

Rings with ideal centres

STEPHEN M. BUCKLEY AND DESMOND MACHALE

October 23, 2012

ABSTRACT. We discuss the condition that the centre of a ring is an ideal. We also show that some classical commutativity results of Jacobson and Herstein have elementary proofs under the added assumption that the centre is an ideal.

1 Introduction Since in a group G , the centre $Z(G)$ is always a normal subgroup, one might expect that the centre $Z(R)$ of a ring would be a (two-sided) ideal in R . This is not true in general, though it can be true in some cases: at one extreme, it is trivially true if R is commutative, and at the other extreme it is also trivially true if R is “extremely non-commutative” in the sense that $Z(R) = \{0\}$. Thus rings where it fails to hold are in some sense “moderately non-commutative”. We say that a ring R has an *ideal centre* if its centre is an ideal.

One of the main aims of this paper is to show that some classical ring commutativity results of Jacobson and Herstein, which we now state, have elementary proofs if we restrict to rings with ideal centres. Jacobson [12] proved that rings R satisfying an identity of the form $x^{n(x)} = x$ are commutative. Rings satisfying such an identity are rather special, but Herstein showed that commutativity is equivalent to the weaker condition $x^{n(x)} - x \in Z(R)$; see [9]. Herstein then generalized this result further:

Theorem A (Herstein [10]). *A ring R is commutative if and only if for each $x \in R$ there exists $f(X) \in X^2\mathbb{Z}[X]$ such that $f(x) - x \in Z(R)$.*

In the above result, $f(X) \in X^2\mathbb{Z}[X]$ means that $f(X)$ is a formal polynomial with integer coefficients (in the indeterminate X) which is formally divisible by X^2 . We view f as a function on R in the natural way.

Subsequently, Herstein gave the following quite different generalization of Jacobson’s theorem; here and later, $[x, y] = xy - yx$ is the *commutator* of x and y .

Theorem B (Herstein [11]). *A ring R is commutative if and only if for each $x, y \in R$ there exists an integer $n(x, y) > 1$ such $[x, y]^{n(x, y)} = [x, y]$.*

Known proofs of Theorems A and B require Jacobson’s structure theory of rings, but we give elementary proofs of the following variants of these results.

Theorem 1. *A ring R with ideal centre is commutative if and only if for each $x \in R$ there exists $f(X) \in X^2\mathbb{Z}[X]$ such that $f(x) - x \in Z(R)$.*

Theorem 2. *The following conditions are equivalent for rings R with ideal centres.*

- (a) R is commutative.
- (b) For each $x, y \in R$ there exists an integer $n(x, y) > 1$ such $[x, y]^{n(x, y)} = [x, y]$.

(c) For each $x, y \in R$ there exists $f(X) \in X^2\mathbb{Z}[X]$ such that $f([x, y]) = [x, y]$.

Obviously Theorem 1 follows immediately from Theorem A, and the equivalence of (a) and (b) in Theorem 2 follows immediately from Theorem B, so the important feature of these results is that our proofs avoid structure theory. We do not however know of any proof that condition (c) in Theorem 2 implies commutativity for general rings.

We can view the above theorems as stating in particular that a polynomial $g(X) \in X\mathbb{Z}[X]$ whose X -coefficient equals ± 1 “forces” commutativity of R if $g(R) = 0$ (meaning that $g(x) = 0$ for all $x \in R$), or more generally $g(R) \subseteq Z(R)$ (meaning that $g(x) \in Z(R)$ for all $x \in R$), or $g([R, R]) = 0$ (meaning that $g([x, y]) = 0$ for all $x, y \in R$). The following result classifies the polynomials that force rings with ideal centre to be commutative in any of these three senses.

Theorem 3. Let $g(X) := \sum_{i=1}^n a_i X^i \in \mathbb{Z}[X]$. Then

(a) All rings R with ideal centre satisfying $g(R) = 0$ are commutative if and only if either:

(i) $a_1 = \pm 1$, or

(ii) $a_1 = \pm 2$, a_2 is odd, and $a_2 + a_3 + \cdots + a_n$ is odd.

(b) All rings R with ideal centre satisfying $g(R) \subseteq Z(R)$ are commutative if and only $a_1 = \pm 1$.

(c) All rings R with ideal centre satisfying $g([R, R]) = 0$ are commutative if and only $a_1 = \pm 1$.

Each part of the above result follow easily from the corresponding results without the ideal centre assumption; for these, see the main theorem in [13] for (a), [5, Proposition 4] for (b), and [6, Theorem 2] for (c). Thus the main value of these parts of Theorem 3 is again that the proof is elementary, although (c) also lead to the investigation of [6, Theorem 2].

We prove Theorems 1–3 in Section 3, but first in Section 2 we give some examples of noncommutative rings in which the centre is an ideal, and also answer the following pair of questions:

What is the order of the smallest finite ring/non-unital ring whose centre is not an ideal?

2 Examples The concept of a ring with an ideal centre is mainly of interest for non-unital rings, since clearly a unital ring has an ideal centre if and only if it is commutative.

If we define a *good example* of a ring R with an ideal centre to be one where $Z(R)$ is both nonzero and proper, then all good examples are non-unital. The following pair of propositions give some families of good examples. In these propositions and later, $M(n, l, r, R_0)$ is the ring of $n \times n$ matrices $A = (a_{i,j})$ over a base ring R_0 such that $a_{i,j} = 0$ if $i > n - l$ or $j \leq r$, and $U(n, m, R_0)$ is the ring of $n \times n$ matrices $A = (a_{i,j})$ over R_0 such that $a_{i,j} = 0$ if $j < i + m$. We use the more common notation $M(n, R_0)$ and $U(n, R_0)$ in place of $M(n, 0, 0, R_0)$ and $U(n, 0, R_0)$, respectively.

Proposition 4. Suppose R_0 is a commutative unital ring with $1 \neq 0$, and that $n, l, r \in \mathbb{N}$ satisfy $n \geq 3$ and $l + r < n$. Then $R := M(n, l, r, R_0)$ is non-commutative, and $Z(R) = M(n, n - r, n - l, R_0)$ is a nontrivial proper ideal in R .

Proof. Let $S := M(n, n-r, n-l, R_0)$. Because $n > n-r > l$ and $n > n-l > r$, it is clear that S is a proper and nontrivial subring of R . Let $\Sigma \in M(n, R_0)$ be the matrix corresponding to the shift map $(x_1, \dots, x_n) \mapsto (x_2, \dots, x_n, 0)$ in R_0^n , so that $\Sigma = (\sigma_{i,j})$, where

$$\sigma_{i,j} = \begin{cases} 1, & \text{if } 2 \leq j = i+1 \leq n, \\ 0, & \text{otherwise.} \end{cases}$$

Note that $R = \Sigma^l M(n, R_0) \Sigma^r$. Since the matrix Σ^n corresponds to the zero map and $S = \Sigma^{n-r} M(n, R_0) \Sigma^{n-l}$, it follows that $AB = BA = 0$ whenever $A \in R$ and $B \in S$. Thus S is an ideal and $S \subseteq Z(R)$.

Taking $A = (a_{i,j}) \in R \setminus S$, it remains to show that $A \notin Z(R)$. For $1 \leq i, j \leq n$, define $M_{i,j} \in M(n, R_0)$ to be the matrix whose (i, j) th entry is 1 and all other entries are 0. Suppose first that $a_{p,q} \neq 0$ for some $1 \leq p, q \leq n$ such that $p > r$. Now $B = M_{1,p} \in R$ and $\Sigma B = 0$, so $AB = 0$. On the other hand, the $(1, q)$ th entry of BA is $a_{p,q}$ so $BA \neq 0$. Thus $A \notin Z(R)$.

The other way that A can fail to be in S is if $a_{p,q} \neq 0$ for some $1 \leq p, q \leq n$ such that $q \leq n-l$. Now $B = M_{q,n} \in R$ and $B\Sigma = 0$, so $BA = 0$. On the other hand, the (p, n) th entry of AB is $a_{p,q}$, so $AB \neq 0$. Thus again $A \notin Z(R)$, and we are done. \square

The equation $Z(R) = M(n, n-r, n-l, R_0)$ proved above, and the fact that $Z(R)$ is an ideal, is true under weaker assumptions on n, l, r : it suffices that $n \geq 2$ and $0 < l+r < n$. However, note that if either $l = 0$ or $r = 0$, then $Z(R) = \{0\}$.

Our second proposition says various families of strictly upper triangular matrices also provide good examples.

Proposition 5. *Suppose R_0 is a commutative unital ring with $1 \neq 0$, and that $n, m \in \mathbb{N}$ satisfy $n \geq 3$ and $m < n/2$. Then $R := U(n, m, R_0)$ is non-commutative, and $Z(R) = M(n, n-m, n-m, R_0)$ is a nontrivial proper ideal in R .*

Proof. It is readily verified that $R \subset M(n, m, m, R_0)$ and that $S := M(n, n-m, n-m, R_0)$ is a proper subset of R . Most of the result now follows from Proposition 4, but we need to verify that if $A \in R \setminus S$ then $A \notin Z(R)$. The matrices B used to prove the corresponding result in Proposition 4 also lie in this ring R , so the same proof works. \square

In contrast with the above propositions, $M(n, R_0)$ and $U(n, R_0)$ are unital, so they have an ideal centre only if they are commutative, i.e. only if $n = 1$.

We now turn our attention to rings without ideal centres. Our first result is the following non-existence result.

Theorem 6. *Suppose R is a non-unital ring of order p^n , where p is prime and $n \in \mathbb{N}$, $n \leq 3$. Then R has an ideal centre.*

Let us introduce some notation that will be useful in this proof and later: if x is an element of a ring R , then $\langle x; Z \rangle$ and $\langle\langle x; Z \rangle\rangle$ are the additive subgroup and the subring, respectively, generated in both cases by x and all $z \in Z(R)$; the ring R will be understood whenever we use such notation. Note that if $x \notin Z(R)$, then $Z(R) \subsetneq \langle x; Z \rangle \subseteq \langle\langle x; Z \rangle\rangle$, and that $\langle\langle x; Z \rangle\rangle$ is commutative.

Proof of Theorem 6. Suppose for the sake of contradiction that R is a non-unital ring of order p^n , $n \leq 3$, and that $Z(R)$ is not an ideal. In particular $Z(R)$ is neither $\{0\}$ nor R so, as an additive subgroup of R , it must have order p^k for some $0 < k < n$. In particular $n > 1$. We can also quickly rule out $n = 2$, since then necessarily $k = 1$, and if $x \in R \setminus Z(R)$,

then $\langle x; Z \rangle$ is commutative and strictly contains $Z(R)$, so it must have order p^2 . Thus R is commutative, contradicting the assumption that $Z(R)$ is not an ideal.

Finally, suppose $n = 3$. We can rule out $k = 2$ in the same way as we ruled out $k = 1$ for $n = 2$, so we must have $k = 1$. Let z be a generator of $Z(R)$ as an additive group. Suppose first that $z^2 = 0$. Since $Z(R)$ is not an ideal, there exists some $u \in R \setminus Z(R)$ such that $zu \notin Z(R)$. Then $\langle u; Z \rangle$ has order at least p^2 and, since R cannot be commutative, $\langle\langle u; Z \rangle\rangle = \langle u; Z \rangle$ must have order p^2 . Thus $zu = iz + ju$, where $i, j \in \mathbb{Z}_p$ and $j \neq 0$. But then

$$0 = z^2u = z(zu) = z(iz + ju) = ijz + j^2u$$

which gives a contradiction because $j^2 \neq 0$ and $u \notin Z(R)$.

Suppose instead that $z^2 \neq 0$, and so $z^2 = sz$ for some $s \in \mathbb{Z}_p$, $s \neq 0$. By distributivity, we see that $z^{t+1} = s^t z$ for all $t \in \mathbb{N}$, and so in particular $ez = z$, where $e = z^{p-1}$. Thus e is an identity on $Z(R)$ and in particular $e^2 = e$. Since $Z(R)$ is not an ideal, there exists $u \in R \setminus Z(R)$ such that $eu \notin Z(R)$. As before, $\langle u; Z \rangle$ has order at least p^2 , and $\langle\langle u; Z \rangle\rangle$ cannot have order p^3 lest R be commutative, so $\langle\langle u; Z \rangle\rangle = \langle u; Z \rangle$ has order p^2 . Thus $eu = ie + ju$ for some $i, j \in \mathbb{Z}_p$, $j \neq 0$. Now

$$ie + ju = eu = e^2u = e(ie + ju) = (i + ij)e + j^2u$$

so $i = i + ij$ and $j = j^2$. Since $j \neq 0$, we have $j = 1$, and hence $i = 0$. Thus $eu = u = ue$.

Now $x \mapsto ex$ is an additive homomorphism on R . Suppose it has trivial kernel. Then this map is a permutation on R , and so some iterate of it is the identity map. Of course the n th iterate of this map is just $x \mapsto e^n x$, and so $x \mapsto ex$, since $e^2 = e$. It follows that e is an identity for R , contradicting the assumption that R is non-unital. Thus there exists $v \in R \setminus \{0\}$ such that $ev = 0$. We deduce that

$$uv = (ue)v = u(ev) = 0 = (ev)u = v(eu) = vu,$$

so the subring S generated by $Z(R)$, u , and v is commutative. But $ex = x$ for $x = e, u$, so $ex = x$ for all $x \in \langle\langle u; Z \rangle\rangle$. Since $ev \neq v$, we see that $v \notin \langle\langle u; Z \rangle\rangle$. But $\langle\langle u; Z \rangle\rangle$ has order p^2 , so S must have order p^3 and equal R . Thus R is commutative, contradicting our assumptions. \square

It is easily proved that a finite ring can be decomposed as a direct sum of rings of prime power order. Indeed if $n = \prod_{p|n} p^{k_p}$ is the prime factorization of n , and $m_p = n/p^{k_p}$ for each $p | n$, then R is the direct sum of the ideals $R_p := m_p R$; see [8].

Clearly the centre of a direct sum is a direct sum of the centres, and a ring has an ideal centre if and only if each direct summand has an ideal centre, so to find a ring of minimal order where the centre is not an ideal it suffices to consider prime powers. It is now a straightforward matter to find the minimal order of (non-unital) rings in which the centre is not an ideal. In fact, we get the following result in which $N(2)$ is the ring of order 2 in which all products are 0.

Theorem 7.

- (a) Suppose R is a unital ring of order p^n , where p is prime and $n \leq 3$. If R does not have an ideal centre, then $n = 3$ and R is isomorphic to $U(2, \mathbb{Z}_p)$.
- (b) If R is a non-unital ring of order p^n , where p is prime and $n \leq 3$, then R has an ideal centre. However, $R_{16} := U(2, \mathbb{Z}_2) \oplus N(2)$ is a non-unital ring of order 2^4 that fails to have an ideal centre.

Consequently, the order of the smallest unital ring failing to have an ideal centre is 8, and the order of the smallest non-unital ring failing to have an ideal centre is 16.

Proof. By the comments above, the minimal orders must be prime powers. If a ring R is unital, then $1 \in Z(R)$, and so $Z(R)$ is an ideal if and only if R is commutative. Thus the unital ring without an ideal centre of minimal order is just the noncommutative unital ring of minimal order. This minimal order is known to be 8, and any such ring of order 8 must be isomorphic to the upper triangular matrix ring $U(2, \mathbb{Z}_2)$; see [7].

Since all prime powers of order less than 16 are of the form p^n for some $n \leq 3$, all such non-unital rings have ideal centres according to Theorem 6. A direct sum has an ideal centre if and only if all of its direct summands have ideal centres, so R_{16} fails to have an ideal centre by (a). The presence of the $N(2)$ summand prevents R_{16} from being unital. \square

Remark 8. Unlike our unital ring of order 8, the non-unital example in the above proof is decomposable as a direct sum of smaller rings. We prove in [4] that all indecomposable non-unital rings of order p^k for $k \leq 4$ have an ideal centre (p being any prime), and that the smallest indecomposable non-unital ring without an ideal centre has order 32.

Remark 9. The previous remark suggests that perhaps finite indecomposable non-unital rings rarely fail to have an ideal centre. On the other hand, we will see in the next section that the assumption that a ring has an ideal centre is of great use for proving commutativity results. This suggests that the ideal centre assumption may be useful for formulating conjectures regarding conditions that may imply commutativity: if we can prove a commutativity result for rings with ideal centres, then it seems reasonable to search for a proof of the corresponding result without the ideal centre assumption. This technique has already led to one success: we have been able to drop the ideal centre assumption in Theorem 2(c) leading to [6, Theorem 2]. Going beyond this, we would like to know if the three conditions in Theorem 2 are equivalent in the class of all rings.

We conclude this section by strengthening the previously mentioned fact that a non-commutative ring with an ideal centre cannot have a unity, but first we record a simple proposition.

Proposition 10. *A ring R has an ideal centre if and only if $cz = 0$ whenever c is a commutator and $z \in Z(R)$.*

Proof. If $x, y \in R$, and $z \in Z(R)$ then $(xy)z = x(zy)$ and $(yx)z = (yz)x = (zy)x$. Thus $[x, y]z = 0$ for all such x, y, z if and only if $zy \in Z(R)$ for all such y, z . \square

Theorem 11. *Suppose a noncommutative ring R has an ideal centre. Then $R/Z(R)$ does not have a unity.*

Proof. Suppose for the sake of contradiction that $R/Z(R)$ has a unity $e + Z(R)$, where $e \in R$. It follows that for all $x \in R$, $x = exe + z_x$, for some $z_x \in Z(R)$. Also $e^2 = e + w$ for some $w \in Z(R)$. Thus

$$\begin{aligned} ex - xe &= e(exe + z_x) - (exe + z_x)e \\ &= e^2xe - exe^2 = wxe - exw = [x, e]w = 0, \end{aligned}$$

where the last equation follows from Proposition 10. Since x is arbitrary, it follows that $e \in Z(R)$, so the unity of $R/Z(R)$ is also the zero element. This contradicts the assumption that $Z(R)$ is not all of R . \square

3 Elementary commutativity results Many results in the literature give elementary proofs of special cases of the results of Jacobson and Herstein mentioned in the introduction; in all cases, we use *elementary* to refer to proofs that do not appeal to Jacobson’s structure theory of rings. The typical special case involves assuming that $n(x)$ or $n(x, y)$ takes on a particular constant value n . Let us review a few such results.

In the case of the identity $x^n = x$, elementary commutativity proofs were given by Morita [17] for all odd $n \leq 25$ and all even $n \leq 50$. MacHale [16] gave an elementary proof of commutativity for all even numbers n that can be written as sums or differences of two powers of 2, but are not themselves powers of 2. Also notable is the proof by Wamsley [19] of Jacobson’s result which uses only a weak form of structure theory (specifically, the fact that a finite commutative ring can be written as a direct sum of fields).

For the condition $x^n - x \in Z(R)$, elementary proofs of commutativity are well known for $n = 2$ (see e.g. [1] and [14]), and such a proof for $n = 3$ can be found in [15, Theorem 2] and [18, Theorem 1]. Elementary proofs for odd $n < 10$, and for infinitely many even values of n , can be found in [3]. In the case of the condition $[x, y]^n = [x, y]$, an elementary proof for $n = 3$ (and a fortiori for $n = 2$) is given in [3, Theorem 17].

Our results are rather different from the above elementary theorems since we do not restrict $n(x)$ or $n(x, y)$ —indeed we consider more general polynomial conditions—but instead we add the assumption that $Z(R)$ is an ideal. The one result of a similar type in the literature of which we are aware is Theorem 6 of [16] which implies in particular that if R is a ring, $Z(R)$ is an ideal, and there exists an even number $n > 1$ such $x^n - x \in Z(R)$ for all $x \in R$, then R is commutative. This implication of course follows from a special case of Theorem 1.

We begin with a well-known lemma, and include a proof for completeness.

Lemma 12. *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 $e \in Z(R)$. \square

We now prove one of our main results.

Proof of Theorem 2. Trivially, (a) implies (b), and (b) implies (c), so we need only prove that (c) implies (a). Suppose $xy = 0$ for some $x, y \in R$. Then $[y, x] = yx$ and so there exists $f(X) \in X^2\mathbb{Z}[X]$ such that $yx = f(yx)$. Each term of the polynomial expression $f(yx)$ is an integer multiple of $(yx)^n$ for some $n > 1$. But $(yx)^n$ can be written in the form $y(xy)x'$ (where $x' = x$ or $x' = x(yx)^{n-2}$, depending on whether $n = 2$ or $n > 2$), and so $yx = y(xy)x' = y(0)x' = 0$. By Lemma 12, idempotents are central.

Let us now fix an arbitrary pair of elements $u, v \in R$, and write $w = [u, v]$. Let $G(X) \in X^2\mathbb{Z}[X]$ be such that $w = G(w)$. Factorizing $G(X) = Xg(X)$, we have $wg(w) = w$, and so $g(w)$ is an identity in the subring generated by w . In particular, $g(w)$ is an idempotent, and so central. Since $w = wg(w)$ and $Z(R)$ is an ideal, it follows that $w \in Z(R)$. Thus all commutators are central.

In an arbitrary ring, the identity $y[x, y] = [yx, y]$ follows immediately from the definition of commutators. Using this identity and the centrality of commutators, we see that for all $a, b \in R$,

$$ab[a, b] = a[ba, b] = [ba, b]a = b[a, b]a = ba[a, b],$$

and so $[a, b]^2 = 0$. Choosing $h(X) \in X^2\mathbb{Z}[X]$ such that $h([a, b]) = [a, b]$, the identity $[a, b]^2 = 0$ readily implies that $h([a, b]) = 0$, and so $[a, b] = 0$. Thus R is commutative. \square

For convenience, we now make the following definition: a ring R is a *H-ring* if for every $x \in R$ there exists $f(X) \in X^2\mathbb{Z}[X]$ for which $f(x) - x \in Z(R)$. (“H” is in honor of Herstein who proved that H-rings are commutative; see Theorem A.)

The key step in proving Theorem 1 is to prove the following special case.

Lemma 13. *Suppose that R is a H-ring with an ideal centre. Then $Z(R)$ contains all $e \in R$ such that $e^2 - e \in Z(R)$.*

Proof. Let $y \in R$ be arbitrary, and define $d := eye - ye$ and $z := e^2 - e$. Suppose that $z \in Z(R)$. Since R has an ideal centre, $ed = zye \in Z(R)$ and consequently $(de)^2 = d(ed)e \in Z(R)$. It then follows that $(de)^k \in Z(R)$ for all $k \in \mathbb{N}$, $k > 1$, and so $f(de) \in Z(R)$ whenever $f(X) \in X^2\mathbb{Z}[X]$. Using the *H-ring* property, we see that $de \in Z(R)$. Thus $eye - ye = de - (ey - y)z \in Z(R)$. By symmetry¹, $eye - ey \in Z(R)$, and so $ey - ye \in Z(R)$.

Now $(ey)(ey - ye) = (ey - ye)(ey)$, so

$$(14) \quad ey^2e = ye^2y = yey + zy^2.$$

Next, we show that

$$(15) \quad (ye)^2 = (ey^2e - zy^2)e = ey^2e.$$

The first equation in (15) follows immediately from (14). Because $z, zy^2 \in Z(R)$, we deduce that $zy^2e = ezy^2 = ey^2z$, and the second equation in (15) now follows immediately from the equation $z = e^2 - e$. We deduce from (15) and symmetry that $(ey)^2 = ey^2e$, and so

$$(16) \quad (ye)^2 = (ey)^2.$$

Now $e(e + x) = e + z + ex$ and $(e + x)e = e + z + xe$, so

$$(e(e + x))^2 = e^2 + z^2 + (ex)^2 + 2ez + 2zex + e^2x + exe$$

and

$$((e + x)e)^2 = e^2 + z^2 + (xe)^2 + 2ez + 2zxe + xe^2 + exe$$

But the expressions on the left of the last two displays are equal by (16) with $y = e + x$, and $zxe = zex$ since $z \in Z(R)$ and $Z(R)$ is an ideal, so we conclude that $e^2x = xe^2$. Since $e^2 - e \in Z(R)$, we finally get $ex = xe$ for all $x \in R$, as required. \square

Proof of Theorem 1. It suffices to prove that a H-ring with ideal centre R is necessarily commutative. Fixing an arbitrary $x \in R$, let $F(X) \in X^2\mathbb{Z}[X]$ be such that $F(x) - x \in Z(R)$. We factorize $F(X) = Xf(X)$, and write $e := f(x)$. By assumption, $xe - x \in Z(R)$. Since $Z(R)$ is an ideal, we deduce inductively that $x^n e - x^n \in Z(R)$ for all $n \in \mathbb{N}$, and so $g(x)e - g(x) \in Z(R)$ for all $g(X) \in X\mathbb{Z}[X]$. In particular, $e^2 - e \in Z(R)$. Lemma 13 now implies that $e \in Z(R)$, and so $x = xe - (xe - x) \in Z(R)$. Since x is arbitrary, we are done. \square

Proof of Theorem 3. Sufficiency of the coefficient conditions in (a) and (b) follows trivially from the proof of the corresponding result for general rings (i.e. the main result in [13] for (a), and [5, Proposition 4] for (b)). The only non-elementary parts of the earlier proofs are the use in both cases of results of Herstein mentioned in the introduction: in fact, an

¹Note that the hypotheses are also satisfied by the opposite ring R^{op} (this is the ring with the same addition as R and multiplication $*$ given in terms of R -multiplication by $x * y = yx$), so appealing to symmetry to reverse the order of the elements here and later is justified.

appeal to Theorem A suffices in both cases. For rings with ideal centre, we therefore get an elementary proof of these implications simply by appealing to Theorem 1 instead of Theorem A. As for the converse implications in (a) and (b), these are established in [13] and [5] by giving counterexamples for each of the various situations in which the coefficient conditions fail. Since it is readily verified that all of these counterexamples are rings with ideal centres, these same counterexamples establish the converse implications in the current result.

Finally, we tackle (c). Sufficiency of the coefficient condition follows from Theorem 2. As for necessity, suppose f is a polynomial such that its coefficient a_1 is not ± 1 . Thus a_1 has a prime factor p . Consider the ring R_p of 3×3 matrices over \mathbb{Z}_p of the form

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

As is readily verified, $Z(R_p)$ consists of all matrices of the above form with $a = c = 0$ and $R_p \cdot Z(R_p) = \{0\}$, so $Z(R_p)$ is an ideal. Moreover, the set of commutators C_p equals $Z(R_p)$, so it follows from the equation $R_p \cdot C_p = \{0\}$ that $f(x) = 0$ for all $x \in C_p$. However, R_p is not commutative, so we are done. \square

REFERENCES

- [1] R. Ayoub, C. Ayoub, *On the commutativity of rings*, Amer. Math. Monthly **71** (1964), 267–271.
- [2] S.M. Buckley and D. MacHale, *Centriflers and ring commutativity*, J. Math. Sci. Adv. Appl. **15** (2012), 139–161.
- [3] S.M. Buckley and D. MacHale, *Variations on a theme: rings satisfying $x^3 = x$ are commutative*, Amer. Math. Monthly **120** (2013), 430–440.
- [4] S.M. Buckley and D. MacHale, *Small rings in which the centre is not an ideal*, Bull. Irish Math. Soc. **70** (2012), 41–49.
- [5] S.M. Buckley and D. MacHale, *Z-polynomials and ring commutativity*, Math. Proc. R. Ir. Acad. **112** (2012), 51–57.
- [6] S.M. Buckley and D. MacHale, *A characterization of commutator-forcing polynomials*, Math. Proc. R. Ir. Acad., to appear. (Available at http://archive.maths.nuim.ie/staff/sbuckley/Papers/bm_comm.pdf)
- [7] K.E. Eldridge, *Orders for finite noncommutative rings with unity*, Amer. Math. Monthly **75** (1968), 512–514.
- [8] L. Fuchs, *Ringe und ihre additive Gruppe*, Publ. Math. Debrecen **4** (1956), 488–508.
- [9] I.N. Herstein, *A generalization of a theorem of Jacobson III*, Amer. J. Math. **75** (1953), 105–111.
- [10] I.N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. **75** (1953), 864–871.
- [11] I.N. Herstein, *A condition for the commutativity of rings*, Canad. J. Math. **9** (1957), 583–586.
- [12] N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. Math. **46** (1945), 695–707.
- [13] T.J. Laffey and D. MacHale, *Polynomials that force a ring to be commutative*, Proc. Royal Irish Acad. **92A** (1992), 277–280.
- [14] D. MacHale, *Rings that are nearly Boolean*, Proc. Roy. Irish Acad. Sect. A **80** (1980), 41–46.
- [15] D. MacHale, *Rings that are nearly Boolean II*, Proc. Roy. Irish Acad. Sect. A **83** (1983), 165–167.
- [16] D. MacHale, *Rings that are nearly Boolean III*, Proc. Roy. Irish Acad. Sect. A **86** (1986), 165–167.
- [17] Y. Morita, *Elementary proofs of the commutativity of rings satisfying $x^n = x$* , Memoirs Def. Acad. Jap. **XVIII** (1978), 1–23.
- [18] S. Vernon, *On commutativity in certain classes of rings*, Proc. Roy. Irish Acad. Sect. A **83** (1983), 197–200.
- [19] J.W. Wamsley, *On a condition for commutativity of rings*, Proc. London Math. Soc. (2) **4** (1971), 331–332.

Communicated by *Klaus Denecke*

S.M. Buckley:

Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.

Email: stephen.buckley@maths.nuim.ie

D. MacHale:

School of Mathematical Sciences, University College Cork, Cork, Ireland.

E-mail: d.machale@ucc.ie