Centrifiers and ring commutativity

S.M. BUCKLEY AND D. MACHALE

Abstract. A result of Herstein says in particular that if there exists $n > 1$ such that $x^n - x \in Z(R)$ for all x in a ring R then R is commutative. We give an elementary proof of this fact for certain values of n, based on the theory of centrifiers which we develop. For $n = 5, 7$, we also give an elementary proof of the commutativity of rings R such that $x^n + x \in Z(R)$ for all $x \in R$.

1. Introduction

Given $n \in \mathbb{N} \setminus \{1\}$, we call a ring R a ZP(n) ring if $x^n - x \in Z(R)$ for all $x \in R$; here $Z(R)$ is the center of R. Trivially, commutative rings are ZP(n) for all n. As a consequence of more general results, Herstein showed conversely that ZP(n) rings are necessarily commutative for all $n > 1$; see [4].

Herstein's proofs use Jacobson's structure theory of rings. Because a proof exists, it follows from Birkhoff's Completeness Theorem [1] that an elementary, purely equational, proof must also exist. This follows because both ZP(n) rings for any fixed n and commutative rings are varieties, i.e. definable by identities. Such elementary proofs cannot employ structure theory because division rings do not form a variety. See [1] or [11] for more details.

Birkhoff's theorem however tells us nothing about how to construct such an elementary proof, or whether such a proof of reasonable length exists for any given n. Elementary proofs of the commutativity of ZP(n) rings are rather well known when $n = 2, 3$: see for instance [7, Theorem 2] for $k = 2$ and [8, Theorem 2] for $k = 3$. We know of no such proofs in the literature beyond this, with the exception that $n = 6, 12$ are handled in [9] for rings with unity. However we do not assume the existence of a unity in our definition of a ring, and we are interested in proofs that require no such additional assumptions on the ring.

This situation contrasts with that of rings satisfying the stronger condition $x^n = x$ for all $x \in R$. In this case, elementary commutativity proofs were given by Morita [10] for all odd $n \leq 25$ and all even $n \leq 50$. Also MacHale [9] gave an elementary proof of commutativity for all even numbers n that are not powers of 2 but that can be written as sums or differences of two powers of 2.

Of course rings satisfying $x^n = x$ for all x are rather special, so it is not surprising that elementary proofs of commutativity are known for more values of n than in the case of ZP(n) rings. However the size of the gap is a little surprising.

In this paper we narrow the gap significantly. In particularly we give an elementary proof of commutativity for some small odd n and for many even numbers that are sums or differences of two powers of 2, and these results imply in particular the following result.

Theorem 1.1. *ZP(n) rings are commutative for all odd $n < 10$ and infinitely many even n, including the following values of $n \leq 30$:*

$$2,\ 6,\ 10,\ 12,\ 14,\ 18,\ 20,\ 24,\ 28,\ 30\,.$$

2010 *Mathematics Subject Classification.* 16R50.

Note the absence of powers of 2 (other than 2) from the above list: among even numbers, powers of 2 seem especially hard to handle by elementary methods. The other even numbers below 30 for which we do not yet have elementary proofs are 22 and 26, the only even numbers below 30 that are not sums or differences of two powers of 2.

To help with our investigation, we introduce the concept of the *centrifier* of an element x in a ring R: this consists of all $z \in R$ that commute with x, such that triple products of x, z, and any other element y are independent of order, e.g. $xyz = yxz = xzy$, etc. Centrifiers are a key tool in our analysis, but may also be of independent interest.

To understand the relevance of centrifiers, consider a ring satisfying the identity $x = x^n$. This trivially implies that $x^2 = x^{n+1}$ for all $k \in \mathbb{N}$, and allows one to deduce that x^{n-1} is central (as are all other idempotents). In the case of a ZP(n) ring R, it does not trivially follow that $x^2 - x^{n+1} \in Z(R)$ but if we can prove this, then the theory of centrifiers allows us to deduce that x^{n-1} is central as a consequence of the fact that certain near-to-idempotent elements are central; see Theorem 3.4 and Corollary 3.7.

For any $n > 1$, we define the *AZP(n) condition* to be $x^n + x \in Z(R)$, $x \in R$. For any given even number n, the ZP(n) and AZP(n) conditions are easily seen to be equivalent (Lemma 2.2), so AZP(n) is of separate interest only when n is odd.

It follows from the main result in [5] that AZP(n) rings are commutative, but this proof also uses the structure theory of rings so again elementary proofs are desirable, and the following result indicates the cases in which we can do this.

Theorem 1.2. *AZP(n) rings are commutative when $n \in \{3, 5, 7\}$.*

Although we are mainly interested in ZP(n) rings in this paper, there are two reasons we give elementary proofs of commutativity of AZP(n) rings for small n. First, there are some commonalities between the proofs of commutativity of ZP(n) and AZP(n) rings. More crucially, the proofs of commutativity of ZP(n) rings for $n = 5, 7, 9$ all use the commutativity of AZP(m) rings for some number $m < n$.

After some preliminaries in Section 2, we introduce and develop the theory of centrifiers in Section 3. We then prove various commutativity results for ZP(n) and AZP(n) rings in Section 4 and Section 5 which imply Theorems 1.1 and 1.2.

2. Preliminaries

Elementary proofs of the next result are rather well known; see [7, Theorem 2] for $k = 2$ and [8, Theorem 2] for $k = 3$. We will use this result repeatedly without explicit reference.

Theorem 2.1. *ZP(k) and AZP(k) rings are commutative for $k = 2, 3$.*

We now state a well-known lemma, which we also use repeatedly without explicit reference; the simple proof can be found for instance in [9, Lemma 1].

Lemma 2.2. *If R is a ZP(n) or an AZP(n) ring for some even number n, then $2R \subset Z(R)$.*

The above lemma implies that the ZP(n) and AZP(n) conditions are equivalent when n is even, so we will examine AZP(n) conditions only for odd n.

We will frequently need information about the parity of binomial coefficients. A result of Kummer [6, pp. 115–116] (see also [3]) says that the exponent of the highest power of p dividing $\binom{n}{m}$ is the number of borrows involved in subtracting m from n in base p. We record here a consequence of this for $p = 2$.

Lemma 2.3. $\binom{n}{m}$ *is odd if and only if the binary expansion of m has a zero in every position where the binary expansion of n has a zero.*

In the above lemma, it is understood that we pad the binary expansion of m with zeros to make it equal in length with the binary expansion of n. We assume implicitly that $0 \le m \le n$ when discussing $\binom{n}{m}$.

3. Centrifiers

Elementary proofs that conditions of the form $x^n = x$ for all $x \in R$ imply that R is commutative typically make use of the fact that idempotents are central in such rings. Analogously, in a ZP(n) ring, we can construct certain elements that are somehow "close-to-idempotent", and we wish to conclude in certain situations that such elements are central. For instance in a ZP(n) ring, $e := x^{n-1}$ is close-to-idempotent in the sense that $e^2 = e + x^{n-2}z$ where $z \in Z(R)$. Knowing that the error term has this form does not make it easy to deduce that e is central. However the notion of centrifiers allows us to prove that some close-to-idempotent elements are central: see Theorem 3.4 below.

Definition 3.1. We say that z *centrifies* an element $x \in R$ if

$$[x, z] = [x, y]z = z[x, y] = [z, xy] = [z, yx] = 0\,, \qquad y \in R\,.$$

The *centrifier of* x, $\mathfrak{C}(x)$, is the set of all $z \in R$ that centrify x.

There is a certain symmetry in the definition of $\mathfrak{C}(x)$: if R^{op} is the ring with the same underlying set and addition operation as R but with multiplication reversed (i.e. multiplication $\circ$ is given by $x \circ y = yx$), then $\mathfrak{C}(x)$ with respect to R^{op} coincides with $\mathfrak{C}(x)$ with respect to R. This symmetry can be used to shorten proofs that $z \in \mathfrak{C}(x)$: if a set of assumptions that also satisfies this symmetry implies that $[x, y]z = [z, xy] = 0$, then we conclude for free that $z[x, y] = [z, yx] = 0$. Without this symmetry in the assumptions, we can instead remove the equation $[z, xy] = 0$ from the definition, since it follows from the other equations.

Theorem 3.2. *Suppose x is an element of a ring R, $z \in \mathfrak{C}(x)$, and $p(X) \in X\mathbb{Z}[X]$. Then*

(a) *$\mathfrak{C}(x)$ is a subring of R.*
(b) *For all $y \in R$, the product xyz is invariant under all re-orderings of its factors. In particular, $xz \in Z(R)$.*
(c) *$x \in \mathfrak{C}(z)$ (i.e. centrification is a symmetric relation).*
(d) *$z \in \mathfrak{C}(p(x))$.*
(e) *$p(x)z = zp(x) \in \mathfrak{C}(x)$.*

Proof. Part (a) follows immediately from the definition, while (b) follows by using the commutator relations repeatedly: $(xy)z = (yx)z = z(yx) = (zx)y = xzy$, and $y(xz) = yzx$. Part (c) follows immediately from part (b).

We now prove (d). Suppose $z \in \mathfrak{C}(x)$. Since each of the commutators in the definition of $\mathfrak{C}(x)$ is $\mathbb{Z}$-linear as a function of x, proving the desired result reduces to proving that $z \in \mathfrak{C}(p(x))$ for $p(x) = x^k$, $k \in \mathbb{N}$. We show this inductively.

The case $k = 1$ is given by assumption, so suppose $z \in \mathfrak{C}(x^k)$ for all $k \le j \in \mathbb{N}$. Then $x^{j+1}z = x^j xz = x^j zx = zx^{j+1}$, so $[x^{j+1}, z] = 0$. Also for every $y \in R$,

$$x^{j+1}yz = x(x^j yz) = (xyz)x^j = yx(zx^j) = yxx^j z = yx^{j+1}z\,,$$

so $[x^{j+1}, y]z = 0$. By symmetry, we get $z[x^{j+1}, y] = 0$. Next

$$zx^{j+1}y = (zx)x^j y = x(zx^j y) = xx^j yz = x^{j+1}yz\,,$$

so $[z, x^{j+1}y] = 0$, and by symmetry we get $[z, yx^{j+1}] = 0$. This completes the inductive step and the proof of (d).

Lastly we prove (e). Since each of the commutators in the definition of $\mathfrak{C}(x)$ is $\mathbb{Z}$-linear as a function of z, we may assume that $p(x)$ has the form $p(x) = x^k$,

$k \in \mathbb{N}$. Since $[x,z]=0$, it is easily to show that $x^k z = zx^k$ and that $[x, x^k z] = 0$. Next $[x,y]x^k z = ([x,y]z)x^k = 0$ and $x^k z[x,y] = 0$, so we need only show that $[x^k z, xy] = [x^k z, yx] = 0$, $k \in \mathbb{Z}$, $k \geq 0$. The case $k = 0$ of these equations is true by assumption, so we assume inductively that these results hold for $0 \leq k \leq j$, where $j \geq 0$. Then

$$(x^{j+1}z)xy = x(x^j z)xy = xxy(x^j z) = x(xyz)x^j = xy(zx^{j+1}) = xyx^{j+1}z\,,$$

so $[x^{j+1}z, xy] = 0$. The fact that $[x^{j+1}z, yx] = 0$ follows similarly. □

The next lemma gives a basic method for identifying elements of centrifiers. In view of Theorem 3.2(b), this method gives all central elements of centrifiers.

Lemma 3.3. *If both z and xz lie in $Z(R)$, then $z \in \mathfrak{C}(x)$. In particular if $mR \subset Z(R)$ for some integer m, then $mR \subset \mathfrak{C}(x)$ for all $x \in R$.*

Proof. First $[x,z] = [z,xy] = [z,yx] = 0$ because $z \in Z(R)$. Next $x(yz) = (xz)y = yxz$ so $[x,y]z = 0$, and hence $z[x,y] = 0$ because z is central.

Suppose next that $mR \subset Z(R)$. If $x, z \in R$, then $mz \in Z(R)$ and $x(mz) = m(xz) \in Z(R)$, so the second statement follows from the first one. □

We now come to our promised result which says that in certain situations, near-to-idempotent elements e are central.

Theorem 3.4. *Suppose R is either a ZP(n) or an AZP(n) ring for some $n > 1$. Suppose $e, x, z \in R$ are such that $e^2 = e + z$, $z \in \mathfrak{C}(x) \cap Z(R)$, and $e = p(x)$ for some $p(X) \in X\mathbb{Z}[X]$. Then $e \in Z(R)$.*

Proof. Let $d := eye - ye$. Then $ed = zye$, and $z \in \mathfrak{C}(e)$ by Theorem 3.2(d). We prove inductively that $(de)^k = (ed)^k$, $k > 1$. First

$$(de)^2 = d(zye)e = (dez)ye = edzye = (ed)^2\,.$$

Suppose therefore that for some $j \geq 2$, $(de)^k = (ed)^k$ for $2 \leq k \leq j$.

$$(de)^{j+1} = de(ed)^j = (dez)ye(ed)^{j-1} = edzye(ed)^{j-1} = (ed)^{j+1}\,.$$

This completes the inductive step and so $(de)^k = (ed)^k$ for all $k > 1$. Taking $k = n$, and using either the ZP(n) or the AZP(n) condition, we conclude that $ed - de \in Z(R)$. But

$$ed - de = zye - (eye + eyz - ye - yz) = ye - eye + yz = ye^2 - eye \in Z(R)\,,$$

so by symmetry we also have $e^2y - eye \in Z(R)$. It follows that $e^2y - ye^2 \in Z(R)$ and, since $e^2 = e + z$ and $yz = zy$, we conclude that $ey - ye \in Z(R)$.

Now $(ey)(ey - ye) = (ey - ye)(ey)$, so $ey^2e = ye^2y = yey + zy^2$. Bearing in mind that $z \in \mathfrak{C}(e)$, we see that

$$(ye)^2 = (ey^2e - zy^2)e = ey^2e = e(ey^2e - zy^2) = (ey)^2\,. \tag{3.5}$$

Now $e(e+y) = e + z + ey$ and $(e+y)e = e + z + ye$, so

$$(e(e+y))^2 = e^2 + z^2 + (ey)^2 + 2ez + 2zey + e^2y + eye$$

and

$$((e+y)e)^2 = e^2 + z^2 + (ye)^2 + 2ez + 2zye + ye^2 + eye$$

But these two expressions are equal by (3.5), and $zye = zey$ since $z \in \mathfrak{C}(e)$, so we conclude that $e^2y = ye^2$. Since $e^2 = e + z$ and z is central, we finally get $ey = ye$, as required. □

Remark 3.6. It is clear from the proof that the assumption that R is either a ZP(n) ring or an AZP(n) ring can be replaced in Theorem 3.4 by the weaker assumption that for each $x \in R$ there exists $n(x) > 1$ such that $x^{n(x)} - h(x) \in Z(R)$, where h is an endomorphism of $(R, +)$ with the property that $x \in Z(R)$ whenever $h(x) \in Z(R)$. Examples of such an endomorphism include $h(x) \equiv x$, $h(x) \equiv -x$, and the involution $*$ in a $*$-ring.

Our first application of Theorem 3.4 is as follows.

Corollary 3.7. *Suppose R is a ZP(n) ring for some $n > 1$, and that $y^2 - y^{n+1} \in Z(R)$ for some $y \in R$. Then $y - y^n \in \mathfrak{C}(y)$ and $y^{n-1} \in Z(R)$. If $mR \subset Z(R)$ for some $m \in \mathbb{N}$, then $\sum_{i=1}^{(n-1)/k} y^{ik} \in Z(R)$ whenever k is a factor of $n-1$, and $(n-1)/k$ is coprime to m.*

Proof. Letting $z := y - y^n \in Z(R)$, we see that $z \in \mathfrak{C}(y)$ (Lemma 3.3), and so $-y^{n-2}z \in \mathfrak{C}(y)$ (Theorem 3.2(e)). But $e := y^{n-1}$ satisfies $e^2 = e - y^{n-2}z$, so $e \in Z(R)$ by Theorem 3.4.

Suppose instead that $mR \subset Z(R)$, that k is a factor of $n-1$, and that $t := (n-1)/k$ is coprime with m. Thus there exists an integer j such that jt is equivalent to 1 mod m. Letting $s := j\sum_{i=1}^{t} y^{ik}$, we see that $sy^k = s - jy^{k-1}z$, and so $s^2 = s + mw + p(y)z$ for some $w \in R$ and some polynomial $p(y)$ in y. But $mw + p(y)z \in \mathfrak{C}(y)$ by Lemma 3.3 and Theorem 3.2(e), so $s \in Z(R)$ by Theorem 3.4. Finally, $ts \in Z(R)$ and by subtracting an element of mR, we conclude that $\sum_{i=1}^{t} y^{ik} \in Z(R)$, as required. □

The following consequence of Corollary 3.7 will be used frequently.

Corollary 3.8. *Suppose R is a ZP(n) ring for some $n > 1$, and that $mR \subset Z(R)$ for some odd integer m. Then $x - x^n \in \mathfrak{C}(x)$ for all $x \in R$. Also $x^{n-1} \in Z(R)$, and more generally $\sum_{i=1}^{(n-1)/k} x^{ik} \in Z(R)$ whenever k is a factor of $n-1$, and $(n-1)/k$ is coprime to m.*

Proof. Letting $z := x - x^n \in Z(R)$, we see that $(x^2 - (x^2)^n) - z^2 = 2xz \in Z(R)$. Since also $mxz \in Z(R)$, we conclude that $xz \in Z(R)$. The result now follows from Corollary 3.7. □

4. Commutativity of ZP(n) and AZP(n) rings for small odd n

In this section, we prove commutativity of ZP(n) rings for $n = 5, 7, 9$, and of AZP(n) rings for $n = 5, 7$. Key parts of the ZP(n) proofs can be reduced to AZP(m) for some $m < n$: in fact, ZP(5) and ZP(9) both reduce to AZP(3), and ZP(7) reduces to AZP(5). The commutativity of ZP(7) rings in turn will be used in the proof of results for even n in the next section: specifically it is used in the proof of Theorem 5.2, which in turn is needed in the proof of Theorem 5.4.

In view of the difficulties of proving commutativity for powers of 2 (as referred to in the next section), it is noteworthy that the proof of commutativity of ZP(9) rings is relatively straightforward.

We first introduce some common notation and conventions that apply throughout this section and the next. We generally denote by $f : R \to Z(R)$ the polynomial that the ZP(n) or AZP(n) condition tells us is central in a ring R, so $f(x) = x \pm x^n$ in all cases. When we define a function g via a formula for $g(x)$, it is implicitly assumed that the domain of g is the ring R under consideration, and normally its range is contained in $Z(R)$. For a given function $g : R \to R$, we write $D_g(x, y) := g(x + y) - g(x) - g(y)$. We typically use x as a generic element of R, so if we write $g(x) \in Z(R)$, we mean that this holds for all $x \in R$, whether or not this is explicitly stated.

We begin with a lemma that is useful for $n = 5, 9$.

Lemma 4.1. *If R is a ZP(n) or an AZP(n) ring, where $n = 2^m+1$ for some $m \in \mathbb{N}$, and if $2R \subset Z(R)$, then R is commutative.*

Proof. The ZP(n) and AZP(n) conditions coincide for rings R satisfying $2R \subset Z(R)$, so we assume that R is a ZP(n) ring. Let $f(x) := x - x^n$, so $f(R) \subset Z(R)$. By Lemma 2.3, we see that $\binom{n}{i}$ is odd only for $i \in \{0, 1, n-1, n\}$, so

$$D_f(x, x^{1+n}) = x^{2n} + x^{n^2} + z \in Z(R)\,,$$

where $z = z_x \in 2S \subset Z(S)$. Thus

$$x + x^2 = f(x) + f(x^2) + f(x^n) + x^{2n} + x^{n^2} \in Z(R)\,,$$

and so R is commutative. □

Forsythe and McCoy [2] gave an elementary proof that a ring R of prime characteristic p satisfying $x^p = x$ is commutative. Their now well-known method of proof is readily adapted to prove the following more general lemma; we include the proof for completeness.

Lemma 4.2. *If R is a ZP(p) or an AZP(p) ring for some prime p, and if $pR \subset Z(R)$, then R is commutative.*

Proof. Let $x, y \in R$ be arbitrary, and let $f(X)$ be either $X^p - X$ or $X^p + X$, depending on whether R is a ZP(p) or an AZP(p) ring. Expanding $f(x+iy) - f(x) - f(iy)$ for $i \in \{1, \ldots, p-1\}$, we see that

$$\sum_{j=1}^{p-1} i^j s_j = z_i \in Z(R)\,.$$

where s_j is the sum of all possible products of p factors, of which j are y and $p-j$ are x; for instance if $p = 3$, then $s_1 = x^2y + xyx + yx^2$, while $s_2 = xy^2 + yxy + y^2x$. This set of equations can be written in the form $Vs = z$, where $V = (v_{ij})_{i,j}$ is a (slightly nonstandard) Vandermonde matrix given by $v_{ij} = i^j$, and s, z are the column vectors whose transposes are defined by $s^t = (s_i)$, and $z^t = (z_i)$.

Denoting by δ the determinant of V, and r_i the cofactor of the element v_{i1}, $i = 1, \ldots, p-1$, we let $W = rV$, where r is the row vector $(r_1, \ldots, r_{p-1})$. Then $Ws = rz \in Z(R)$. But by basic linear algebra, we see that $Ws = \delta s_1$. By the theory of Vandermonde matrices, δ is a product of factors of the form a or $a-b$, for $1 \le a, b \le p-1$ and $a \ne b$. In particular δ is a unit in $\mathbb{Z}_p$, and so $s_1 \in Z(R)$. Thus $xs_1 = s_1x$, and so $x^py = yx^p$. Thus $x^p \in Z(R)$ for all $x \in R$. But $x^p \pm x \in Z(R)$, and so $x \in Z(R)$. □

Theorem 4.3. *ZP(5) rings are commutative.*

Proof. Let $f(x) := x - x^5$. Then $32f(x) - f(2x) = 30x \in Z(R)$. Since $x = 15x - 7(2x)$, R is a sum of the subrings $15R$ and $2R$. Moreover $(15x)(2y) = (2y)(15x) = 0$, so it suffices to show that each of these subrings is commutative. The ring $S := 15R$ satisfies $2S \subset Z(S)$, so it is commutative by Lemma 4.1.

Let $S := 2R$. Then $15S \subset Z(S)$, and Corollary 3.8 implies that $f(x) \in \mathfrak{C}(x)$ and that $x + x^3 = (x + x^2 + x^3 + x^4) - (x^2 + x^4) \in Z(S)$. But the centrality of $x + x^3$ implies that S is commutative. □

Theorem 4.4. *AZP(5) rings are commutative.*

Proof. Let $f(x) := x + x^5$. Again $32f(x) - f(2x) = 30x \in Z(R)$ and, arguing as in Theorem 4.3, we see that it suffices to prove that each of the subrings $15R$, $6R$, and $10R$ are commutative. Now $S := 15R$ satisfies $2S \subset Z(S)$, so it is commutative by Lemma 4.1, and $S = 6R$ is commutative by Lemma 4.2.

Finally suppose $S = 10R$, and so $3x \in Z(S)$ for all $x \in S$. Now $(f(x))^2 - f(x^2) = 2x^6 \in Z(S)$ for all $x \in S$, so $x^6 = 2(2x^6) - 3x^6 \in Z(S)$. Thus

$$x^6 + x^{24} - (x + x^4)^6 = x^{15} + z \in Z(R)$$

for some $z \in 3S \subset Z(S)$, and so $f(x^3) - x^{15} = x^3 \in Z(S)$ for all $x \in S$. Next

$$D_f(x, \pm x^2) = \mp x^6 + x^7 \pm x^8 - x^9 + z \in Z(S)\,,$$

for some $z \in Z(R)$. Now x^6 and x^9 are central, so $x^7 \pm x^8 \in Z(S)$. Taking a difference of these last expressions, we deduce that $x^8 \in Z(R)$ for all $x \in S$. Thus $x^{25} = (x^8)^2(x^3)^3 \in Z(S)$ and so $x = f(x) - f(x^5) + x^{25} \in Z(S)$ for all $x \in S$. □

Theorem 4.5. *ZP*(7) *rings are commutative.*

Proof. Let $f(x) := x - x^7$. By considering $k^7 f(x) - f(kx)$ for $k = 2, 3$, we see that $126R \subset Z(R)$ and $2184R \subset Z(R)$, and so $42R \subset Z(R)$, since $42 = \gcd(126, 2184)$. Thus it suffices to prove the result for the three subrings $14R$, $6R$, and $21R$.

Suppose first that $S = 6R$, so $7S \subset Z(S)$. Then commutativity follows by Lemma 4.2. Alternatively, Corollary 3.8 implies that

$$x + x^5 = \left(\sum_{x=1}^{6} x^i\right) - \left(\sum_{i=1}^{3} x^{2i}\right) - \left(\sum_{i=1}^{2} x^{3i}\right) + x^6 \in Z(S)\,,$$

and so S is commutative by Theorem 4.4.

Suppose next that $S = 14R$, and so $3S \subset Z(S)$. By Corollary 3.8, we see that $x^6 \in Z(S)$, and $x^3 = (x^3 + x^6) - x^6 \in Z(S)$ for all $x \in S$. Also $(f(x))^2 - f(x^2) = 2x^8 \in Z(S)$, so $x^8 = (2(2) - 3)x^8 \in Z(S)$. Thus $(x^8)^2(x^3)^{11} = x^{49} \in Z(S)$, and so $x = f(x) + f(x^7) + x^{49} \in Z(S)$ for all $x \in S$.

Finally suppose $S = 21R$, and so $2S \subset Z(S)$. Considering $D_f(x^j, x^{j+7})$ for $j \in \mathbb{N}$, and using the ZP(7) condition for powers of x^7, we see that $s_j(x) := \sum_{i=j+1}^{j+6} x^i \in Z(S)$. Thus $t_j(x) := s_j(x) - s_{j+1}(x) = x^{j+1} - x^{j+7} \in Z(R)$ for all $j \in \mathbb{N}$.

In particular, both $z := f(x)$ and $xz = t_1(x)$ are central. By Corollary 3.7, $e := x^6$ and $d := x^2 + x^4 + x^6$ both lie in $Z(S)$. Next

$$h(x) := x + x^3 + x^5 = f(x) + s_1(x) - d \in Z(S)\,,$$

and $D_h(x, x^2) = x^4 + x^5 + x^6 + x^9 + z$ for some $z \in 2S \subset Z(S)$. Since also $x^6 \in Z(S)$ and $t_2(x) = x^3 + x^9 \in Z(S)$, it follows that $x^3 + x^4 + x^5 \in Z(S)$. Subtracting this quantity from $h(x)$, we see that $x - x^4 \in Z(S)$. But now $x^3 - (x^3)^4 \in Z(S)$ and $x^{12} = (x^6)^2 \in Z(S)$, so $x^3 \in Z(S)$. Thus $h(x) - x^3 = x + x^5 \in Z(S)$, and so R is commutative by Theorem 4.4 (or indeed by Theorem 4.3, since $2S \in Z(S)$). □

Theorem 4.6. *AZP*(7) *rings are commutative.*

Proof. Let $f(x) := x + x^7$. As in the proof of Theorem 4.5, it suffices to prove the result for the three subrings $14R$, $6R$, and $21R$. For $S := 21R$, we have $2S \subset Z(S)$, so $x - x^7 \in Z(S)$ and commutativity follows by Theorem 4.5. If $S = 6R$, then $7S \subset Z(S)$ and commutativity follows by Lemma 4.2.

Finally suppose that $S = 14R$, and so $3S \subset Z(S)$. Now $(f(x))^2 - f(x^2) = 2x^8 \in Z(S)$, so $x^8 = (2(2) - 3)x^8 \in Z(S)$. Deleting an element of $3S$ and multiples of x^{8k} from $2D_f(x^2, -x^4) - 2D_f(x^2, x^4)$, we see that $x^{20} \in Z(R)$, and so $x^4 = f(x^4) - x^{20} \cdot x^8 \in Z(R)$. Now deleting an element of $3S$ and multiples of x^{4k} from $2D_f(x^1, -x^2) - 2D_f(x^1, x^2)$, we similarly see that $x^{10} \in Z(R)$, and hence that $h(x) := x^2 \in Z(R)$. Thus $2D_h(x, x^2) - 3x^3 = x^3 \in Z(R)$, and so $x = f(x) - (x^2)^2 x^3 \in Z(R)$. □

Theorem 4.7. *ZP*(9) *rings are commutative.*

Proof. Suppose R is a ZP(9) ring, so $f(x) := x - x^9 \in Z(R)$. By considering $k^9 f(x) - f(kx)$ for $k = 2, 3$, we see that $510R \subset Z(R)$ and $19680R \subset Z(R)$, and so $30R \subset Z(R)$, since $30 = \gcd(510, 19680)$. As usual, it suffices to prove the result under each of the additional assumptions $2R \subset Z(R)$, $3R \subset Z(R)$, and $5(R) \subset Z(R)$. In the case $2R \subset Z(R)$, R is commutative by Lemma 4.1.

In the other cases we have $mR \subset Z(R)$ for some odd m, so we conclude by Corollary 3.8 that x^8, x^4, $g(x) := x^2 + x^6$, and $x + x^3 + x^5 + x^7$ are all central.

Suppose $3R \subset Z(R)$. For all $t \in \mathbb{Z}$,

$$\begin{aligned} h(x,t) &:= D_g(x, tx^2) \\ &= 2tx^3 + 6tx^7 + 15t^2x^8 + 20t^3x^9 + 15t^4x^{10} + 6t^5x^{11} \in Z(R)\,. \end{aligned}$$

Thus $x^3 + x^9$ is central because it differs from $h(x, -1)$ by an element of $3R$, and so $x + x^3 = f(x) + (x^3 + x^9) \in Z(R)$, which implies R is commutative.

Suppose instead that $5R \subset Z(R)$. Now $(x + tx^2)^4 - x^4 - (tx^2)^4 \in Z(R)$, so $u(x,t) := 4tx^5 + 6t^2x^6 + 4t^3x^7 \in Z(R)$. Now $v(x,t) := u(x,t) - u(x,-t) = 8tx^5 + 8t^3x^7 \in Z(R)$. Since $8v(x,1) - v(x,2) = 48x^5$, we see that x^5 is central, and so $x = f(x) + f(x^9) - x^5(x^4)^{19} \in Z(R)$. □

5. Commutativity of ZP(n) rings for certain even n

In this section we prove commutativity of ZP(n) rings for some even values of n. Although the proofs for $n = 5, 7, 9$ in the last section contained some common ideas and methods, they were essentially ad hoc in nature. By contrast, the results below for even n each handle an infinite family of even numbers, and all associated proofs employ variations of a common method. The values of n that we can handle are all sums or differences of two powers of 2, and Lemma 2.2 is a key simplification at the beginning of these proofs.

Our methods do not apply to powers of 2 larger than 2. Indeed these numbers seem to be especially hard to treat by elementary means.

We do not consider AZP(n) for even n since Lemma 2.2 tells us that it is equivalent to ZP(n) in this case.

Since 6 is of the form $2^n + 2^m$, the commutativity of ZP(6) rings follows as a special case of Theorem 5.2 below. However we first present two proofs of this special case. The first is an ad hoc proof reminiscent of some of the earlier proofs for odd n, while the second is really a special case of the proof of Theorem 5.2 below.

Theorem 5.1. *ZP*(6) *rings are commutative.*

Proof 1 of Theorem 5.1. Assume that $f(x) := x - x^6 \in Z(R)$ for all x in a ring R. Now $2x \in Z(R)$ for all $x \in R$ and, since $D_f(x, x^2) \in Z(R)$, we see that $x^8 + x^{10} \in Z(R)$, and so $x^{24} + x^{30} \in Z(R)$. Adding $f(x^4) + f(x^5) \in Z(R)$ to this last expression, we see that $g(x) := x^4 + x^5 \in Z(R)$. Now $D_g(x, x^2) + f(x) \in Z(R)$ implies that $h(x) := x + x^9 \in Z(R)$, so $u(x) := h(x^2) + f(x^3) = x^2 + x^3 \in Z(R)$. Thus $v(x) := u(x^2) + f(x) = x + x^4 \in Z(R)$. Also

$$g(x)u(x) + f(x) = (x^4 + x^5)(x^2 + x^3) + x - x^6 \in Z(R)\,,$$

so $x + x^8 \in Z(R)$. However $v(x^2) = x^2 + x^8 \in Z(R)$, and so $x - x^2 \in Z(R)$, which implies commutativity. □

Proof 2 of Theorem 5.1. Assume that $f(x) := x - x^6 \in Z(R)$ for all x in a ring R. Since

$$D_f(x^i, x^{i+3}) + f(x^{i+1}) + f(x^{i+2}) \in Z(R)$$

and $2x \in Z(R)$, we deduce that $g_i(x) := x^{i+2} - x^{i+1} \in Z(R)$ for all $i \in \mathbb{N}$. Thus $x - x^2 = f(x) + \sum_{i=1}^4 g_i(x) \in Z(R)$, which implies that R is commutative. □

We now prove two results for even numbers of the form $2^n + 2^m$.

Theorem 5.2. *If R is a ZP$(2^n + 2^m)$ ring, where $m > 0$ and $n - m \in \{1, 2\}$, then R is commutative.*

Proof. First, we note that $2R \subset Z(R)$. Let $N := 2^n$, $M := 2^m$, $K := N + M$, $r := N/M$, and $f(x) := x + x^K$, so that $f : R \to Z(R)$. We claim that

$$s(\alpha, \beta) := x^\alpha - x^\beta \in Z(R)\,, \qquad \text{whenever } \alpha, \beta \in \mathbb{N} \setminus \{1\} \text{ and } (r-1) \mid (\beta - \alpha)\,.$$

The assumption $n - m \le 2$ is not required for this claim.

According to Lemma 2.3, the binomial coefficient $\binom{N+M}{j}$, $1 \le j \le K - 1$, is odd only when $j = M$ and $j = N$. It follows that for all $i \in \mathbb{N}$,

$$f(x^i + x^{i+r+1}) + f(x^i) + f(x^{i+r+1}) = x^{(i+1)(N+M)} + x^{(i+r)(N+M)} + z \in Z(R)\,,$$

for some $z \in Z(R)$. Adding $f(x^{i+1}) + f(x^{i+r})$ to this last expression, we see that

$$e(x, i) := x^{i+1} - x^{i+r} \in Z(R)\,, \qquad i \in \mathbb{N}\,.$$

Since

$$\sum_{k=0}^{t-1} e(x, i + (r-1)k) = x^{i+1} - x^{i+1+t(r-1)}\,,$$

the claim follows.

If $n = m + 1$, then $r - 1 = 1$ and

$$x - x^2 = f(x) - f(x^2) - s(N + M, 2(N + M)) \in Z(R)\,,$$

which implies that R is commutative.

Suppose instead that $n = m + 2$, and so $r - 1 = 3$. $N + M$ is equivalent to either 1 or 2 mod 3. In the first case, by taking $\alpha = 7$ and $\beta = N + M$, we see that $x - x^7 \in Z(R)$, and so R is commutative by Theorem 4.5. In the second case, by taking $\alpha = 2$ and $\beta = N + M$, we see that $x - x^2 \in Z(R)$, and so R is again commutative. □

By the above proof, we see that if R is a ZP$(2^n + 2^m)$ ring for any $n > m > 0$, then R is also a ZP(k) ring whenever $k \ge 2$ and $(r-1) \mid (2^n + 2^m - k)$. This enabled us to give an elementary proof of commutativity above whenever $0 < n - m \le 2$, but it also gives an elementary proof of commutativity in certain other cases.

Theorem 5.3. *Suppose R is a ZP$(2^n + 2^m)$ ring, where $n > m > 0$, and $n + 1$ is coprime with $d := n - m$. Then R is commutative.*

Proof. Let $k := 2^d - 1$, $K := 2^n + 2^m$, and $D(x, a, b) := x^{2^a} - x^{2^b}$ for $0 \le a, b \in \mathbb{Z}$. By the proof of Theorem 5.2, $x^\alpha - x^\beta \in Z(R)$ whenever $\alpha, \beta \in \mathbb{N} \setminus \{1\}$, and $k \mid (\alpha - \beta)$. By factorization, we see that if $d \mid (a - b)$, $a, b \in \mathbb{N}$, then $k \mid (2^a - 2^b)$, and so $D(x, a, b) \in Z(R)$.

Since $K = 2^{n-d}(2^d + 1)$ and $2^d + 1 \equiv 2 \pmod{k}$, we see that $K \equiv 2^{n+1} \pmod{k}$ and so R is a ZP(2^{n+1}) ring. Since

$$D(x, 0, n + 1 - jd) = D(x, 0, n + 1) + D(x, n + 1, n + 1 - jd) \in Z(R)\,,$$

for all $j \in \mathbb{Z}$ such that $n + 1 - jd > 0$, we see that R is also a ZP(2^{n+1-jd}) ring for all such j.

Since $n+1$ is not divisible by d, we may choose j so that $a := n+1-jd$ satisfies $1 \le a < d$. Note that a and d are coprime, so we can choose $b, c \in \mathbb{N}$ such that $ba - cd = 1$. The ZP(2^a) condition tells us that $D(x, (i-1)a, ia) \in Z(R)$ for each $0 \le i < b$. Summing these expressions, we see that $D(x, 0, ba) = D(x, 0, cd + 1) \in Z(R)$, and so

$$x - x^2 = D(x, 0, cd + 1) + D(x, cd + 1, 1) \in Z(R)\,,$$

which implies that R is commutative. □

Note that the above corollary says that if d is prime and $n+1$ is not a multiple of d, then R is commutative. It also tells us that if $n-m$ is a divisor of n, then again R is commutative.

We now consider numbers of the form $2^n - 2^m$.

Theorem 5.4. *If R is a ZP$(2^n - 2^m)$ ring where $m > 0$ and $n - m \in \{2, 3\}$, then R is commutative.*

Proof. Much of the proof is similar to that of Theorem 5.2, so we concentrate on the differences. Let $N := 2^n$, $M := 2^m$, $K := N - M$, $r := N/M$, and $f(x) := x + x^K$, so that $f : R \to Z(R)$, and again $2R \subset Z(R)$. We claim that $s(\alpha, \beta) := x^\alpha - x^\beta \in Z(R)$ whenever $\alpha, \beta \in \mathbb{N} \setminus \{1\}$ and $(r-2) \mid (\beta - \alpha)$.

According to Lemma 2.3, the binomial coefficient $\binom{N-M}{j}$, $1 \le j \le K-1$, is odd precisely when j is a multiple of M. It follows that

$$S(x, i) := f(x^i + x^{i+r-1}) + f(x^i) + f(x^{i+r-1}) = x^{i(N-M)} \sum_{k=1}^{r-2} x^{k(N-M)} + z \in Z(R)\,,$$

for some $z \in R$. Considering $S(x,i) - S(x, i+1)$, we see that

$$x^{(i+1)(N-M)} - x^{(i+r-1)(N-M)} \in Z(R)\,, \qquad i \in \mathbb{N}\,.$$

The claim now follows in a similar fashion to the claim in the proof of Theorem 5.2.

If $n = m+2$, then $r - 2 = 2 \mid (N - M - 2)$, so as in Theorem 5.2 we see that $x - x^2 \in Z(R)$, and so R is commutative.

Suppose instead that $n = m+3$, and so $r - 2 = 6$. Now $N - M$ is equivalent to either 2 or 4 mod 6, depending on the parity of N. By taking $\beta = N - M$, and α to be 2 or 10, we see that R is also a ZP(α) ring. Thus R is commutative (using Theorem 5.2 for $\alpha = 10$). □

As for ZP$(2^n + 2^m)$, the claim in the above proof can be used to prove that ZP$(2^n - 2^m)$ rings are commutative for certain other numbers n, m, as evidenced by the following result.

Theorem 5.5. *Suppose R is a ZP$(2^n - 2^m)$ ring, where $n - 1 > m > 0$, and $n - 1$ is coprime with m. Then R is commutative.*

Proof. Let $d := n - m - 1$, $k := 2^d - 1$, $K := 2^n - 2^m$, and $D(x, a, b) := x^{2^a} - x^{2^b}$ for $0 \le a, b \in \mathbb{Z}$. By the proof of Theorem 5.4, $x^\alpha - x^\beta \in Z(R)$ whenever $\alpha, \beta \in \mathbb{N} \setminus \{1\}$ and $(2k) \mid (\alpha - \beta)$. By factorization, we see that if $d \mid (a - b)$, $a, b \in \mathbb{N}$, then $2k \mid (2^a - 2^b)$, and so $D(x, a, b) \in Z(R)$.

Since $K = 2^{n-d-2}(2^{d+2} - 2)$ and $2^{d+2} - 2 \equiv 2 \pmod{2k}$, we see that $K \equiv 2^{n-1}$ (mod $2k$) and so R is a ZP(2^{n-1}) ring. As in the proof of Theorem 5.3, it follows that R is a ZP(2^a) ring where $a := n - 1 - jd$ satisfies $1 \le a < d$. Now $n - 1$ and d are coprime, and so a and d are coprime. Choosing $b, c \in \mathbb{N}$ such that $ba - cd = 1$, we deduce as in the proof of Theorem 5.3 that

$$x - x^2 = D(x, 0, ba) + D(x, cd + 1, 1) \in Z(R)\,,$$

which implies that R is commutative. □

Note that Theorem 1.2 follows immediately from the combination of Theorems 2.1, 4.4, and 4.6. We now prove Theorem 1.1.

Proof of Theorem 1.1. The commutativity of ZP(n) rings for $n = 2, 3$ is given by Theorem 2.1, and for $n = 5, 7, 9$ by Theorems 4.3, 4.5, and 4.7, respectively. Each of Theorems 5.2, 5.3, 5.4, and 5.5 provide us with infinite families of even numbers n for which ZP(n) rings are necessarily commutative. Finally with regards to the specific values of even $n \le 30$ that are listed, commutativity follows when $n \in \{6, 10, 12, 20, 24\}$ by Theorem 5.2, when $n = 18$ by Theorem 5.3, when $n \in \{14, 28\}$ by Theorem 5.4, and when $n = 30$ by Theorem 5.5. □

As mentioned in the Introduction, it seems especially difficult to prove commutativity by elementary means of ZP(n) rings when $n > 2$ is a power of 2. We would be very interested in any such proof, even just for $n = 4$.

References

[1] G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. **31** (1935), 433–454.

[2] A. Forsythe and N.H. McCoy, *On the commutativity of certain rings*, Bull. Amer. Math. Soc. **52** (1946), 523–526.

[3] J.W.L. Glaisher, *On the residue of a binominal-theorem coefficient with respect to a prime modulus*, Quart. J. Pure Appl. Math. **30** (1899), 150–156.

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

[5] I.N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. **75** (1953), 864–871.

[6] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.

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

[8] D. MacHale, *Rings that are nearly Boolean II*, Proc. Roy. Irish Acad. Sect. A **83** (1983), 165–167.

[9] D. MacHale, *Rings that are nearly Boolean III*, Proc. Roy. Irish Acad. Sect. A **86** (1986), 165–167.

[10] Y. Morita, *Elementary proofs of the commutativity of rings satisfying $x^n = x$*, Memoirs Def. Acad. Jap. **XVIII** (1978), 1–23.

[11] T. Ramsamujh, *Equational Logic and Abstract Algebra*,
`http://sections.maa.org/florida/proceedings/2001/ramsamujh.pdf`

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