Irish Math. Soc. Bulletin
Number 70, Winter 2012, 41–49
ISSN 0791-5578

Small rings without ideal centres

STEPHEN M. BUCKLEY AND DESMOND MACHALE

Abstract. We show that the smallest indecomposable non-unital ring in which the centre is not an ideal has order 32.

1. Introduction

We say that a ring R has an *ideal centre* if its centre $Z(R)$ is an ideal. It is easy to see that a unital ring has an ideal centre if and only it is commutative, so this concept is mainly of interest for non-unital rings.

Rings with ideal centres are discussed in [1], where it is shown that certain classical results of Jacobson and Herstein, whose usual proofs involve Jacobson's structure theory, can be proved in an elementary fashion if we restrict to rings with ideal centres. A notable example is Herstein's result [5] that a ring R is commutative if and only if for every $x \in R$ there exists an integer $n(x) > 1$ such that $x^{n(x)} - x \in Z(R)$.

It is easily proved that a finite ring can be decomposed as a direct sum of rings of prime power order [4], that the centre of a direct sum is a direct sum of the centres, and that a ring has an ideal centre if and only if each direct summand has an ideal centre, so the task of finding a ring of minimal order whose centre fails to be an ideal reduces to considering only prime powers p^n. Here and throughout the paper, p denotes a prime number.

Various families of noncommutative non-unital rings with ideal centres are given in [1], but few examples are given of non-unital rings in which the centre fails to be an ideal. In this note, we will prove that most non-unital rings of small order, whether commutative or not, have ideal centres. This stands in contrast to the

2010 *Mathematics Subject Classification.* 16R50.
Key words and phrases. Non-unital ring, noncommutative ring.
Received on 10-3-2011; revised 7-4-11.

situation in unital rings which fail to have an ideal centre if and only if they are noncommutative.

In view of the discussions above, there is one way of constructing *obvious examples* of non-unital rings (with order p^4 or higher) that fail to have an ideal centre: just take the direct sum of a noncommutative unital ring and a non-unital ring. Giving a non-obvious example amounts to giving an indecomposable example, ideally of minimal order, and we do so below.

In order to state more precisely the results for small rings in [1], we first define two rings: $U(2,\mathbb{Z}_n)$ is the ring of 2×2 upper triangular matrices over the ring $\mathbb{Z}_n$ of integers mod $n>1$, i.e. all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \qquad a,b,c\in\mathbb{Z}_n\,, \tag{1}$$

and $N(p)$ is the ring with p elements in which all products are zero.

The following result is Theorem 4 in [1].

Theorem 1.1.

(i) Suppose R is a unital ring of order p^n, where p is prime and $n\le 3$. If R does not have an ideal centre, then $n=3$ and R is isomorphic to $U(2,\mathbb{Z}_p)$.

(ii) If R is a non-unital ring of order p^n, where p is prime and $n\le 3$, 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.

Theorem 1.1(i) was not new, since it just amounts to saying that if R is a noncommutative unital ring of order p^n for $n\le 3$, then R is isomorphic to $U(2,\mathbb{Z}_p)$, a result that was proved by Eldridge [2]. Although Theorem 1.1(ii) was new, the example given there is certainly decomposable, and is an obvious example in the sense discussed above; by contrast, $U(2,\mathbb{Z}_p)$ is easily seen to be indecomposable. It would be nice to improve (b) by giving an indecomposable example of order 16. However the following pair of theorems show that no such example exists, and that the smallest indecomposable example has order 32.

Theorem 1.2. *The direct sum $U(2,\mathbb{Z}_p)\oplus N(p)$ is the unique non-unital ring of order p^4 in which the centre fails to be an ideal.*

Theorem 1.3. *Let S be the subring of $U(2, \mathbb{Z}_4)$ consisting of all elements of the form (1) with c even. Then S has order 32, and it is the smallest indecomposable non-unital ring in which the centre fails to be an ideal.*

2. Preliminaries

We also use the following notation throughout, where in all cases x is an element of some ring R that is omitted from our notation.

$\langle x, \ldots \rangle$ is the additive subgroup generated by $x, \ldots$.

$\langle\langle x, \ldots \rangle\rangle$ is the subring generated by $x, \ldots$.

$\langle x, \ldots ; Z \rangle = \langle x, \ldots \rangle + Z(R)$ is the additive subgroup generated by $x, \ldots$, and all elements of $Z(R)$.

$\langle\langle x, \ldots ; Z \rangle\rangle$ is the subring generated by $x, \ldots$, and all elements of $Z(R)$.

$\langle x; Z \rangle^- = \langle x; Z \rangle \setminus Z(R)$.

Thus

$$\langle x, \ldots \rangle \subset \langle\langle x, \ldots \rangle\rangle ,$$
$$\langle x, \ldots \rangle \subset \langle x, \ldots ; Z \rangle \subset \langle\langle x, \ldots ; Z \rangle\rangle ,$$

Note that $\langle\langle x; Z \rangle\rangle$ is always commutative, and so it never equals R if R is noncommutative. In particular, if R is not commutative, then the additive factor group $R/Z(R)$ cannot be cyclic. Note also that in a finite non-unital ring R, the additive homomorphisms $x \mapsto xy$ and $x \mapsto yx$ must have nontrivial kernel for all $y \in Z(R)$, since otherwise we have a permutation which we can iterate to get a unity.

We now give two preparatory lemmas.

Lemma 2.1. *Suppose R is a ring. If $z \in Z(R)$ and $u, v \in R$ are such that $zu = u$ and $zv \in Z(R)$, then $uv = vu$.*

Proof. We simply note that $uv = (uz)v = u(zv) = (vz)u = v(zu) = vu$. □

Lemma 2.2. *Suppose R is a finite ring with a subring S. If $z \in S$ and $x \in R$ are such that $zx = ix + z'$ for some $i \in \mathbb{Z}$, $z' \in S$, and if $i^n x \notin S$ for all $n \in \mathbb{N}$, then there exist $m, N \in \mathbb{N}$, such that $y := z^m x \notin S$, $e := z^N$ is a nonzero idempotent, and $ey = y$.*

Proof. By distributivity, we have $z^j x = i^j x + b_j$ for all $j \in \mathbb{N}$, where $b_j \in S$. In particular $z^j x \in R \setminus S$ and so $z^j \neq 0$, for all $j \in \mathbb{N}$.

Since R is finite, we can pick $m, n \in \mathbb{N}$ such that $z^m x = z^{n+m} x$. Similarly we can find $k > 1$ such that $z^n = z^{nk}$. Then $e := z^{n(k-1)}$ and $y := z^m x$ have the desired properties. □

3. Proofs of main results

We first use Lemma 2.2 to prove a lemma for a finite ring with centre of index p^2.

Lemma 3.1. *Suppose that R is a finite ring and that the additive factor group $G := R/Z(R)$ is of order p^2 for some prime p. If $z \in Z(R)$ and $x \in R$ are such that $zx \notin Z(R)$, then there exist $m, N \in \mathbb{N}$, such that $y := z^m x \notin Z(R)$, $e := z^N$ is a nonzero idempotent, and $ey = y$.*

Proof. First $|G| = p^2$ and $x \notin Z(R)$, so $x + Z(R)$ has order p^k in G, where $k \in \{1, 2\}$. But it cannot have order p^2, since the additive factor group cannot be cyclic. Thus $ix \in Z(R)$ if and only i is divisible by p. Also $zx \in \langle x; Z \rangle$, since otherwise $\langle\langle x; Z\rangle\rangle \supset \langle x, zx; Z\rangle$ would have order $p^2|Z(R)|$ and $R = \langle\langle x; Z\rangle\rangle$ would be commutative. Thus $zx = ix + z'$ for some $z' \in Z(R)$, and $i \in \mathbb{N}$ not divisible by p. The result now follows from Lemma 2.2. □

The following lemma will be particularly useful to cut down on the number of cases that need to be examined.

Lemma 3.2. *Suppose that R is a finite non-unital ring of order p^n for some prime p and integer $n \geq 3$. Suppose further that*

(i) $Z(R)$ is not an ideal, and
(ii) the additive factor group $G := R/Z(R)$ is of order p^2.

Then $Z(R)$ is non-unital and $(Z(R), +)$ is non-cyclic. Furthermore, there exists a nonzero idempotent $e \in Z(R)$ and an element $y \in R \setminus Z(R)$ such that $ey = y$.

Proof. Since $Z(R)$ is not an ideal, there exists $z \in Z(R)$ and $x \in R$ such that $zx \notin Z(R)$. Applying Lemma 3.1, we get a nonzero idempotent $e \in Z(R)$ and $y \in R \setminus Z(R)$ such that $ey = y$.

All elements in $pZ(R)$ are nilpotent, so if $(Z(R), +)$ were cyclic, nonzero idempotents would necessarily generate $(Z(R), +)$. But if e is idempotent and generates $(Z(R), +)$, then it is a unity for $Z(R)$. Thus to finish the proof, it suffices to prove that $Z(R)$ is non-unital.

Suppose for the sake of contradiction that u is a unity for $Z(R)$. Since R is finite and non-unital, $w \mapsto wu$ must have nonempty kernel

in R, so there must exist $v \neq 0$ such that $uv = 0$. Now $ey = y$ and $ev = euv = 0$, so y and v commute by Lemma 2.1. It follows that $\langle y, v; Z\rangle$ is commutative, and so $\langle y, v; Z\rangle$ cannot be all of R. Since $y \notin Z(R)$, we see that the additive group $R/\langle y; Z\rangle$ has size at most p. It follows that $v \in \langle y; Z\rangle$, so $v = iy + w$ for some $i \in \mathbb{Z}_p$ and $w \in \mathbb{Z}(R)$. Thus

$$0 = uv = iuy + uw = iuey + uw = iey + w = v \neq 0\,,$$

giving the desired contradiction. □

Lemma 3.3. *Suppose that R is a non-unital ring of order p^4 for some prime p and that $Z(R)$ is of order p^2 and is not an ideal. Then $Z(R)$ is isomorphic to $\mathbb{Z}_p \oplus N(p)$.*

Proof. By Lemma 3.2, we know that there is a nonzero idempotent $e \in Z(R)$, that $Z(R)$ is non-unital, and that $(Z(R), +)$ is not cyclic. This is already enough to deduce the lemma if we examine the list of all nine isomorphism classes of commutative rings of order p^2 given in [3]. However it is not hard to give a self-contained proof so let us proceed.

Since $(Z(R), +)$ is not cyclic, it is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$, and $Z(R)$ is a $\mathbb{Z}_p$-algebra of dimension 2. Suppose $z \in Z(R) \setminus \langle e\rangle$, so $\{e, z\}$ is a basis for $Z(R)$ and $ez = ie + jz$ for some $i, j \in \mathbb{Z}_p$. The equation $ez = e^2z$ expands to $ie + jz = (i + ij)e + j^2z$, and so $ij = 0$. Thus $ez \in \{e, z, 0\}$. Now $ez = z$ would imply that e is a unity for $Z(R)$, so we can rule that out. We may assume that $ez = 0$ since if $ez = e$, then replacing z by $z - e$ reduces to this case. Next $z^2 = ae + bz$ for some $a, b \in \mathbb{Z}_p$. The equation $z^2e = 0$ yields $ae = 0$ and so $a = 0$. Thus $z^2 = bz$.

If $b \neq 0$, and we define $w := e + b^{-1}z$ (with the inverse taken in $\mathbb{Z}_p$), then $(e + w)x = x$ for $x \in \{e, z\}$, and so $e + w$ is a unity for $Z(R)$. Since $Z(R)$ is non-unital, it follows that $b = 0$, and that $Z(R)$ is isomorphic to $\mathbb{Z}_p \oplus N(p)$. □

Proof of Theorem 1.2. Throughout this proof, we assume that R is a non-unital ring of order p^4 in which the centre is not an ideal. In particular R is not commutative. By $R/Z(R)$, we always mean the additive factor group. Since $R/Z(R)$ cannot be cyclic, and since $Z(R)$ is not an ideal, it follows that $|Z(R)| = p^k$ for $k \in \{1, 2\}$, and that $(R, +)$ is not cyclic. Since R is noncommutative, R is never equal to $\langle\langle x; Z\rangle\rangle$ for any $x \in R$.

The proof consists of examining in turn each of the four possible isomorphism types of $(R,+)$ that remain: two two-generator types, one three-generator type, and one four-generator type (which splits into two cases).

Case 1: $(R,+) = \mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$.

Let u, v be generators of $(R,+)$, with u being of order p^3 and v of order p. Now u and v do not commute, but $puv = pvu = 0$, so $Z(R)$ must equal $\langle pu \rangle$. But $\langle pu \rangle$ is an ideal, so R cannot be of this additive type. (Alternatively $\langle pu \rangle$ is cyclic, which contradicts Lemma 3.2.)

Case 2: $(R,+) = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$.

$Z(R)$ cannot contain an element x of order p^2 in $(R,+)$, since if we then took y such that $\langle x, y \rangle = R$, it would follow that $R = \langle x, y \rangle = \langle \langle y; Z \rangle \rangle$ is commutative. All other nonzero elements have order p, so $Z(R)$ contains pu for some element u of order p^2. If we now pick $v \in R \setminus \langle u \rangle$, then $(pu)v = v(pu)$, so $pv \in Z(R)$ also. Thus $Z(R)$ contains pR. Since $|pR| = p^2$, we must have $Z(R) = pR$. But pR is an ideal in R, so R cannot be of this additive type. (Alternatively all elements in pR are nilpotent, contradicting Lemma 3.2.)

Case 3: $(R,+) = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Suppose first that there is a central element z of order p^2. Since $|Z(R)| \leq p^2$, we have $Z(R) = \langle z \rangle$. But this is cyclic, contradicting Lemma 3.2.

Let w be an element of order p^2 in R. Since $(R,+)$ is generated by w and a pair of elements of order p, and since pw annihilates all elements of order p, we see that $\langle pw \rangle = \langle \langle pw \rangle \rangle$ is an ideal of order p contained in $Z(R)$, and so it cannot be all of $Z(R)$. Thus $Z(R)$ must be of order p^2, so there exists a nonzero idempotent $e \in Z(R)$ and $y \in R \setminus Z(R)$ such that $ey = y$. Since e has order p, y must also be of order p. This rules out the possibility that $y \in \langle w \rangle$ since then e would be an identity for $\langle pw, e \rangle = Z(R)$, contradicting Lemma 3.2. It follows that $R = \langle w, e, y \rangle$, and that y does not commute with w.

Note that $\langle y; Z \rangle$ is commutative and of order p^3, and so it must consist of all $x \in R$ such that $px = 0$. We also see that $\langle y; Z \rangle$ consists of all $x \in R$ that commute with y. Now $p(ew) = 0$, so ew must commute with y, and certainly ew commutes with w. We deduce that ew is central. Applying Lemma 2.1 with data (z, u, v)

given by (e, y, w), we see that y and w commute, contradicting our assumptions.

Case 4: $(R, +) = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $Z(R)$ is of order p.

Let z be a nonzero element in $Z(R)$. Suppose first that $z^2 = 0$. Since z is not an ideal, we must have $zu = v$ for some $v \notin Z(R)$. If $v = zu \in \langle u; Z\rangle$, then $zu = iu+jz$ for some $i, j \in \mathbb{Z}_p$, $i \neq 0$. But then $z^2u = i^2u + ijz \notin Z(R)$ contradicting the fact that $z^2u = (0)u = 0$. Thus $v \notin \langle u; Z\rangle$ and $S := \langle\langle z, u, v\rangle\rangle$ must be of order p^3 (since it is commutative) and S is also generated as a $\mathbb{Z}_p$-vector subspace of R by z, u, v. Let $w \in R \setminus \langle\langle z, u, v\rangle\rangle$, so that $\{z, u, v, w\}$ forms a basis of R. Suppose $wz = qz+ru+sv+tw$, for some $q, r, s, t \in \mathbb{Z}_p$. Since z, u, v lie in a subring S that omits w, it follows from the equation $wz^2 = 0$ that $t = 0$. Thus $wz \in S$ commutes with u and we get $wv = wzu = uwz = uzw = vw$. Now v commutes with w as well as e, u, and v, contradicting the assumption that $Z(R) = \langle z\rangle$.

Thus $z^2 \neq 0$, so multiplication by z gives a permutation of $Z(R)$. We deduce that $Z(R)$ has an identity, and we may assume that this is z. Since the centre is not an ideal there exist $x, u \in R \setminus Z(R)$ such that $zx = u$. Now $zu = z(zx) = z^2x = u$. Thus z is an identity on $\langle\langle u; Z\rangle\rangle$. However R does not have an identity so there must exist $v \neq 0$ such that $zv = 0$. By Lemma 2.1, $\langle\langle u, v; Z\rangle\rangle$ is commutative. Let $w \in R \setminus \langle\langle u, v; Z\rangle\rangle$. Now $wz = zw$ cannot lie in $\langle\langle u, v; Z\rangle\rangle$, since otherwise it would commute with u and we would get $uw = uzw = zwu = wzu = wu$, from which it would follow that $u \in Z(R)$, contradicting the assumption that $Z(R) = \langle z\rangle$. Thus $wz = qz + ru + sv + tw$ for some $q, r, s, t \in \mathbb{Z}_p$, $t \neq 0$. We deduce that $wz^2 = (q + qt)z + (r + rt)u + stv + t^2w$ and, since $z = z^2$, we must have $q = r = 0$, so $wz = sv+tw$. Multiplying by $j = t^{-1} \in \mathbb{Z}_p$, we get $w = jwz + s'v$, where $s' = -js$. Since $vz = 0$, we deduce that

$$vw = v(jwz + s'v) = jvzw + s'v^2 = s'v^2$$

and we similarly see that $wv = s'v^2$. Thus v commutes with w as well as e, u, and v, contradicting the assumption that $Z(R) = \langle z\rangle$.

Case 5: $(R, +) = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $Z(R)$ is of order p^2.

By Lemmas 3.2 and 3.3, $Z(R)$ is isomorphic to $\mathbb{Z}_p \oplus N(p)$, and there exists $u \in R \setminus Z(R)$ such that $eu = u$, where e is the unique nonzero idempotent in $Z(R)$. Let $z \in Z(R)$, $z \neq 0$, be such that $z^2 = 0$ (and so also $ez = 0$).

Choosing $w \in R \setminus \langle u; Z\rangle$, we must have $we = ew \notin \langle\langle u; Z\rangle\rangle$ since otherwise $uw = uew = ewu = weu = wu$, and u would be in $Z(R)$. Thus we can apply Lemma 2.2 to get $v \in \langle w; Z\rangle \setminus Z(R)$ such that $ev = v$. Now $zu = zeu = 0$ and $zv = zev = 0$ so $zR = \{0\}$. Also $ex = x$ for all $x \in \langle\langle e, u, v\rangle\rangle$, and R is non-unital, so we must have $\langle e, u, v\rangle = \langle\langle e, u, v\rangle\rangle$. We denote this last subring by S: note that S is a noncommutative ring of order p^3 with unity e. Since also $T := \langle z\rangle$ is isomorphic to $N(p)$, and since z annihilates the generators of S, we see that $R = S \oplus T$. To finish we appeal to the proposition on p.513 of [2] which tells us that a noncommutative unital ring of order p^3 must be isomorphic to $U(2, \mathbb{Z}_p)$. □

Proof of Theorem 1.3. All rings of prime power order less than 32 have order p^n for some prime p and $n \leq 4$, so by Theorem 1.1(ii) and Theorem 1.2, they have ideal centre. Thus the minimal example has order at least 32.

It is readily verified that S is a non-unital ring of order 32, and that $Z(S)$ is of order 2: in fact $Z(S)$ consists of the two multiples of the identity matrix in $U(2, \mathbb{Z}_4)$ that lie in S. It is also clear that $Z(S)$ is not an ideal: in fact the product $S \cdot Z(S)$ equals $2S$ and has order 4.

It remains to prove that S is not decomposable. Suppose for the sake of contradiction that $S = S_1 \oplus S_2$, where the orders n_i of S_i satisfy $n_1 \geq n_2 > 1$. Thus we either have $n_1 = 16$ and $n_2 = 2$, or $n_1 = 8$ and $n_2 = 4$. As mentioned in the introduction, $Z(S) = Z(S_1) \oplus Z(S_2)$ and S has an ideal centre if and only if both S_1 and S_2 have ideal centres.

Now $(S, +)$ has the form $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$, so each of these additive direct summands must be allocated to either S_1 or S_2. Suppose first that $n_1 = 16$. Then $(S_1, +) = \mathbb{Z}_4 \oplus \mathbb{Z}_4$, and S_1 cannot have an ideal centre since S_2 must be commutative. By Theorem 1.2, rings of order 16 without ideal centres have additive type $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, so we conclude that S_1 cannot be non-unital. On the other hand, if S_1 were unital, we could take its unity 1 as one of its two generators. Now 1 commutes with the other generator of S_1, forcing S_1 and hence S, to be commutative, which it cannot be. Thus $n_1 \neq 16$.

Suppose instead that $n_1 = 8$. Since the smallest ring with non-ideal centre has order 8, S_2 must have ideal centre and S_1 must not. By Theorem 1.1, S_1 would have to be $U(2, \mathbb{Z}_2)$. But $(U(2, \mathbb{Z}_2), +) =$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, whereas S_1 must be of type $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, so this case is also ruled out. □

The results of this paper suggest that perhaps finite indecomposable non-unital rings rarely fail to have an ideal centre. On the other hand, it is clear from the results in [1] 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.

References

[1] S.M. Buckley and D. MacHale, *Rings with ideal centres*, preprint `http://www.maths.nuim.ie/staff/sbuckley/Papers/bm_ideal.pdf`.

[2] K.E. Eldridge, *Orders for finite noncommutative rings with unity*, Amer. Math. Monthly 75 (1968), 512–514.

[3] B. Fine, Classification of finite rings of order p^2, Math. Mag. 66 (1993), 248–252.

[4] L. Fuchs, *Ringe und ihre additive Gruppe*, Publ. Math. Debrecen 4 (1956), 488-508.

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

Stephen Buckley received his Ph.D. from the University of Chicago. He is a Professor of Mathematics at NUI Maynooth, where he has taught for twenty years. His research interests include metric space curvature, geometric analysis, harmonic analysis, and ring theory.

Desmond MacHale received his Ph.D. from the University of Keele and is Emeritus Professor of Mathematics at University College Cork where he taught for nearly forty years. His research interests include commutativity in groups and rings, automorphisms of groups, Euclidean geometry, number theory, and mathematical humour.

(S. Buckley) Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland

(D. MacHale) School of Mathematical Sciences, University College Cork, Cork, Ireland

E-mail address, S. Buckley: `stephen.buckley@maths.nuim.ie`

E-mail address, D. MacHale: `d.machale@ucc.ie`