VARIATIONS ON A THEME
RINGS SATISFYING $x^3 = x$ ARE COMMUTATIVE

S.M. BUCKLEY AND D. MACHALE

Dedicated to the memory of I.N. Herstein
who wrote a wonderful book called Topics in Algebra.

ABSTRACT. A ring satisfying $x^3 = x$ is necessarily commutative. We consider a variety of weaker forms of this condition and show that many but not all of them imply commutativity. We also present a variety of elementary proofs of the fact that $x^3 = x$ implies commutativity.

1. Introduction

Both of us learned much of our undergraduate algebra from *Topics in Algebra* [9]. Herstein is said to have remarked that one exercise in his book gave rise to more correspondence from readers than all the other items put together. It was Exercise 19^* in Chapter 3.4 on page 136, and it reads as follows:

> Let R be a ring in which $x^3 = x$, for all $x \in R$. Prove that R is a commutative ring.

In this paper we consider various generalizations of this result, and show that many imply commutativity, but for a few of them we give counterexamples. We also present a variety of proofs of the original result. In the spirit of Herstein's book, the emphasis is entirely on self-contained elementary methods, and in particular we can avoid appealing to the powerful Jacobson structure theory for rings. Indeed we claim that this note could profitably be read by a student who has merely encountered the axioms and elementary theory of a ring $(R, +, \cdot)$, and wishes to see their immense versatility in action.

Why present a variety of proofs? We believe that just as it is important to find a single technique that can be used to prove many different theorems, it is often equally important to find many different proofs of the same theorem. There are several reasons for holding this view of which the following are perhaps the most significant.

(a) The more different proofs one has, the more reasons one can see *why* a theorem is true. Additional proofs give a clearer insight into, and understanding of, the result.
(b) Perhaps more importantly, different proofs show the potential for generalizing the theorem in different directions. Furthermore, Proof B may have the potential for establishing a stronger generalization than Proof A.
(c) Examining different proofs of the same result can introduce a student to the much needed topics of esthetics in mathematics and the historical development of the subject. One's first goal should always be to find a valid proof of a result by hook or by crook using all available information and techniques. A valid proof may be long, clumsy, heavy-handed, or tedious. On the other hand, it may be short, clever, slick, or downright beautiful. How else can the quest for a shorter, "better", or more beautiful proof begin unless mathematicians consider many different proofs? The history of mathematics is littered with examples of this phenomenon of revisionist proofs.

2010 *Mathematics Subject Classification.* 16R50.

We use Herstein's definition of a ring, so we do not require it to have a unity element. $(R, +, \cdot)$ is a ring where $x \cdot y$ is written as xy.

R has an additive identity 0, and distributivity implies that $0x = x0 = x$ for all $x \in R$.

$Z(R)$, the *center of* R is $\{x \in R \mid xr = rx \text{ for all } r \in R\}$; $Z(R)$ is a subring of R and $0 \in Z(R)$.

An *idempotent* in R is an element e such that $e^2 = e$, while a *nilpotent* is an element x such that $x^n = 0$ for some $n \in \mathbb{N}$.

A *(ring) commutator* is an element of the form $xy - yx$, and this difference is denoted $[x, y]$. Clearly $[x, y] = 0$ if and only if $xy = yx$, and $[x, y] = -[y, x]$ for all x, y.

We would like to thank the referee for a useful critique of our paper and in particular for suggesting Lemma 6.

2. Results on commutativity with assumptions on second powers

In this section, we consider some commutativity results related to results involving second powers. These results tend to be particularly easy. Most of the results in this section—or more general results that imply these results—can be found in various papers throughout the literature, so we will not attempt to trace the history of each result. Some relevant references include [1], [2], and [12].

Set theory is at the very foundations of mathematics. Suppose A and B are subsets of a nonempty set S, and let us define $A + B$ to be $(A \cup B) \setminus (A \cap B)$ and $A \cdot B$ to be $A \cap B$. It is not difficult to show that $(P(S), +, \cdot)$ is a ring, where $P(S)$ indicates the power set of S. Moreover for every X in this ring, $X^2 = X \cap X = X$; a ring satisfying this equation is said to be *Boolean*, and it is easy to show that a Boolean ring is commutative. The standard proof goes as follows.

Theorem 1. *A Boolean ring is commutative.*

Proof. For all $x \in R$, $-x = (-x)^2 = x^2 = x$, so $x + x = 0$ for all x. Next

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2\,, \qquad \text{for all } x, y \in R\,,$$

Since $(R, +)$ is a group, cancellation gives $xy + yx = 0 = xy + xy$, from above. Again by cancellation we have $xy = yx$, and so R is commutative. □

Theorem 1 has the following well-known generalization which will be useful in the sequel.

Theorem 2. *If $x^2 - x \in Z(R)$, for all $x \in R$, then R is commutative.*

Proof. We have

$$(x + y)^2 - (x + y) = (x^2 - x) + (y^2 - y) + xy + yx \in Z(R)\,,$$

so $xy + yx \in Z(R)$. Then $x(xy + yx) = (xy + yx)x$, so $x^2y + xyx = xyx + yx^2$ and $x^2y = yx^2$. Thus $x^2 \in Z(R)$, so $x^2 - (x^2 - x) = x \in Z(R)$ for all x, and so R is commutative. □

The following variant of Theorem 2 is also useful.

Theorem 3. *If $x^2 + x \in Z(R)$, for all $x \in R$, then R is commutative.*

Proof. Replacing x by $-x$ gives $(-x)^2 - x \in Z(R)$, so $x^2 - x \in Z(R)$, and R is commutative by Theorem 2. □

We note that the conditions of Theorems 2 and 3 are both necessary and sufficient for commutativity, whereas those of Theorem 1 are sufficient but not necessary. Also note that Theorems 2 and 3 can be expressed in commutator form.

Theorem 4. *A ring is commutative if and only if $[x^2, y] = [x, y]$, for all $x, y \in R$.*

Proof. If R is commutative, then $[x^2, y] = 0 = [x, y]$, as required. For the converse, we use the fact that $[a, c] \pm [b, c] = [a \pm b, c]$ (as can be easily verified by expansion of both sides). Thus the equation $[x^2, y] = [x, y]$ can be rewritten as $[x^2 - x, y] = 0$ for all x, y, which implies that $x^2 - x \in Z(R)$ for all x. □

Since $[x, y] = -[y, x]$, we can similarly write Theorem 3 in the following form.

Theorem 5. *A ring is commutative if and only if $[x^2, y] = [y, x]$, for all $x, y \in R$.*

Idempotents play an important role in ring commutativity theorems, often because of the following technical lemma.

Lemma 6. *If e is idempotent in a ring R, then $(ey - eye)^2 = 0 = (ye - eye)^2$ for all $y \in R$.*

Proof. Simply expand and use idempotency:

$$(ey-eye)^2 = (ey)^2+(eye)^2-(ey)(eye)-(eye)(ey) = (ey)^2+(ey)^2e-(ey)^2e-(ey)^2 = 0\,.$$

The second part of the assertion is proved similarly. □

In a Boolean ring R, every element is an idempotent, so Lemma 6 tells us that $xy - xyx = 0 = yx - xyx$ for all $x, y \in R$, which yields a different proof of Theorem 1. An advantage of this new proof is that the following improvement of Theorem 1 also follows immediately.

Theorem 7. *Let R be a ring in which $x^2 = 0$ implies $x = 0$. If $e \in R$ is an idempotent, then $e \in Z(R)$.*

Proof. Since $(ey - eye)^2 = (ye - eye)^2 = 0$, we have $ey - eye = ye - eye = 0$ for all $y \in R$. Thus $ey = ye$ and $e \in Z(R)$. □

Actually the condition that $x^2 = 0$ implies $x = 0$ is equivalent to the condition that R has no nonzero nilpotents. It is obvious that the absence of nonzero nilpotents implies that if $x^2 = 0$ then $x = 0$. Conversely suppose $x = 0$ whenever $x^2 = 0$, and suppose that $r \in R$ is such that $r^n = 0$ for some $n > 1$. Let t be the smallest power of two greater than or equal to n, so that $x^t = 0$ also. Since $x^2 = 0$ implies $x = 0$, we deduce that $r = 0$ by successively halving t.
[For instance if $r^{13} = 0$, then $r^{16} = 0$ and so we deduce in turn that r^8, r^4, r^2, and finally r, must equal 0.]

Note that both $er - ere = eer - ere = [e, er]$ and $re - ere = [re, e]$ are commutators, so we can now state:

Theorem 8. *Let R be a ring that has no nonzero nilpotent commutators. If $e \in R$ is an idempotent, then $e \in Z(R)$.*

The condition that idempotents are central is so useful, that we mention some other conditions under which it holds.

Theorem 9. *Let R be a ring in which $xy = 0$ implies $yx = 0$. If e is an idempotent in R, then $e \in Z(R)$.*

Proof. For all $r \in R$, $e(r - er) = er - eer = er - er = 0$, so $(r - er)e = 0$, and so $re = ere$. By considering $(r - re)e$, we similarly deduce that $er = ere$. Thus $er = re$ and so $e \in Z(R)$. □

Note that Theorem 7 follows from Theorem 9 by virtue of the fact that

Condition A: $x^2 = 0$ implies $x = 0$

implies

Condition B: $xy = 0$ implies $yx = 0$

because if Condition A holds and $xy = 0$, then $(yx)^2 = y(xy)x = 0$, and so $yx = 0$.

However Condition B does not always imply Condition A: in $\mathbb{Z}_4$, the ring of residues mod 4, $xy = 0$ implies $yx = 0$ (since $\mathbb{Z}_4$ is commutative), but $2^2 = 0$ while $2 \neq 0$.

Theorem 7 can be strengthened in the following manner.

Theorem 10.
(a) Let R be a ring in which $x^2 = 0$ implies $x \in Z(R)$. Then all idempotents are central.
(b) Let R be a ring in which $xy \in Z(R)$ implies $yx \in Z(R)$. Then all idempotents in R are central.

Proof. For (a), we again use Lemma 6 to deduce that $er - ere \in Z(R)$ if e is idempotent and $r \in R$. Thus $e(er - ere) = (er - ere)e = 0$, and so $er = ere$. Similarly $re = ere$ and so $e \in Z(R)$. For (b), we have $(er - ere)e = 0 \in Z(R)$ and so $e(er - ere) = er - ere \in Z(R)$, yielding the result as in (a). □

3. Variations on a theme

In this section, we study rings satisfying the identity $x^3 = x$. Trivially Boolean rings satisfy the identity $x^3 = x$. The reverse implication is false, as evidenced by the ring of residue classes mod 6, $(\mathbb{Z}_6, +, \cdot)$, which is of course commutative and satisfies the identity $x^3 = x$, but not the identity $x^2 = x$.

However, the next result emphasizes the fact that rings satisfying $x^3 = x$ for all x are quite special.

Theorem 11. *Let R be a ring in which $x^3 = x$ for all $x \in R$. Then $6x = 0$ for all $x \in R$.*

Proof. We have $2x = (2x)^3 = 8x^3 = 8x$, so $6x = 0$. □

The next result will be crucial for proving commutativity of rings satisfying $x^3 = x$.

Theorem 12. *Let R be a ring in which $x^3 = x$ for all $x \in R$. Then $x^2 \in Z(R)$ for all $x \in R$.*

Proof. Suppose that $x^2 = 0$ for some $x \in R$. Then $x = x^3 = x^2 \cdot x = 0$ so $x^2 = 0$ implies $x = 0$. By Theorem 7, all idempotents are central. But $(x^2)^2 = x^4 = x^3 \cdot x = x \cdot x = x^2$. Thus x^2 is an idempotent, and so central, for all $x \in R$. □

We are now ready to give a variety of proofs of the following result.

Theorem 13. *Let R be a ring in which $x^3 = x$ for all $x \in R$. Then R is commutative.*

Proof 1. Let $x, y \in R$. Expansion of the equation $(x + y)^3 = x + y$ gives

$$x^2y + xyx + yx^2 + y^2x + yxy + xy^2 = 0$$

Putting $-y$ in place of y gives

$$-x^2y - xyx - yx^2 + y^2x + yxy + xy^2 = 0$$

Adding we get

$$2y^2x + 2yxy + 2xy^2 = 0 \in Z(R)\,,$$

and so

$$(2y^2x + 2yxy + 2xy^2)y = y(2y^2x + 2yxy + 2xy^2)\,.$$

After simplification and cancellation this reduces to $2xy^3 = 2y^3x$ or $(2x)y = y(2x)$. Hence $2x \in Z(R)$ for all $x \in R$.

Now for each $x \in R$,

$$x^2 + x = (x^2 + x)^3 = x^6 + 3x^5 + 3x^4 + x^3 = x^2 + 3x + 3x^2 + x = 4(x^2 + x)\,,$$

which implies that $3(x^2 + x) = 0 \in Z(R)$. But by the above $2(x^2 + x) \in Z(R)$, so subtraction gives $x^2 + x \in Z(R)$. By Theorem 3, R is commutative. □

Proof 2. As in Proof 1, we have

$$2y^2x + 2yxy + 2xy^2 = 0\,.$$

If we multiply on the left by y, we get

$$2(y^3x + yxy^2 + y^2xy) = 0$$

while if we multiply instead on the right by y, we get

$$2(y^2xy + xy^3 + yxy^2) = 0$$

Subtracting we get $2yx = 2xy$, so $2(xy - yx) = 0$.

As in Proof 1, $3(x^2 + x) = 0$, so

$$0 = 3((x + y)^2 + (x + y)) = 3((x^2 + x) + (y^2 + y) + (xy + yx))\,.$$

Thus $3(xy + yx) = 0$. But $6yx = 0$ by Theorem 11, so $3(xy - yx) = 0$. Combining this with $2(xy - yx) = 0$, we get $xy - yx = 0$, so R is commutative.
[This proof has been attributed to Hanna Neumann [14], but the source is unknown.] □

Proof 3. By Theorem 12, $(x^2 + x)^2 \in Z(R)$, so $x^4 + 2x^3 + x^2 = 2(x^2 + x) \in Z(R)$. As in Proof 1, $3(x^2 + x) \in Z(R)$. Thus $x^2 + x = 3(x^2 + x) - 2(x^2 + x) \in Z(R)$. By Theorem 3, R is commutative.
[This is a "y-less" proof in the sense that we do not have to expand expressions involving both x and y. However it depends on Theorem 3 which does involve both x and y.] □

Proof 4. As in Proofs 1 and 2, we have $2(xy-yx) = 0$ for all x, y. Also $3(x^2+x) = 0$ and so $3x^2 = 3x$ since $6x = 0$. Now consider $T = \{3x \mid x \in R\}$. It can easily be seen that T is a subring of R since $3a \pm 3b = 3(a \pm b)$ and $(3a)(3b) = 9ab = 3(3ab)$. Now for $t \in T$,

$$t^2 = (3x)^2 = 9x^2 = 3x^2 = 3x = t\,.$$

Thus T is a Boolean ring and so is commutative. Thus $(3x)(3y) = (3y)(3x)$, so $9(xy - yx) = 0$. Since also $2(xy - yx) = 0$, we deduce that $xy - yx = 0$ and so R is commutative. □

Proof 5. By Theorem 12, all squares lie in the center of R, so R satisfies the identities $x^3 = x$ and $x^2y = yx^2$. Thus

$$yx = (yx)^3 = y(xy)^2x = (xy)^2yx = xyxyyx = xyxxyy = xyx^2y^2 = x^3y^3 = xy\,.$$ □

Proof 6. In this proof we exploit the fact that R satisfies the condition $ab = 0 \Rightarrow ba = 0$. Now

$$0 = yx - yx = yx - y^3x = y(x - y^2x)\,.$$

Thus

$$(x - y^2x)y = 0 = x^2(x - y^2x)y = x^3 - x^2y^2xy$$

so $xy = x^2y^2xy$. Thus

$$\begin{aligned} 0 &= x^2y^2xy - xy = x^2y^2xy - (xy)^3 = [x(xy - yx)yx]y = [yx(xy - yx)]yx \\ &= (yx)^2(xy - yx) = (xy - yx)(yx)^2 = (xy - yx)(yx)^3 = (xy - yx)yx\,. \end{aligned}$$

Finally,

$$(xy - yx)^2 = (xy - yx)xy - (xy - yx)yx = -(yx - xy)xy - (xy - yx)yx = 0\,,$$

and R is commutative.
[This proof is based on a proof of Ted Herman [4].] □

Our final proof is perhaps the slickest.

Proof 7. $(x^2+x)^2 \in Z(R)$, so $x^4+2x^3+x^2 \in Z(R)$, and so $2x^3 = 2x \in Z(R)$. Also $x^2+x = (x^2+x)^3 = x^6+3x^5+3x^4+x^3$, so $3x+3x^2 = 0 \in Z(R)$. But $3x^2 \in Z(R)$, and so $3x \in Z(R)$. Since also $2x \in Z(R)$, R is commutative.
[This is a completely "y-less" proof depending only on Theorem 7.] □

Many variations on the above proofs are possible, and we would be pleased to hear from readers who have other proofs. Other proofs in the literature include those in [1], [3], and [11].

4. Generalizations

Proof 5 of Theorem 13 verbatim yields the following result since that proof does not use the additive operation in R.

Theorem 14. *If $(S,\cdot)$ is a semigroup which satisfies the identities $x^3 = x$ and $x^2y = yx^2$ for all $x, y \in S$, then S is commutative.*

Theorem 15. *Let R be a ring such that $(xy)^3 = xy$ for all $x, y \in R$. Then R is commutative.*

Proof. Putting $x = y$ we get $x^6 = x^2$. If $yx = 0$ then $x(yx)^2y = 0$, and so $xy = (xy)^3 = 0$. Thus idempotents are central and, since $((xy)^2)^2 = (xy)^2$, we have $(xy)^2 \in Z(R)$. Putting $x = y$, we have $x^4 \in Z(R)$. Now $(x^2\cdot x)^3 = x^2\cdot x$, so $x^9 = x^3$, and so $x^{12} = x^6 = x^2$. Thus $x^{12} = x^4 = x^2$, so $x^2 \in Z(R)$. As in [13], this implies that $(xy)^2 = (yx)^2$ since

$$\begin{aligned}(xy)^2 = x(yxy) &= x[(yx)^2 + y^2 - (yx-y)^2 - y^2x] \\ &= [(yx)^2 + y^2 - (yx-y)^2 - y^2x]x = (yxy)x = (yx)^2\,.\end{aligned}$$

Next $[x(x^2+x)]^3 = x(x^2+x)$, or $[x^3+x^2]^3 = x^3+x^2$, gives $3x^8+3x^7 = 0$, and so $3x^2+3x^3 = 0$. In particular, $3(xy)^2+3(xy)^3 = 0$ and, since $3(xy)^2 \in Z(R)$, we conclude that $3xy \in Z(R)$.

Now $[x(x+y)]^2 = [(x+y)x]^2$, or $(x^2+xy)^2 = (x^2+yx)^2$. Using $(xy)^2 = (yx)^2$ and the centrality of squares, this reduces to $2x^3y = 2yx^3$, so $2x^3 \in Z(R)$. Thus $2xy = 2(xy)^3 \in Z(R)$. But $3xy \in Z(R)$ from above, so $xy \in Z(R)$. Since all products are central, we deduce that

$$xy = (xy)^3 = x(yxyxy) = (yxyxy)x = (yx)^3 = yx\,.$$ □

Rings satisfying $x^3 = x$ for all x are not just commutative rings, but rather special commutative rings. However this condition can be weakened to give necessary and sufficient conditions for commutativity in rings. We now state and prove two such theorems.

Theorem 16. *A ring R is commutative if and only if $x^3 - x \in Z(R)$, for all $x \in R$.*

Theorem 16 is of course equivalent to the following:

Theorem 16′ *A ring R is commutative if and only if $[x^3, y] = [x, y]$, for all $x, y \in R$.*

"Taking the exponent 3 outside" in this last result gives us another theorem:

Theorem 17. *A ring R is commutative if and only if $[x, y]^3 = [x, y]$, for all $x, y \in R$.*

Proof of Theorem 16. We define $f(x) = x^3 - x$. Clearly all commutative rings satisfy $f(x) \in Z(R)$, so it suffices to show that rings satisfying $f(x) \in Z(R)$ for all x, are commutative.

Suppose therefore that $f(x) \in Z(R)$, $x \in R$. Expanding and simplifying

$$f(x+y) - f(x-y) - 2f(y) \in Z(R)$$

gives $A = 2(x^2y + xyx + yx^2) \in Z(R)$. Now $Ax = xA$ simplifies to $y(2x^3) = (2x^3)y$. Thus $2x^3 \in Z(R)$ and so $2x^3 - 2f(x) = 2x \in Z(R)$.

Expanding and simplifying $f(x+x^4)-f(x)-f(x^4) \in Z(R)$, we get $3(x^6+x^9) \in Z(R)$. Since $2y \in Z(R)$ for all $y \in R$, we deduce that $x^6+x^9 \in Z(R)$. Simplifying $x^6+x^9-f(x^2)-f(x^3)-f(x) \in Z(R)$, we see that $x+x^2 \in Z(R)$. Now Theorem 3 implies that R is commutative. □

Before proving Theorem 17, we give some preliminary results. For brevity, we say that a ring R is a *C(3) ring* if $[x,y]^3 = [x,y]$ for all $x, y \in R$.

Theorem 18. *Suppose R is a C(3) ring. Then*

(a) R has no nonzero nilpotent commutators.
(b) If $xy = 0$ in R, then $yx = 0$ also.
(c) Idempotents in R are central. In particular, $[x,y]^2$ is a central idempotent.

Proof. By induction we see that $[x,y] = [x,y]^n$ for every odd $n \in \mathbb{N}$. This clearly rules out the possibility of a nonzero nilpotent commutator.

As for (b), if $xy = 0$ then $[y,x] = yx$ so $yx = (yx)^3 = y(xy)(xyx) = 0$. The first statement in (c) follows from Theorem 8 (or Theorem 9). As for the second part of (c), note that $([x,y]^2)^2 = [x,y] \cdot [x,y]^3 = [x,y]^2$, so $[x,y]^2$ is idempotent. □

Our next result reduces the task of proving Theorem 17 to proving commutativity in a special case.

Theorem 19. *If $[x,z]$ and $[y,z]$ commute for all x, y, z in a ring R, then $[x,y]^4 = 0$ for all $x, y \in R$. In such a ring R, a commutator c satisfies an equation of the form $c^n = c$ for some $n > 1$ if and only if $c = 0$.*

Proof. Suppose $c = [x,y]$ for some $x, y \in R$. Note that $cx = [x, yx] = [-yx, x]$ and $c = [-y, x]$ so, by assumption, cx and c commute. Thus $xc^2 = cxc$, and similarly $yc^2 = cyc$. Since $yc = [yx, y] = [-y, yx]$, we see that yc and cx commute. Thus

$$(cx)(yc)c = (yc^2)xc = cy(cxc) = cyxc^2\,,$$

where in each case the parentheses enclose one or both factors that are commuted in the next equation. Subtracting the extreme right hand side from the extreme left, we get that $c^4 = 0$, as required.

Since $3n-2 \geq 4$, we deduce that $c^{3n-2} = 0$ for all $n > 1$. If $c^n = c \cdot c^{n-1} = c$, then $0 = c^{3n-2} = c^{2n-1} = c^n = c$. □

We are now ready to prove Theorem 17.

Proof of Theorem 17.
Clearly all commutative rings are C(3) rings, since all commutators are zero, so it suffices to prove that C(3) rings are commutative. Suppose therefore that R is a C(3) ring. In view of Theorem 19, it suffices to prove that $[c,d] = 0$ whenever $c = [x,z]$ and $d = [y,z]$, for some $x, y, z \in R$. We split the remainder of the proof into two parts.

Part 1: Reduction to a ring with special properties.
Suppose for the sake of contradiction that a given pair c, d of this type do not commute.

Note that $c^2, d^2 \in Z(R)$ by Theorem 18(c). Let

$$x' = c^2d^2x\,, \quad y' = c^2d^2y\,, \quad z' = c^2d^2z\,, \quad c' = c^2d^2c = cd^2\,, \quad d' = c^2d^2d = dc^2\,.$$

Now x', y' both lie in the subring $R' := c^2d^2R = Rc^2d^2$. (Actually R' is an ideal, but we do not need this.) Furthermore, c', d' are commutators in R', since $c' = [x', z']$ and $d' = [y', z']$, and c', d' fail to commute since

$$[c', d'] = (cd^2)(dc^2) - (dc^2)(cd^2) = c^3d^3 - d^3c^3 = [c,d]\,.$$

It is clear that $(c')^2 = (d')^2 = c^2d^2$ acts as a unity in R'.

Note that $c' \pm d'$ is also a commutator. Moreover $[c', c' \pm d'] = \pm[c', d']$ and $[d', c' \pm d'] = -[c, d]$, so $(c' \pm d')^2$ is absorbed by $[c', d'] = [c, d]$ in the same way as $(c')^2$ and $(d')^2$ were. Thus if we define

$$e := (c' + d')^2(c' - d')^2(c')^2(d')^2\,, \quad f := ec\,, \quad g := ed\,,$$

then we can reduce the task to getting a contradiction from the non-commutativity of f and g. Note that f, g lie in the subring $S := eR = Re$, and that e is a nonzero unity for S with $f^2 = g^2 = (f + g)^2 = (f - g)^2 = e$.

Part 2: C(3) rings are commutative.
Now $(f + g)^2 = e$, and by expansion we see that

$$-e = (f + g)^2 - 2e = f^2 + g^2 + fg + gf - 2e = fg + gf\,. \tag{20}$$

A similar expansion of $e = (f - g)^2$ implies that $fg + gf = e$, and hence $2e = 0$. It follows that $2s = 0$ for all $s \in S$. Next note that $(fg + fgf)f = fgf + fg$, so $(fg+fgf)(e+f) = 0$. By Theorem 18(b), $(e+f)(fg+fgf) = fg+fgf+g+gf = 0$. Using (20), we get $fgf = e + g$ and, by multiplying on the left by f, we get $gf = f+fg$. Combining this last equation with (20) we get $f = e$, and by symmetry $g = e$, which contradicts $e = fg + gf$. □

We now consider some variations of the above commutativity conditions that fail to imply commutativity. Since we were able to weaken $x^3 = x$ to $(xy)^3 = xy$ and still deduce commutativity, one might hope that it could be weakened further to $(xyz)^3 = xyz$. However we see now that even the stronger condition $(xyz)^2 = xyz$ does not guarantee commutativity.

Theorem 21. *There exist noncommutative rings R that satisfy the equation $(xyz)^2 = xyz$ for all $x, y, z \in R$.*

Proof. Consider the ring R of 3×3 matrices of the form

$$x = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}\,, \qquad a, b, c \in \mathbb{R}\,.$$

Then R is not commutative: for instance

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \neq \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\,.$$

However it is readily verified that $xyz = 0$ for all $x, y, z \in R$. □

We mention without proof a more advanced example which can also be used to deduce Theorem 21. First define $\mathbb{H}_9$, the ring consisting of formal sums $a \cdot 1 + bi + cj + dk$ of quaternions with coefficients in $\mathbb{Z}_9$, i.e. $(\mathbb{H}_9, +)$ is a direct sum of four copies of $\mathbb{Z}_9$, and multiplication is defined as we would expect: for instance, $(bi)(cj) = (bc)k$, where bc is a $\mathbb{Z}_9$ product. If we now define a new multiplication $\odot$ by the rule $x \odot y = 3xy$, then $(\mathbb{H}_9, +, \odot)$ is a non-commutative ring satisfying the equation $x \odot y \odot z = 0$ for all $x, y, z \in R$.

Since both of the conditions $x^3 - x \in Z(R)$ and $(xy)^3 = xy$ imply commutativity, one might hope that $(xy)^3 - xy \in Z(R)$ would imply commutativity. Alternatively since $(xy - yx)^3 = xy - yx$ implies commutativity, one might hope that

$$(xy - yx)^3 - (xy - yx) \in Z(R)$$

would imply commutativity. However neither of these implications work, since even the stronger condition $xy \in Z(R)$ does not guarantee commutativity.

Theorem 22. *There exist noncommutative rings R such that $xy \in Z(R)$ for all $x, y \in R$.*

Proof. The same ring R as in the proof of Theorem 21 suffices. It is readily verified that every product xy has the form

$$\begin{pmatrix} 0 & 0 & d \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad d \in \mathbb{R},$$

and that such matrices lie in $Z(R)$. □

As before, a more advanced example with quaternions can be used to prove the above theorem. Define $(\mathbb{H}_8, +, \cdot)$, the ring of quaternions over $\mathbb{Z}_8$, in a manner analogous to the earlier definition of $(\mathbb{H}_9, +, \cdot)$. By defining $x \odot y = 2xy$, we get a noncommutative ring $(\mathbb{H}_8, +, \odot)$ in which all products are central. We leave the details to the reader.

We remark that the problem of showing that a ring satisfying $x^3 = x$ is commutative has been used as a test example for computer algorithms which use rewrite rules and reduction theory for polynomial rings in non-commuting variables. What the machine programs lack in subtlety, they make up for in persistence, often negotiating hundreds of steps until the equation $xy - yx = 0$ is achieved. For details, see [15].

Finally, we note that much stronger versions of Theorems 13, 16, and 17 can be proved using the structure theory of rings. Jacobson [10] proved that rings satisfying $x^{n(x)} = x$ for all $x \in R$ are commutative; see also [7]. Herstein also proved using structure theory that if $x^{n(x)} - x \in Z(R)$ for all $x \in R$, or if $[x, y]^{n(x,y)} = [x, y]$ for all $x, y \in R$, then R is commutative; see [5] and [6]. In all these results, $n(x)$ and $n(x, y)$ can be any integers greater than 1. We recommend [8] for an account of structure theory, and proofs of results of this type.

References

[1] R. Ayoub, C. Ayoub, *On the commutativity of rings*, Amer. Math. Monthly **71** (1964), 267–271.

[2] H.E. Bell, *Certain near-rings are rings*, J. London Math. Soc. (2) **4** (1971), 264–270.

[3] R. Gross, post on `sci.math` (22 December 1993); included in `http://www.mathematik.uni-bielefeld.de/~sillke/PUZZLES/herstein` (18 September 2011).

[4] T. Herman, *On a theorem of Jacobson*, in Beauty is our Business: A birthday salute to Edsger W. Dijkstra, Eds. W.H.J. Feijen, A.J.M. van Gasteren, D. Gries, J. Misra, Texts and Monographs in Computer Science, 1990, Sect. 20, 176–181.

[5] I.N. Herstein, *A generalization of a theorem of Jacobson III*, Amer. J. Math. **75** (1953), 105–111.

[6] I.N. Herstein, *A condition for the commutativity of rings*, Canad. J. Math. **9** (1957), 583–586.

[7] I.N. Herstein, *Wedderburn's theorem and a theorem of Jacobson*, Amer. Math. Monthly **68** (1961), 249–251.

[8] I.N. Herstein, Noncommutative rings, Carus Mathematical Monographs, Mathematical Association of America, Washington, DC, 1968.

[9] I.N. Herstein, Topics in Algebra, 2nd edition, John Wiley and sons, New York, 1975.

[10] N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. Math. **46** (1945), 695–707.

[11] J. Luh, *An elementary proof of a theorem of Herstein*, Math. Mag. **38** (1965), 105–106.

[12] D. MacHale, *Rings that are nearly Boolean*, Proc. Roy. Irish Acad. Sect. A **80** (1980), 41–46.

[13] D. MacHale and M. Ó Searcóid, *Two Elementary Generalizations of Boolean Rings*, Amer. Math. Monthly **93** (1986), 121–122.

[14] A. van der Poorten, *Concerning computing*, letter in Austral. Math. Soc. Gaz. **21** (1994), 68.

[15] J.J. Wavrik, *Commutativity Theorems: Examples in Search of Algorithms* in: ISSAC '99 Proceedings of the 1999 international symposium on Symbolic and algebraic computation (1999), 31–36.

S.M. Buckley:
Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.
E-mail address: stephen.buckley@maths.nuim.ie

D. MacHale:
School of Mathematical Sciences, University College Cork, Cork, Ireland.
E-mail address: d.machale@ucc.ie