BULL. AUSTRAL. MATH. SOC. MOS 17A05
VOL. 3 (1970), 75-79.

A commutativity theorem for power-associative rings

D. L. Outcalt and Adil Yaqub

Let R be a power-associative ring with identity and let I be an ideal of R such that R/I is a finite field and $x \equiv y \pmod{I}$ implies $x^2 = y^2$ or both x and y commute with all elements of I. It is proven that R must then be commutative. Examples are given to show that R need not be commutative if various parts of the hypothesis are dropped or if "$x^2 = y^2$" is replaced by "$x^k = y^k$" for any integer $k > 2$.

1. Introduction

Wedderburn's Theorem, asserting that a finite associative division ring is necessarily commutative, has recently been generalized by the authors in [1; 2]. Indeed, the following theorem, the case $N = (0)$ of which yields Wedderburn's Theorem, was proved in [2]:

THEOREM 1. *Let R be an associative ring with identity in which every element is either nilpotent or a unit in R. Then*

(a) the set N of nilpotent elements in R is an ideal and R/N is a division ring;

(b) if (i) R/N is finite, and (ii) $x \equiv y \pmod{N}$ implies $x^2 = y^2$ or both x and y commute with all elements of N, then R is commutative.

Our present object is to extend Theorem 1 to the case where R is a

Received 12 April 1970. The first author was supported by US Air Force Office of Scientific Research Grant No. 698-67, and the second author by US National Science Foundation Grant GP-5929.

power-associative ring and where I is a more general ideal in R than N. Indeed, we prove the following

THEOREM 2. *Let R be a power-associative ring with identity* 1, *and let I be an ideal in R. If, further,*

(i) R/I is a finite field, and

(ii) $x \equiv y \pmod{I}$ implies $x^2 = y^2$ or both x and y commute with all elements of I,

then R is commutative.

We also give examples to show that Theorem 2 need not be true if either hypothesis *(i)* or *(ii)* is dropped, or if the hypothesis that R has an identity is deleted. Moreover, it turns out, somewhat surprisingly perhaps, that this theorem is not necessarily true if "$x^2 = y^2$" in *(ii)* is replaced by "$x^k = y^k$" for *any* $k > 2$ (see examples below).

2. Main section

Proof of Theorem 2. First, we prove that I is commutative. Suppose that $a_1, a_2 \in I$ and $a_1a_2 \neq a_2a_1$. We shall show that this leads to a contradiction. Since $a_1 \equiv 0 \pmod{I}$, $a_2 \equiv 0 \pmod{I}$, $a_1 + a_2 \equiv 0 \pmod{I}$, and $a_1a_2 \neq a_2a_1$, we have by *(ii)*,

$$a_1^2 = 0 \ , \quad a_2^2 = 0 \ , \quad (a_1+a_2)^2 = 0 \ .$$

Hence, $a_1a_2 + a_2a_1 = 0$. Moreover, since $a_1 + 1 \equiv 1 \pmod{I}$ and $(a_1+1)a_2 \neq a_2(a_1+1)$, we have using *(ii)* again, $(a_1+1)^2 = 1$. Hence, since $a_1^2 = 0$, $2a_1 = 0$. Therefore

$$a_1a_2 = -a_2a_1 = a_2a_1 \ ,$$

and thus I is indeed commutative.

Now, suppose $a \in I$ and $b \in R$. We shall show that $ab = ba$. Suppose not. Since $a + b \equiv b \pmod{I}$ and $ab \neq ba$, we have by *(ii)*, $(a+b)^2 = b^2$ and hence $a^2 + ab + ba = 0$. Since, moreover, $-a + b \equiv b \pmod{I}$, a similar argument shows that $a^2 - ab - ba = 0$. Hence, upon subtracting, we get $2(ab+ba) = 0$. Moreover, since $ab \neq ba$, $a(b+1) \neq (b+1)a$, and hence we may repeat the above argument using $b + 1$

https://doi.org/10.1017/S0004972700045676 Published online by Cambridge University Press

instead of b to get $2\{a(b+1)+(b+1)a\} = 0$. Combining this equation with $2(ab+ba) = 0$, we get $4a = 0$ and hence $-2a = 2a$. Thus $2ab = -2ba = 2ba$, and hence

(1) $$2(ab-ba) = 0 .$$

Now, let p be the characteristic of the finite field R/I (see *(i)*). Then $pb \in I$, and hence $a(pb) = (pb)a$. Therefore

(2) $$p(ab-ba) = 0 .$$

We now distinguish two cases.

Case 1. $p \neq 2$. Then p is an odd prime and (1), (2) readily imply $ab - ba = 0$, a contradiction.

Case 2. $p = 2$. In this case the finite field R/I has exactly 2^k elements for some integer k . Hence $(\bar{b})^{2^k} = \bar{b}$, and thus $b^{2^k}-b \in I$. Therefore,

(3) $$a\left(b^{2^k}-b\right) = \left(b^{2^k}-b\right)a .$$

Moreover, since $(a+b)^2 = b^2$ and R is power-associative, we obtain $\{(a+b)^2\}^{2^{k-1}} = (b^2)^{2^{k-1}}$, hence $(a+b)^{2^k} = b^{2^k}$. Now, by the power-associativity of R , $(a+b)(a+b)^{2^k} = (a+b)^{2^k}(a+b)$, therefore $(a+b)b^{2^k} = b^{2^k}(a+b)$. Thus, using power-associativity again, we get

(4) $$ab^{2^k} = b^{2^k}a .$$

Combining (3) and (4), we get $ab = ba$, a contradiction. We have thus obtained a contradiction whether $p \neq 2$ or $p = 2$. This contradiction proves that

(5) $$ab = ba \text{ for all } a \in I \text{ and all } b \in R .$$

To complete the proof of the theorem, suppose $x, y \in R$. In view of (5), we may assume that $x \notin I$ and $y \notin I$. Let $\bar{\xi} = \xi + I$ be a generator for the multiplicative cyclic group of non-zero elements of the finite field R/I . Then for some integers i, j , and some elements $a, a' \in I$, we have,

$$x = \xi^i + a , \quad y = \xi^j + a' .$$

Hence, by (5), the power-associativity of R, and the fact (proved above) that I is commutative, we readily obtain that $xy = yx$. This proves the theorem.

3. Examples and remarks

In this section, we give some examples to show that Theorem 2 need not be true if either hypothesis *(i)*, *(ii)* is deleted, or if the hypothesis that R has an identity is dropped.

EXAMPLE 1. Let R be the ring of quaternions, and let $I = (0)$. Here R satisfies *(ii)*, but *(i)* fails to hold. Another example is furnished by taking R to be the complete matrix ring, $M_n(F)$, over a field F, and $I = (0)$. Clearly both of these rings are not commutative.

EXAMPLE 2. Let

$$R = \left\{ \begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix} \middle| \; a, b, c, d \in GF(2) \right\},$$

$$I = \left\{ \begin{bmatrix} 0 & b & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{bmatrix} \middle| \; b, c, d \in GF(2) \right\}.$$

It is readily verified that R satisfies *(i)*, but *(ii)* fails to hold. Moreover, R is not commutative.

EXAMPLE 3. Let

$$R = GF(q) \oplus L ,$$

$$I = L ,$$

where L is a Lie ring of characteristic not 2. Then R satisfies all the hypotheses of Theorem 2, except that R has no identity 1. Moreover, R is not commutative.

We now remark that the equation "$x^2 = y^2$" in *(ii)* of Theorem 2 cannot in general be replaced by "$x^k = y^k$" for *any* $k > 2$. For, consider the ring R defined by

$$R = \left\{ \begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix} \;\middle|\; a,\, b,\, c,\, d \in GF(p) \;,\;\; p = \text{prime} \right\} ,$$

where p is chosen, in two stages, as follows: if k is odd, take p to be any fixed prime divisor of k ; while, if k is even, take p to be any fixed prime divisor of $k/2$. Since $k > 2$, such a prime p always exists. Let

$$I = \left\{ \begin{bmatrix} 0 & b & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{bmatrix} \;\middle|\; b,\, c,\, d \in GF(p) \right\} .$$

It is easily seen that R satisfies all the hypotheses of Theorem 2, except that "$x^2 = y^2$" is now replaced by "$x^k = y^k$" in *(ii)*. However, R is *not* commutative.

Now, if in Theorem 2, we specialize R to be an *associative* ring with identity such that every element in R is either nilpotent or a unit in R , then it is easily seen that the set N of nilpotent elements in R forms an ideal, and that R/N is indeed an associative division ring. If, in addition, R/N is finite, then R/N is a field (by Wedderburn's Theorem), and Theorem 1 now follows at once from Theorem 2 upon specializing the ideal I to be N itself.

Whether or not the assumption of power-associativity in Theorem 2 is essential remains an open question.

References

[1] D.L. Outcalt and Adil Yaqub, "A generalization of Wedderburn's theorem", *Proc. Amer. Math. Soc.* 18 (1967), 175-177.

[2] D.L. Outcalt and Adil Yaqub, "A commutativity theorem for rings", *Bull. Austral. Math. Soc.* 2 (1970), 95-99.

University of California,
Santa Barbara, California.