitrary. The simplicity of G implies that $G = \langle g\rangle$, and so G is cyclic. Because $\mathbb{Z}$ has proper, nontrivial subgroups, we deduce that G is a finite cyclic group, say of order $n > 1$. It remains to show that n is prime. If $n = rs$ for some integers r and s with $1 < r, s < n$, then $\langle g^r\rangle$ is a proper, nontrivial subgroup of G, contradicting that G is simple. This concludes the proof. □

We arrive at the main result of this note, which classifies the homogeneous rings. As the reader will see, the argument we give to prove the ring version of Lemma 1 is more complicated than the argument just given above.

Theorem 1. *Let R be a ring. Then R is homogeneous if and only if one of the following holds*:

(i) $R \cong \mathbb{F}_p$, *where $\mathbb{F}_p$ is the field of p elements and p is a prime number*,

(ii) $R \cong \mathbb{Z}/\langle p\rangle$ *with trivial multiplication* (*that is*, $xy = 0$ *for all x and y*), *or*

(iii) $R \cong \mathbb{Z}$ *with trivial multiplication.*

Proof. Consider first the field $\mathbb{F}_p$, where p is prime. If S is a nontrivial subring of $\mathbb{F}_p$, then under addition, S is a nontrivial subgroup of $(\mathbb{F}_p, +)$. By Lagrange's theorem, $S = \mathbb{F}_p$, and thus $S \cong \mathbb{F}_p$ as rings. The same argument shows that $\mathbb{Z}/\langle p\rangle$ with trivial multiplication is homogeneous. As for (iii), suppose that S is a nontrivial subring of $\mathbb{Z}$ (with trivial multiplication). Then additively, S is a nontrivial subgroup of $(\mathbb{Z}, +)$. By Lemma 1, $(S, +) \cong (\mathbb{Z}, +)$; let $f : S \to \mathbb{Z}$ be an additive isomorphism. Because the multiplication on $\mathbb{Z}$ is trivial, it follows that f is also a ring isomorphism. We have verified that the rings in (i)–(iii) are homogeneous.

We now work toward establishing the converse. For $m \in \mathbb{Z}$, let $m\mathbb{Z}$ be the subring of $\mathbb{Z}$ consisting of all integer multiples of m. We claim that

$$\text{the ring } m\mathbb{Z} \text{ is not homogeneous for any } m \in \mathbb{Z}. \tag{2-1}$$

If $m = 0$, then $m\mathbb{Z} = \{0\}$; thus is not homogeneous by definition. If $|m| = 1$, then observe that $m\mathbb{Z} = \mathbb{Z} \ncong 2\mathbb{Z}$ since the ring $\mathbb{Z}$ has an identity but the ring $2\mathbb{Z}$ does not. Now suppose that $|m| > 1$. Then $m\mathbb{Z}$ has a nonzero element α (namely m) such that $\alpha^2 = m\alpha$, yet the subring $m^2\mathbb{Z}$ does not possess such an element. To see this, suppose that $\beta \in m^2\mathbb{Z}\backslash\{0\}$ is such that $\beta^2 = m\beta$. We have $\beta = m^2 n$ for some $n \in \mathbb{Z}\backslash\{0\}$. Thus $m^4 n^2 = \beta^2 = m\beta = m(m^2 n)$. But then $mn = 1$, and m is a unit of $\mathbb{Z}$, which is impossible because $|m| > 1$. We conclude that $m\mathbb{Z} \ncong m^2\mathbb{Z}$. This completes the verification of (2-1).

Next, for a nonzero element r of a ring R, let

$$r\mathbb{Z}[r] := \{m_1 r + m_2 r^2 + \cdots + m_k r^k : k \in \mathbb{Z}^+, m_i \in \mathbb{Z}\}$$

be the subring of R generated by r. If $f : r\mathbb{Z}[r] \to R$ is a ring isomorphism, then one can see that $R = f(r)\mathbb{Z}[f(r)]$. Hence:

$$\begin{gathered}\text{If } R \text{ is a homogeneous ring, then } R = r\mathbb{Z}[r] \text{ for some } r \in R\backslash\{0\}.\\ \text{Thus } R \text{ is commutative.}\end{gathered} \tag{2-2}$$

Now let D be a commutative domain with identity $1 \neq 0$, and let $D[X^2, X^3]$ be the ring generated by D, X^2, and X^3, where X is an indeterminate which commutes with the members of D. Consider the ideal $\langle X^2, X^3\rangle$ of $D[X^2, X^3]$ generated by X^2 and X^3. We claim that

$$\langle X^2, X^3\rangle \text{ is not a principal ideal of } D[X^2, X^3]. \tag{2-3}$$

Note first that

$$X \notin D[X^2, X^3], \tag{2-4}$$

lest X be a unit of $D[X]$. Suppose by way of contradiction that $\langle X^2, X^3\rangle = \langle f(X)\rangle$ for some $f(X) \in D[X^2, X^3]$. Then $X^2 \mid f(X)$ and $f(X) \mid X^2$ in the ring $D[X]$. We deduce that $f(X) = uX^2$ for some unit $u \in D$. Because $f(X) \mid X^3$ in the ring $D[X^2, X^3]$, we have $uX^2 g(X) = X^3$ for some $g(X) \in D[X^2, X^3]$. But then $X = u \cdot g(X) \in D[X^2, X^3]$, contradicting (2-4). We have now established (2-3). Next, let $XD[X]$ be the subring of $D[X]$ consisting of all $f(X) \in D[X]$ for which $f(0) = 0$. We prove that

$$XD[X] \text{ is not homogeneous.} \tag{2-5}$$

Suppose otherwise, and let R be the subring of $XD[X]$ generated by X^2 and X^3. Then R is also homogeneous, and by (2-2), there is $f(X) \in R$ such that $R = f(X)\mathbb{Z}[f(X)]$. Next, let I be the ideal of $D[X^2, X^3]$ generated by R. Then it follows that $I = \langle X^2, X^3\rangle = \langle f(X)\rangle$, and we have a contradiction to (2-3) above.

Finally, we are ready to classify the homogeneous rings. Toward this end, let R be an arbitrary homogeneous ring. We shall prove that one of (i)–(iii) holds. Suppose first that R possesses a nonzero nilpotent element α. Let $n > 1$ be least such that $\alpha^n = 0$. Setting $\beta := \alpha^{n-1}$, we have $\beta \neq 0$, yet $\beta^2 = 0$. Let $S := \{m\beta : m \in \mathbb{Z}\}$. One checks at once that S is a nonzero subring of R with trivial multiplication. Because R is homogeneous, $R \cong S$; hence R is a nontrivial ring with trivial multiplication. But then every subgroup of R is a subring of R. The homogeneity of R gives $H \cong K$ for any nontrivial subgroups H and K of $(R, +)$. Applying Lemma 1, we see that either (ii) or (iii) holds.

Thus we assume that

$$R \text{ is reduced; that is, } R \text{ has no nonzero nilpotent elements.} \tag{2-6}$$

Our next assertion is that

$$R \text{ has no nonzero zero divisors.} \tag{2-7}$$

Suppose by way of contradiction that $r_0 \in R\backslash\{0\}$ is a zero divisor. Let $T_1 := r_0\mathbb{Z}[r_0]$ and $S_1 := \{r \in R : rT_1 = \{0\}\}$. We have seen that T_1 is a nonzero subring of R. As R is commutative by (2-2) and r_0 is a zero divisor, S_1 is a *nonzero* subring of R. Because R is reduced, it follows immediately that

$$S_1 \cap T_1 = \{0\}, \qquad \text{and} \qquad xy = 0 \quad \text{for all } x \in S_1 \text{ and } y \in T_1. \tag{2-8}$$

As R is homogeneous, $R \cong S_1$. We conclude that there exist nonzero subrings S_2 and T_2 of S_1 such that $S_2 \cap T_2 = \{0\}$ and $xy = 0$ for all $x \in S_2$ and $y \in T_2$. Continuing recursively and setting $S_0 := T_0 := R$, we obtain sequences $\{S_n : n \geq 0\}$ and $\{T_n : n \geq 0\}$ of nonzero subrings of R such that for every $n \geq 0$, S_{n+1} and T_{n+1} are nonzero subrings of S_n such that $S_{n+1} \cap T_{n+1} = \{0\}$ and $xy = 0$ for all $x \in S_{n+1}$ and $y \in T_{n+1}$. Next, we establish that for all positive integers k,

$$\begin{gathered}\text{if } n_1, \dots, n_k > 0 \text{ are distinct, and } t_1 + \cdots + t_k = 0 \text{ with } t_i \in T_{n_i}, \\ \text{then } t_i = 0 \text{ for } i = 1, \dots, k.\end{gathered} \tag{2-9}$$

To prove this, we induct on k. Note that the base case of the induction is the assertion that if $t_1 = 0$ and $t_1 \in T_{n_1}$, then $t_1 = 0$, which is true. Suppose that the claim holds for some $k > 0$, and let $0 < n_1 < n_2 < \cdots < n_{k+1}$ and $t_1, \dots, t_{k+1}$ be such that $t_1 + \cdots + t_{k+1} = 0$ with $t_i \in T_{n_i}$ for all $1 \leq i \leq k$. One checks that $t_2, \dots, t_{k+1} \in S_{n_1}$; set $\alpha := t_2 + \cdots + t_{k+1}$. Then $t_1 + \alpha = 0$, $t_1 \in T_{n_1}$, and $\alpha \in S_{n_1}$. Since $S_{n_1} \cap T_{n_1} = \{0\}$, it follows that $t_1 = \alpha = 0$. Applying the inductive hypothesis, we see that $t_2 = \cdots = t_{k+1} = 0$, and (2-9) is verified. We further claim that

$$\text{if } 0 < n < m \text{ and } x \in T_n,\ y \in T_m, \text{ then } xy = 0. \tag{2-10}$$

This is straightforward: as above, $y \in S_n$, and the result follows. We deduce from (2-9), (2-10), and the homogeneity of R that R is isomorphic to the internal direct sum of the rings T_n, $n > 0$. More compactly,

$$R \cong \bigoplus_{n>0} T_n. \tag{2-11}$$

Thus $\bigoplus_{n>0} T_n$ is homogeneous. By (2-2), there is $(r_n) := r \in \bigoplus_{n>0} T_n$ such that $\bigoplus_{n>0} T_n = r\mathbb{Z}[r]$. Now, $r_i = 0$ for almost all i. Thus there is a k such that if $r_i \neq 0$, then $i \in \{1, \dots, k\}$. But then for *every* $(\alpha_n) := \alpha \in r\mathbb{Z}[r]$, if $\alpha_i \neq 0$, then $i \in \{1, \dots, k\}$. Since $\bigoplus_{n>0} T_n = r\mathbb{Z}[r]$, we deduce that the same is true of every member of $\bigoplus_{n>0} T_n$. But of course, this is absurd: recall that each T_i is a *nonzero* ring, so for every $k \in \mathbb{Z}^+$ there exists a sequence $(t_n : n \in \mathbb{N}) \in \bigoplus_{n>0} T_n$ such that $t_k \neq 0$. Finally, we have proven (2-7).

We pause to take inventory of what we have established thus far. By (2-2) and (2-7), R is a commutative domain, though we have not yet proven that R has a multiplicative identity. Let

$$K := \{a/b \colon a \in R,\ b \in R \backslash \{0\}\}$$

be the quotient field of R. It is well known that R embeds into K via the map $r \mapsto (rd)/d$, where $d \in R$ is some fixed nonzero element of R. We identity R with its image in K. Now let D be the subring of K generated by 1. Fix some nonzero $r \in R$. One checks at once that $rD[r]$ is a nonzero subring of R, whence

$$R \cong rD[r]. \tag{2-12}$$

The map $\varphi \colon XD[X] \to rD[r]$ defined by $\varphi(Xg(X)) := rg(r)$ is a surjective ring map. We apply (2-12) to conclude that $rD[r]$ is homogeneous. Therefore, (2-5) implies that the kernel of φ is nonzero. Choose a nonzero polynomial $Xf(X) := d_1X + d_2X^2 + \cdots + d_nX^n \in XD[X]$ of minimal degree n for which $rf(r) = 0$. We claim that

$$d_1 \neq 0. \tag{2-13}$$

If $n = 1$, this follows since $Xf(X) \neq 0$. Suppose now that $n > 1$. If $d_1 = 0$, then we have $d_2r^2 + \cdots + d_nr^n = 0$. Recalling that R is a domain and $r \neq 0$, this equation reduces to $d_2r + \cdots + d_nr^{n-1} = 0$, and this contradicts the minimality of n. So we have

$$d_1r + d_2r^2 + \cdots + d_nr^n = 0 \quad \text{and} \quad d_1 \neq 0. \tag{2-14}$$

Viewing the above equation in the quotient field K of R, we may divide through by r to get $d_1 + d_2r + \cdots + d_nr^{n-1} = 0$. Solving the equation for d_1, we see that

$$d_1 \in R. \tag{2-15}$$

Recall that $d_1 \in D$, the ring generated by 1_K (the multiplicative identity of K). Thus $d_1 = m \cdot 1_K$ for some $m \in \mathbb{Z}$. Because K is a field, either $D \cong \mathbb{Z}$ or $D \cong \mathbb{Z}/\langle p \rangle$ for some prime p. In the former case, it follows from (2-13), (2-15), and the homogeneity of R that $R \cong m\mathbb{Z}$ for some $m \in \mathbb{Z}$. However, this is precluded by (2-1). We deduce that $D \cong \mathbb{F}_p$ for some prime p. But then by (2-15), we see that (up to isomorphism) $d_1 \in (\mathbb{F}_p \backslash \{0\}) \cap R$. Applying homogeneity a final time, we see that R is isomorphic to the ring generated by d_1. Thus, as $d_1 \neq 0$, we have $R \cong \mathbb{F}_p$, and the proof is complete. □

We conclude the paper with the following corollary, which characterizes the fields of order p.

Corollary 1. *Let R be a ring with nontrivial multiplication. Then R is a field with p elements* (p *a prime*) *if and only if any two nontrivial subrings of R are isomorphic.*

Acknowledgment

We thank the referee for an extremely thorough reading of our paper and for offering numerous helpful suggestions.

References

[Abrams et al. 2017] G. Abrams, P. Ara, and M. Siles Molina, *Leavitt path algebras*, Lecture Notes in Mathematics **2191**, Springer, 2017. Zbl

[Coleman 1996] E. Coleman, "Jonsson groups, rings and algebras", *Irish Math. Soc. Bull.* 36 (1996), 34–45. MR Zbl

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

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

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

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

[Scott 1952] W. R. Scott, "Groups and cardinal numbers", *Amer. J. Math.* **74** (1952), 187–197. MR Zbl

Received: 2017-08-15 Revised: 2017-11-11 Accepted: 2017-11-20

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

goman@uccs.edu Department of Mathematics, 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 2018 is US $190/year for the electronic version, and $250/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

2018 vol. 11 no. 5

On the minuscule representation of type B_n 721
WILLIAM J. COOK AND NOAH A. HUGHES

Pythagorean orthogonality of compact sets 735
PALLAVI AGGARWAL, STEVEN SCHLICKER AND RYAN SWARTZENTRUBER

Different definitions of conic sections in hyperbolic geometry 753
PATRICK CHAO AND JONATHAN ROSENBERG

The Fibonacci sequence under a modulus: computing all moduli that produce a given period 769
ALEX DISHONG AND MARC S. RENAULT

On the faithfulness of the representation of $\mathrm{GL}(n)$ on the space of curvature tensors 775
COREY DUNN, DARIEN ELDERFIELD AND RORY MARTIN-HAGEMEYER

Quasipositive curvature on a biquotient of $\mathrm{Sp}(3)$ 787
JASON DEVITO AND WESLEY MARTIN

Symmetric numerical ranges of four-by-four matrices 803
SHELBY L. BURNETT, ASHLEY CHANDLER AND LINDA J. PATTON

Counting eta-quotients of prime level 827
ALLISON ARNOLD-ROKSANDICH, KEVIN JAMES AND RODNEY KEATON

The k-diameter component edge connectivity parameter 845
NATHAN SHANK AND ADAM BUZZARD

Time stopping for Tsirelson's norm 857
KEVIN BEANLAND, NOAH DUNCAN AND MICHAEL HOLT

Enumeration of stacks of spheres 867
LAUREN ENDICOTT, RUSSELL MAY AND SIENNA SHACKLETTE

Rings isomorphic to their nontrivial subrings 877
JACOB LOJEWSKI AND GREG OMAN

On generalized MacDonald codes 885
PADMAPANI SENEVIRATNE AND LAUREN MELCHER

A simple proof characterizing interval orders with interval lengths between 1 and k 893
SIMONA BOYADZHIYSKA, GARTH ISAAK AND ANN N. TRENK