Research Article

Powers of Commutators and Anticommutators

Stephen M. Buckley[1] and Desmond MacHale[2]

[1] *Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Kildare, Ireland*
[2] *School of Mathematical Sciences, University College Cork, Cork, Ireland*

Correspondence should be addressed to Stephen M. Buckley, stephen.buckley@maths.nuim.ie

For $n = 3, 4$, we give elementary proofs of commutativity of rings in which the identity $c^n = c$ holds for all commutators c. For even n, we show that the commutativity of rings satisfying such an identity is equivalent to the anticommutativity of rings satisfying the corresponding anticommutator equation.

1. Introduction

Let us recall a commutativity result of Herstein; here and later, $[x, y] := xy - yx$ denotes the (additive) *commutator* of the pair x, y.

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

We have the following corresponding result for *anticommutators* $\langle x, y \rangle := xy + yx$. A ring is said to be *anticommutative* if $\langle x, y \rangle = 0$ for all x, y.

Theorem B (see MacHale [2]). *A ring R is anticommutative if and only if for each $x, y \in R$ there exists an even integer $n(x, y) > 1$ such that $\langle x, y \rangle^{n(x,y)} = \langle x, y \rangle$.*

The restriction to even integers above is necessary: $\mathbb{Z}_3$ fails to be anticommutative even though it satisfies the identity $\langle x, y \rangle^n = \langle x, y \rangle$ for every odd n.

The proofs of the above pair of results depend on Jacobson's structure theory of rings. In the case of the much stronger identity $x^{n(x)} = x$ for some $n(x) > 1$, which was proved to imply commutativity by Jacobson [3], there are *elementary proofs* (meaning proofs that do not

require structure theory) of many special cases of the result. For instance, in the case of the identity $x^n = x$, $n > 1$ fixed, elementary commutativity proofs were given by Morita [4] for all odd $n \leq 25$, and all even $n \leq 50$, and by MacHale [5] 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 [6] 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.

By comparison, there are far fewer elementary proofs in the literature of special cases of Theorems A and B, and they appear to be more difficult to construct. This is perhaps not surprising, since the sets of commutators or anticommutators do not in general form even additive subgroups of a ring.

To aid our subsequent discussion, let us call R a CP(S) *ring*, where $S \subset \mathbb{N} \setminus \{1\}$ if, for each $x, y \in R$, there exists $n(x, y) \in S$ such that $[x, y]^{n(x,y)} = [x, y]$; CP stands for commutator power. Similarly we call R an ACP(S) *ring*, where $S \subset 2\mathbb{N}$ if, for each $x, y \in R$, there exists $n(x, y) \in S$ such that $\langle x, y \rangle^{n(x,y)} = \langle x, y \rangle$. We write CP($n$) and ACP($n$) instead of CP($\{n\}$) and ACP($\{n\}$), respectively. A CP *ring* and an ACP *ring* mean a CP($\mathbb{N} \setminus \{1\}$) ring and an ACP($2\mathbb{N}$) ring, respectively.

By the above theorems, all CP rings are commutative and all ACP rings are anticommutative. An elementary proof of the commutativity of CP(n) rings was given for $n = 2$ in [7], and for $n = 3$ in [8]. The only other elementary proof of a special case of Theorem A of which we are aware is the proof in [9] that a CP ring R is necessarily commutative if its centre is an ideal. In Section 2, we prove that CP(4) rings are commutative and also give a new proof that CP(3) rings are commutative; both proofs are elementary.

As for ACP(n) rings, an elementary proof of their anticommutativity was given in [2] for $n = 2$, but we are not aware of any other such proofs in the literature. In Section 3, we give an elementary proof that for any given $S \subset 2\mathbb{N}$, the commutativity of CP(S) rings is equivalent to the anticommutativity of ACP(S) rings. Thus the aforementioned proof of commutativity of CP(4) rings yields an elementary proof of anticommutativity of ACP(4) rings, and the proof that a CP($2\mathbb{N}$) ring is necessarily commutative if its centre is an ideal yields an elementary proof of anticommutativity of an ACP($2\mathbb{N}$) ring whose centre is an ideal.

2. Commutators

Suppose that R is a ring. We gave an elementary proof in [8, Theorem 17] that CP(3) rings are commutative. Here we give a somewhat similar (but surprisingly much easier!) proof that CP(4) rings are commutative. We then give a new proof that CP(3) rings are commutative. We begin with two well-known lemmas that give useful information about all CP rings and include the short proofs for convenience.

Lemma 2.1. *Suppose that R is a CP ring. Then*

$$xy = 0 \implies yx = 0, \quad x, y \in R. \tag{2.1}$$

Proof. Let $n > 1$ be such that $(yx - xy)^n = yx - xy$ for some $n > 1$. Then

$$yx = (yx)^n = y(xy)u = 0, \tag{2.2}$$

where $u = x$ (if $n = 2$) or $u = x(yx)^{n-2}$ (if $n > 2$). $\square$

Lemma 2.2. *Suppose a ring R satisfies* (2.1). *Then idempotents are central. Consequently, $x^{m-1} \in Z(R)$ whenever $x \in R$ satisfies $x^m = x$ for some $m > 1$.*

Proof. Let e be an idempotent, let $y \in R$, and let $d = ey - eye$. Clearly $de = 0$, and so $ed = ey - eye = 0$. By symmetry, $ye = eye = ey$.

The last statement follows from the first since if $m > 2$, then

$$\left(x^{m-1}\right)^2 = x^m x^{m-2} = xx^{m-2} = x^{m-1}. \tag{2.3}$$

$\square$

We now recall the following elementary result [8, Theorem 19].

Lemma C. *If $[x, z]$ and $[y, z]$ commute for all x, y, z in some 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 $c = 0$.*

The commutativity of CP(4) rings is now easily established.

Theorem 2.3. *CP(4) rings are commutative.*

Proof. Let R be CP(4). In view of Lemma C, it suffices to prove that $cd = dc$ whenever $c = [x, z]$ and $d = [y, z]$, for some $x, y, z \in R$. Since $-c = [-x, y]$, we have $c = c^4 = (-c)^4 = -c$, so $2c = 0$. It follows that $f(c) := c + c^2$ is an idempotent, and so $f(c) \in Z(R)$ by Lemma 2.2. Since $c + d = [x + y, z]$ is a commutator, it follows that $f(c + d) - f(c) - f(d) = cd + dc \in Z(R)$. In particular $c(cd + dc) = (cd + dc)c$, and so $c^2 d = dc^2$. Since $c + c^2 \in Z(R)$, it follows that $cd = dc$ as required. $\square$

We now give a new proof of the commutativity of CP(3) rings. Like the original proof in [8], this proof uses our two lemmas above. However it avoids the reduction of Lemma C.

Theorem 2.4. *CP(3) rings are commutative.*

Proof. Consider $c = [x, y]$ for fixed $x, y \in R$, so that $e := c^2$ is a central idempotent. Let $a = ex$, $b = ey$, and let S be the subring of R generated by a and b. It is also clear that $c = [a, b]$ and, since $ex = xe = x$ for $x \in \{a, b\}$, e is a unity for S. Note that there is a symmetry between the three elements a, b, and $a + b$: S is also generated by $a + b$ and b, and $c = [a + b, b]$. Since e is a unity, $c = c^{-1}$ in S, and any equation of the form $uc = vc$ in S implies that $u = v$.

We will use the fact that the following are commutators lying in S: $ca = [a, ba]$, $ac = [a, ab]$, $w := [a, c]$, $cw = [ca, c] = cac - a$, and $wc = [ac, c] = a - cac = -cw$. Thus we can apply the CP(3) identity to these, and their squares are central idempotents. In particular, note that

$$wc = wc(wc)^2 = w(wc)^2 c = w^2 cw = -w^3 c = -wc. \tag{2.4}$$

Thus $2wc = 0$ and $2w = 0$, so $2a$ commutes with c (and trivially with a).

Now note that if any $d \in S$ commutes with a and c, then $dc = [a, db]$ is a commutator so

$$dc = (dc)^3 = d^3 c^3 = d^3 c. \tag{2.5}$$

Thus $d = d^3$, and d^2 is a central idempotent (in R). Now also $s = d + d^2$ commutes with a and c and $ds = d^2 + d^3 = s$, so $s^2 = 2s$. Thus $s = s^3 = 2s^2 \in Z(R)$, and $d = s - d^2 \in Z(R)$. Also, since $(ac)^2$ is a central idempotent,

$$(ac)^2 = c(ac)^2 c^{-1} = (ca)^2. \tag{2.6}$$

Applying this to $d = 2a$, we get that $2a \in Z(R)$, so $2c = [2a, b] = 0$, and so $2e = (2c)(c) = 0$. Thus $2S = 0$.

Now using (2.6) and the CP(3) property for the commutators ac, ca, and c, we see that

$$\begin{aligned}
w = w^3 \\
= (ac)^3 - (ac)^2(ca) - (ac)(ca)(ac) - (ca)(ac)^2 + (ac)(ca)^2 \\
\quad + (ca)(ac)(ca) + (ca)^2(ac) - (ca)^3 \\
= ac - ca - a^3c - ca + ac + ca^3 + ac - ca \\
= 3w + ca^3 - ac^3.
\end{aligned} \tag{2.7}$$

But $2w = 0$, so $ca^3 = a^3c$. Thus $a^3 \in S$ commutes with a and c, so, by our earlier analysis for $d = a^3$, we see that $a^3 \in Z(R)$.

Note that S is also generated by $e + a$ and b, since $[e + a, b] = c$ and $e + a - c^2 = a$. Thus we may replace a by $e + a$ in the last paragraph and deduce that $(e + a)^3 \in Z(R)$. Expanding this and using the fact that $2S = 0$, we deduce that $a + a^2 \in Z(R)$. By symmetry, both $b + b^2$ and $(a + b) + (a + b)^2$ also lie in $Z(R)$, so

$$ab + ba = (a + b) + (a + b)^2 - \left(a + a^2\right) - \left(b + b^2\right) \in Z(R). \tag{2.8}$$

Thus $a(ab + ba) = (ab + ba)a$, so $a^2 \in Z(S)$ (since S is generated by a and b). But $a + a^2 \in Z(S)$, so $a \in Z(S)$ and $c = [a, b] = 0$, as required. $\qquad \square$

3. Anticommutators

In this section, we give an elementary proof of the following result.

Theorem 3.1. *Suppose that $S \subset 2\mathbb{N}$. Then all CP(S) rings are commutative if and only if all ACP(S) rings are anticommutative.*

In view of Theorem 2.3, we thus have an elementary proof of the following result.

Corollary 3.2. *ACP(4) rings are anticommutative.*

Note that Theorem 3.1 allows us to deduce Theorem B from Theorem A. Of course this is not an elementary proof, since Herstein's result relies on structure theory, but it is an alternative to the proof in [2] which appeals both to Herstein's result and to structure theory.

To prove Theorem 3.1, we first need some preparatory lemmas. We omit the simple proof of our first lemma, which follows just like that of Lemma 2.1, and which implies that idempotents are central in ACP rings.

Lemma 3.3. *Every ACP ring R satisfies (2.1); that is, $yx = 0$ whenever $xy = 0$, $x, y \in R$.*

Observation 1. If $a^m = a$ and $b^n = b$, for some $m, n \in \mathbb{N} \setminus 1$, then $a^t = a$ and $b^t = b$, where $t = (m-1)(n-1) + 1$. Moreover if m, n are both even, then so is t.

We now state a simple but useful lemma.

Lemma 3.4. *Suppose that R is an ACP ring, Then*

(a) $2\langle x, y \rangle = 0$ *for all* $x, y \in R$.

(b) $2x^2 = 0$ *for all* $x \in R$. *If instead R is a $CP(2\mathbb{N})$ ring then*

(c) $2[x, y] = 0$ *for all* $x, y \in R$.

Proof. Both $a := \langle x, y \rangle$ and $-a = \langle -x, y \rangle$ are anticommutators. Using Observation 1 and the ACP condition, we see that that there is an even integer $t > 0$ such that $a = a^t = (-a)^t = -a$, which gives (a). We omit the proof of (c), which is very similar to that of (a).

As for (b), first let $x = y$ in (a) to get $4y^2 = 0$ for all $y \in R$. Next use the ACP condition to deduce that there exists some even integer $n > 0$ such that $(2x^2)^n = \langle x, x \rangle^n = 2x^2$. But $(2x^2)^n = 2^n(x^n)^2 = 0$ because of the identity $4y^2 = 0$. Thus $2x^2 = 0$, as required. □

We now prove an anticommutator analogue of Lemma C.

Lemma 3.5. *Suppose that $\langle x, z \rangle$ and $\langle y, z \rangle$ commute for all x, y, z in some ring R. Then $\langle x, y \rangle^2 [x, y] = 0$ for all $x, y \in R$. If R is additionally assumed to be an ACP ring, then R is anticommutative.*

Proof. Suppose $a = \langle x, y \rangle$ for some $x, y \in R$, and we also write $c = [x, y]$. Note that $ax = \langle x, yx \rangle = \langle yx, x \rangle$ and $a = \langle y, x \rangle$, so by assumption ax and a commute. Similarly a commutes with $xa = \langle xy, x \rangle$. Thus $a(ax) = a(xa) = xa^2$ where in each case the parentheses enclose one of the factors that is commuted in the next equation. Thus squares of anticommutators are central and moreover we have $a^2 x = axa = xa^2$. Since ax and ya are anticommutators, it follows that

$$\left(a^2\right)(xy) = (ax)(ya) = (yaa)x = a^2 yx. \tag{3.1}$$

Subtracting the extreme right hand side from the extreme left, we get that $a^2 c = 0$, as required.

By distributivity, we have $ac = xyxy - yxyx + yxxy - xyyx$. Assume now that R is an ACP ring. Using Lemma 3.4(b), we see that $-yxyx = yxyx$ and $-xyyx = xyyx$, and so $a^2 = ac$. Thus $a^3 = a^2 c = 0$. Now $a = a^{n(x,y)} = a^{2n(x,y)-1} = 0$ because $2n(x, y) - 1 \geq 3$. □

Proof of Theorem 3.1. We suppose first that R is an ACP(S) ring for some fixed $S \subset 2\mathbb{N}$, and we suppose that every CP(S) ring is commutative. By Lemma 3.5, it suffices to prove that $ab = ba$, where $a = \langle x, z \rangle$, $b = \langle y, z \rangle$, and $x, y, z \in R$ are fixed but arbitrary.

Now there are even integers $m, n \in \mathbb{N}$ such that $a^m = a$ and $b^n = b$. Since idempotents are central, it follows that a^{m-1}, b^{n-1}, and $e := a^{m-1}b^{n-1}$ are all central idempotents. Thus if we write $a' = \langle ex, ez \rangle$ and $b' := \langle ey, ez \rangle$, then $a' = e^2 a = ea$, $b' = e^2 b = eb$, and
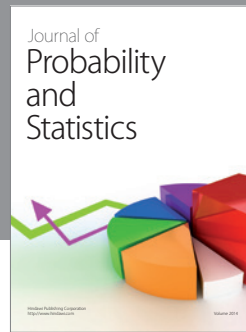
$$a'b' = \left(e^2\right)\left(e^2\right)ab = eab = a^m b^n = ab. \tag{3.2}$$

Similarly $b'a' = ba$. Thus $ab + ba = 0$ if and only if $a'b' + b'a' = 0$ and, since $a'b' \in eR = Re$, it suffices to show that eR is anticommutative. By Lemma 3.4, $2e = 0$ so eR has characteristic 2 and is an ACP(S) ring. But for rings of characteristic 2, the ACP(S) condition is equivalent to the CP(S) condition, and so by assumption eR is commutative, and commutativity is also equivalent to anticommutativity in rings of characteristic 2, so we are done.

The converse direction is very similar. Assume that ACP(S) rings are anticommutative, where $S \subset 2\mathbb{N}$ is fixed. Suppose R is a CP(S) ring. We first reduce to proving that $cd = dc$, where $c = [x, z]$, $d = [y, z]$, and $x, y, z \in R$ are fixed but arbitrary. Writing $e = c^{m-1}d^{n-1}$, where $c^m = c$ and $d^n = d$, we see as before that $[ex, ez][ey, ez] = cd$ and $[ey, ez][ex, ez] = dc$, so the required result follows from the commutativity of eR. But R has characteristic 2, so we can finish the result as before. $\qquad\square$

References

[1] I. N. Herstein, "A condition for the commutativity of rings," *Canadian Journal of Mathematics*, vol. 9, pp. 583–586, 1957.

[2] D. MacHale, "An anticommutativity consequence of a ring commutativity theorem of Herstein," *The American Mathematical Monthly*, vol. 94, no. 2, pp. 162–165, 1987.

[3] N. Jacobson, "Structure theory for algebraic algebras of bounded degree," *Annals of Mathematics. Second Series*, vol. 46, pp. 695–707, 1945.

[4] Y. Morita, "Elementary proofs of the commutativity of rings satisfying $x^n = x$," *Memoirs of the Defense Academy. Mathematics, Physics, Chemistry and Engineering*, vol. 18, no. 1, pp. 1–24, 1978.

[5] D. MacHale, "Rings that are nearly Boolean. III," *Proceedings of the Royal Irish Academy A*, vol. 86, no. 1, pp. 31–33, 1986.

[6] J. W. Wamsley, "On a condition for commutativity of rings," *Journal of the London Mathematical Society*, vol. 4, pp. 331–332, 1971.

[7] M. Ó Searcóid and D. MacHale, "Two elementary generalisations of Boolean rings," *The American Mathematical Monthly*, vol. 93, no. 2, pp. 121–122, 1986.

[8] S. M. Buckley and D. MacHale, "Variations on a theme: rings satisfying $x^3 = x$ are commutative," to appear in *The American Mathematical Monthly*.

[9] S. M. Buckley and D. MacHale, "Rings with ideal centres," preprint.