DUO RINGS: SOME APPLICATIONS TO COMMUTATIVITY THEOREMS

Howard E. Bell

(received January 2, 1968)

Proofs of commutativity theorems for general rings usually employ the Jacobson structure theory; however, alternative approaches to the "$x^n = x$ theorem" [1, 2] suggest that the power of the Jacobson theory is not required. In this note we prove two commutativity theorems of Herstein in an elementary way. Both proofs involve establishing first that the rings under consideration are duo-rings - rings in which every one-sided ideal is two-sided.

THEOREM 1. *Let R be a ring such that for every $x, y \in R$ there is an integer $n(x, y) > 1$ for which $(xy - yx)^{n(x,y)} = xy - yx$. Then R is commutative.*

THEOREM 2. *If $n > 1$ is a fixed positive integer and $x^n - x$ is central for every element x of the ring R, then R is commutative.*

We shall refer to rings satisfying the hypotheses of Theorem 2 as *H-rings*, and we shall denote the centre of R by Z. An ideal P will be called *completely prime* if $ab \in P$ implies $a \in P$ or $b \in P$.

1. *Proof of Theorem 1.* The proof in the case that R is a division ring may be found in [3]. Our extension to the general case is a modification of Herstein's readily-available proof of the "$x^n = x$ theorem" [2, 7], and we note only the necessary changes.

Observe that

(1) $(xy - yx)^n = xy - yx$ implies $(xy - yx)^{n-1}$ is idempotent.

(2) R has no non-zero nilpotent commutators.

(3) In any ring without non-zero nilpotent commutators, idempotents are central, since for e idempotent and $x \in R$ we have $[e(ex) - (ex)e]^2 = [e(xe) - (xe)e]^2 = 0$.

Using these observations we show that R is a duo ring. Let I be a right ideal and $a \in I$. Then

$$u = a(ar - ra) = a(ar) - (ar)a \in I.$$

Since u is a commutator, there is a $k > 1$ such that $u^k = u$ and u^{k-1} is central; hence

$$ra(ar - ra) = ru = ru^{k-1}u = u^{k-1}ru \in I.$$

Since $ar \in I$, we have $(ar - ra)^2 \in I$ and therefore $(ar - ra)^n \in I$ for all $n \geq 2$. Thus, $ar - ra \in I$ and $ra \in I$.

Once we know that R is a duo ring, the extension from the division ring case to the general case proceeds as in [2].

2. Theorem 2 for division rings. For the sake of completeness, we include the proof given in [4]. Suppose the division ring R is an H-ring and $r \notin Z$. Then for any $z \in Z$, we have $z^n(r^n - r) \in Z$ and $(zr)^n - zr \in Z$, which imply $(z^n - z)r \in Z$. This result is incompatible with the fact that $r \notin Z$ unless $z^n - z = 0$; thus $z^n = z$ for all $z \in Z$ and Z is a finite field.

Now let x be an arbitrary element of R. Since $x^{n^i} - x \in Z$ for all $i \geq 1$, there exist unequal integers j, k such that $x^{n^j} = x^{n^k}$, which implies $x^{n(x)} = x$. But this contradicts the "$x^n = x$ theorem"; hence we must have had $R = Z$.

3. Theorem 2 for R without zero-divisors. In this case we use a well-known device (6) to embed R in a field. Let $Z^\#$ be the set of non-zero elements of Z; and note that $Z^\#$ is non-empty, since for a given $a \neq 0$ either $a^n - a \in Z^\#$ or (by (3)) $a^{n-1} \in Z^\#$. If we define an equivalence relation $\sim$ on $R \times Z^\#$ by making $(r_1, z_1) \sim (r_2, z_2)$ if and only if $r_1 z_2 = r_2 z_1$, the set of equivalence classes $[r, z]$ forms a ring R^* with addition and multiplication defined by

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b][c, d] = [ac, bd].$$

The ring R^* has an identity element $[z, z]$, and R is embedded in R^* by the mapping $\phi(r) = [rz, z]$. Moreover, the centre Z^* of R^* is the set of classes $[r, z]$ where $r \in Z$; and the invertible elements of R^* are the classes $[r, z]$ where $r \in Z^\#$. We establish Theorem 2 for R without zero-divisors by showing that R^* is a division ring and an H-ring.

Let U^* be a non-zero right ideal of R^* and $[a, z]$ a non-zero element of U^*. Then $[a, z][z^2, z] = [az, z] \in U^*$; and, depending on whether $a^n - a$ is non-zero or zero, $[az, z]^n - [az, z] = [(a^n - a)z^{n+1}, z^{n+1}]$

https://doi.org/10.4153/CMB-1968-042-0 Published online by Cambridge University Press

or $[az, z]^{n-1} = [a^{n-1}z^{n-1}, z^{n-1}]$ is an invertible element of U*. Hence, R* has no proper right ideals and must be a division ring.

The condition that R* is an H-ring reduces to the statement that $a^n z - az^n \in Z$ for all $a \in R$ and all $z \in Z$. To establish the latter, we need only note that $(a^n - a)(z^n + z) = a^n z^n - az + a^n z - az^n \in Z$ and that $a^n z^n - az \in Z$.

4. Theorem 2 for R without non-zero nilpotent elements. We show that R contains a family $\{P_\alpha\}$ of completely prime ideals with zero intersection, in which case R is a subdirect sum of the rings $\frac{R}{P_\alpha}$, each of which is an H-ring without zero-divisors and is thus commutative. The existence of the P_α is explicitly stated in Lemma 1, which is well-known. Our proof has an element of novelty - a non-standard kind of annihilator ideal.

LEMMA 1. A ring R without non-zero nilpotent elements contains completely prime ideals, the intersection of all of which is zero.

Proof. Under the hypotheses of Lemma 1, $ax = 0$ implies $xa = 0$ and thus for any $r \in R$, $rxa = 0$ and $arx = 0$. Hence if a finite product of elements of R is zero, the insertion of additional factors in any position leaves a product of zero. We shall refer to this result as the insertion-of-factors principle (IFP).

Now consider m*-systems, multiplicative subsemigroups of R which do not contain 0. Clearly R has m*-systems (e.g. $\{a, a^2, a^3, \ldots\}$ for any non-zero $a \in R$); and a straightforward application of Zorn's Lemma shows that every m*-system is contained in a maximal m*-system.

Let M be a maximal m*-system and define

$$A(M) = \{x \in R \mid ax = 0 \text{ for at least one } a \in M\}.$$

By IFP, A(M) is a two-sided ideal. If $x \notin M$, then the multiplicative subsemigroup generated by M and x must contain 0; and since R has no non-zero nilpotent elements, some finite product containing x as at least one factor and having at least one factor from M must be zero. Repeated application of IFP establishes the existence of an $m \in M$ such that mx is nilpotent and hence 0. Therefore the set-theoretic complement of A(M) is M, and A(M) is a completely prime ideal. Clearly every non-zero element of R is excluded from at least one of the ideals A(M).

https://doi.org/10.4153/CMB-1968-042-0 Published online by Cambridge University Press

5. H-rings are duo rings. It follows immediately from the definition of H-ring that nilpotent elements are central. Hence the nilpotent elements of R form an ideal N; and $\frac{R}{N}$, having no non-zero nilpotent elements, is commutative. Thus all commutators of R are nilpotent, hence central. This fact enables us to prove

LEMMA 2. If R is an H-ring, then every one-sided ideal of R is two-sided.

Proof. Let I be a right ideal, $a \in I$, and $r \in R$. Since commutators are central, we have

$$r(ra) - (ra)r = r(ra - ar) = (ra - ar)r \in Z;$$

i.e. $rar = ar^2 + z_1$, where $z_1 \in Z$. It follows that $(ra)^2 \in I$ and $(ra)^n \in I$.

Since R is an H-ring, we have $ra = (ra)^n + z_2$, where z_2 is central; and thus from $(ra)^n \in I$ follows the result that $ra^2 \in I$ and $ra^n \in I$. Using the fact that $a^n - a \in I \cap Z$, we have $r(a^n - a) = (a^n - a)r \in I$; hence $ra = ra^n - (a^n - a)r \in I$.

6. Theorem 2 for subdirectly irreducible rings. This case completes the proof of Theorem 2 for arbitrary H-rings, since any H-ring is a subdirect sum of subdirectly irreducible H-rings.

LEMMA 3. [Thierrin, 8]. Let R be a subdirectly irreducible duo ring and D the set of right zero-divisors. Then D is an ideal of R. If in addition R contains an element which is not a right zero-divisor, then $\frac{R}{D}$ is a division ring.

Proof. Let $S \neq 0$ be the intersection of the non-zero ideals of R. Then the set $A(S) = \{x \mid Sx = 0\}$, which is clearly a right ideal, is a two-sided ideal; and $A(S) \subseteq D$. In addition, if $d \in D$, then $I = \{x \mid xd = 0\}$ is a two-sided ideal; hence $S \subseteq I$, $d \in A(S)$, and $D = A(S)$ is an ideal.

To complete the proof, suppose $R \neq D$ and $a \notin D$; and note that for any non-zero element $s \in S$, we have $sR = saR = S$. Thus there exists an element $y \in R$ such that $s = say$; and for any $b \notin D$ we have $sb = sayb$, $s(b - ayb) = 0$, and therefore $b - ayb \in D$. This implies $\frac{R}{D}$ is a division ring.

LEMMA 4. If R is a subdirectly irreducible H-ring, then $D \subseteq Z$.

https://doi.org/10.4153/CMB-1968-042-0 Published online by Cambridge University Press

Proof. Note that the definition of H-ring implies

(4) $\qquad ab - ba = a^n b - ba^n$ for all $a, b \in R$.

If a, b are such that $(ab - ba)a = a(ab - ba) = 0$, then $aba = ba^2 = a^2 b$; and these equalities applied repeatedly to the right side of (4) yield $ab - ba = 0$. Similarly, if $x(ab - ba)a = 0$ for some x, then $x(ab - ba) = 0$.

Suppose now that $a \in D$ and $a \notin Z$. Then there exists an element b such that $(ab - ba)a \neq 0$. Thus $(ab - ba)R \neq 0$ and $S \subseteq (ab - ba)R$; therefore, if s is a non-zero element of S, there is an x such that $s = (ab - ba)x \neq 0$. But then we are faced with the result that $sa = (ab - ba)xa = x(ab - ba)a = 0$ while at the same time $x(ab - ba) \neq 0$ - a contradiction.

COROLLARY. If R is a subdirectly irreducible H-ring such that $R \neq D$ and $[e]$ is the identity element of $\frac{R}{D}$, then $e \in Z$. Moreover, if $c \notin D$ and $c \in Z$ and if $[d]$ is the inverse of $[c]$ in $\frac{R}{D}$, then $d \in Z$.

Proof. For all $a \in R$, $ae - a$ and $ea - a \in D \subseteq Z$, from which it follows on multiplication by a that $a^2 e = aea = ea^2$. The argument at the beginning of the proof of Lemma 4 then shows that $ae = ea$.

To establish the second part, note that $cd - e \in D \subseteq Z$, hence $cd \in Z$. Thus for any $a \in R$ we have $c(ad - da) = (ca)d - (cd)a = (ac)d - a(cd) = 0$; cancelling c yields $ad - da = 0$.

We now proceed to the proof of Theorem 2 for R subdirectly irreducible; in view of Lemma 4, we need consider only the case that $R \neq D$. Suppose that such a ring contains an element $a \notin Z$, and let $b \in Z$. We begin by showing that $b^n - b \in D$.

Suppose $b^n - b \notin D$ for some $b \in Z$. By the argument employed in Section 2, we have $(b^n - b)a \in Z$. If $[d]$ is the inverse of $[b^n - b]$ in $\frac{R}{D}$, then by the corollary to Lemma 4, $d \in Z$ and hence $d(b^n - b)a \in Z$. But $d(b^n - b)a - a \in D \subseteq Z$, and this implies $a \in Z$, contrary to our assumption.

We have shown that $b^n - b \in D$ for all $b \in Z$; therefore, for all $a \in R$ we have $(a^n - a)^n - (a^n - a) \in D$. Thus, since all elements of R/D satisfy the same polynomial equation, R/D is a finite field. Since the multiplicative group of a finite field is cyclic, all non-divisors

https://doi.org/10.4153/CMB-1968-042-0 Published online by Cambridge University Press

of zero in R can be written in the form $x^i + z$ where $z \in Z$ and x is a fixed element of R. But this is incompatible with the existence of an element $a \notin Z$. Our proof of Theorem 2 is now complete.

Theorem 2 is true if n is not fixed but depends on x (see [3]); however, the division ring case here requires some specialized machinery. Most of the arguments we have used apply to the more general case - in particular, Lemma 2 goes through - and an elementary proof for the case where R has no zero-divisors would again obviate the use of the Jacobson structure theory.

REFERENCES

1. A Forsythe and N. McCoy, On the commutativity of certain rings. Bull. Amer. Math. Soc. 52 (1946) 523-526.

2. I.N. Herstein, An elementary proof of a theorem of Jacobson. Duke Math. J. 21 (1954) 45-48.

3. _____ , A condition for the commutativity of rings. Canadian J. Math. 9 (1957) 583-586.

4. _____ , A generalization of a theorem of Jacobson. Amer. J. Math. 73 (1951) 756-762.

5. _____ , A generalization of a theorem of Jacobson III. Amer. J. Math. 75 (1953) 105-111.

6. _____ , A theorem on rings. Canadian J. Math. 5 (1953) 238-241.

7. H. Paley and P. Weichsel, A first course in abstract algebra. (Holt, Rinehart and Winston, 1966).

8. G. Thierrin, On duo rings. Canadian Math. Bull. 3 (1960) 167-172.

Brock University

https://doi.org/10.4153/CMB-1968-042-0 Published online by Cambridge University Press