BULL. AUSTRAL. MATH. SOC. MOS 1630, 1649

VOL. 2 (1970), 95-99.

A commutativity theorem for rings

D. L. Outcalt and Adil Yaqub

Let R be an associative ring with identity in which every element is either nilpotent or a unit. The following results are established. The set N of nilpotent elements in R is an ideal. If R/N is finite and if $x \equiv y \pmod{N}$ implies $x^2 = y^2$ or both x and y commute with all elements of N, then R is commutative. Examples are given to show that R need not be commutative if "$x^2 = y^2$" is replaced by "$x^k = y^k$" for any integer $k > 2$. The case $N = (0)$ yields Wedderburn's Theorem.

1. Introduction

Wedderburn's Theorem, asserting that a finite associative division ring is necessarily commutative, has recently been generalized in [1]. Our purpose is to extend Wedderburn's Theorem to the case where R is an associative (but not necessarily finite) ring with identity in which every element is either nilpotent or a unit. The quaternions show that this alone need not force R to be commutative, hence additional conditions are needed. We prove that the set N of nilpotent elements of R is an ideal in R, and then impose conditions on N and R/N which yield the commutativity of R. Indeed, we establish the following

THEOREM. *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;

Received 18 September 1969. The first author was supported by Air Force Office of Scientific Research Grants AFOSR 698-65 and 698-67, and the second author by National Science Foundation Grant GP-5929.

(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.*

Note that the case $N = (0)$ recovers Wedderburn's Theorem.

We also show that this theorem need not hold if either hypothesis (i) or (ii) is deleted. Moreover, it turns out, perhaps somewhat surprisingly, 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 part *(a)*. Let $a \in N$, $b \in R$, and let $ab = c$. Suppose $c \notin N$. Then c is a unit. Let $a^k = 0$, k minimal. Then $0 = (a^k b)c^{-1} = (a^{k-1}c)c^{-1} = a^{k-1}$, contradicting the minimality of k. Thus, upon considering ba similarly, we have

(1) $\qquad a \in N$ and $b \in R \Rightarrow ab \in N$ and $ba \in N$.

Next, let $a \in N$, $b \in N$, and set $a - b = u$. Suppose $u \notin N$. Then u is a unit and $a = u + b$. Hence $au^{-1} = 1 - \gamma$, where $\gamma = -bu^{-1} \in N$ by (1). Let $\gamma^n = 0$, and let $w = 1 + \gamma + \gamma^2 + \ldots + \gamma^{n-1}$. Then $au^{-1} w = w\, au^{-1} = 1 - \gamma^n = 1$. Hence au^{-1} is a unit, a contradiction since, by (1), $au^{-1} \in N$. We have thus shown that

(2) $\qquad a \in N$ and $b \in N \Rightarrow a-b \in N$.

Part *(a)* readily follows from (1) and (2).

COROLLARY. *Let* R *and* N *be as in part (a) of the theorem. Then* R/N *is a division ring.*

Proof. First, by part *(a)*, N is an ideal in R and hence R/N makes sense. For any $a \in R$, let $\bar{a} = a+N \in R/N$. Suppose that $\bar{a} \neq \bar{0}$. Then $a \notin N$, and hence a is a unit in R. Therefore $ac = ca = 1$ for some $c \in R$, and hence $\bar{a}\bar{c} = \bar{c}\bar{a} = \bar{1}$. Thus $\bar{a}$ is a unit in R/N, and hence R/N is a division ring.

Next we prove two lemmas leading up to part *(b)* of the theorem.

https://doi.org/10.1017/S0004972700041630 Published online by Cambridge University Press

LEMMA 1. *Let R and N satisfy part (b) of the theorem. Then N is a commutative subring of R.*

Proof. Let $a \in N$, $b \in N$. Suppose $ab \neq ba$. Since $a \equiv 0 \pmod{N}$, $b \equiv 0 \pmod{N}$, $a + b \equiv 0 \pmod{N}$, we have by (ii), $a^2 = 0$, $b^2 = 0$, $(a+b)^2 = 0$, and hence $ab + ba = 0$. This follows, since otherwise (ii) would force $ab = ba$. Similarly, since $a + 1 \equiv 1 \pmod{N}$, $(a+1)^2 = 1$, and hence $2a = 0$. Therefore $ba = -ab = ab$, a contradiction. This proves the lemma.

LEMMA 2. *Let R, N, R/N satisfy all the hypotheses of Lemma 1. Then every element of N commutes with every element of R.*

Proof. Let $a \in N$, $b \in R$, and suppose $ab \neq ba$. Since $a + b \equiv b \pmod{N}$, therefore by (ii), $(a+b)^2 = b^2$. Hence

$$0 = (a+b)(a+b)^2 - (a+b)^2(a+b) = (a+b)b^2 - b^2(a+b) = ab^2 - b^2a .$$

Therefore,

$$ab^2 = b^2a . \tag{3}$$

Now, since $ab \neq ba$, $a(b+1) \neq (b+1)a$, and hence we may repeat the above argument to $b + 1$ (instead of b) to get $a(b+1)^2 = (b+1)^2a$. This equation, when combined with (3), yields

$$2(ab-ba) = 0 . \tag{4}$$

But, by the corollary, R/N is a division ring which, by (i) and Wedderburn's Theorem, must be a finite field of characteristic p, say. Hence $pb \in N$, and thus by Lemma 1, $a(pb) = (pb)a$. Therefore,

$$p(ab-ba) = 0 . \tag{5}$$

Now, if $p \neq 2$, then (4), (5) readily imply $ab - ba = 0$, a contradiction. Next, suppose $p = 2$. Then the finite field R/N has exactly 2^k elements for some integer k. Hence $(\bar{b})^{2^k} = \bar{b}$, and thus $b^{2^k} - b \in N$. Therefore, by Lemma 1, we get

$$a\left(b^{2^k}-b\right) = \left(b^{2^k}-b\right)a . \tag{6}$$

Now, iterative multiplication of both sides of (3) by b^2 yields

$$ab^{2^k} = b^{2^k}a . \tag{7}$$

https://doi.org/10.1017/S0004972700041630 Published online by Cambridge University Press

Hence, by (6), (7), we get $ab = ba$, a contradiction. We have thus obtained a contradiction whether $p \neq 2$ or $p = 2$. This contradiction proves the lemma.

We are now in a position to complete the proof of the theorem.

Proof of part *(b)*. In view of Lemmas 1 and 2 we may assume that $x \notin N$ and $y \notin N$. Now, by the corollary, hypothesis (i), and Wedderburn's Theorem, R/N is a finite field, and hence the multiplicative group of non-zero elements of R/N is cyclic. Let $\bar{\xi} = \xi + N$ be a generator for R/N, $\xi \in R$. Then for some integers i, j, and some $a, a' \in N$, we have, $x = \xi^i + a$, $y = \xi^j + a'$. Hence, by Lemmas 1 and 2, $xy = yx$, and the theorem is proved.

3. Examples

The following examples serve to show that part *(b)* of the theorem need not hold if either of the hypotheses (i), (ii) is deleted.

EXAMPLE 1. Let R be any division ring which is not commutative (e.g., the quaternions). Here R satisfies (ii), but (i) fails to hold.

EXAMPLE 2. Let

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

Here R is not commutative, and N consists of the *strictly* upper triangular matrices in R. Moreover, R satisfies (i) but (ii) fails to hold.

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

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

where p is chosen as follows: if k is odd take p to be any fixed prime divisor of k, and if k is even take p to be any fixed prime

https://doi.org/10.1017/S0004972700041630 Published online by Cambridge University Press

divisor of $k/2$. Since $k > 2$, such a prime p always exists. It is readily verified that the ring R satisfies all the hypotheses of part *(b)*, except that "$x^2 = y^2$" is now replaced by "$x^k = y^k$" in (ii). Note, however, that R is not commutative.

We observe that the theorem applies to infinite rings and to rings with non-zero nilpotent elements. An example is furnished by adjoining to $GF(p)$ an infinite number of commuting nilpotent elements $\eta_1, \eta_2, \ldots$: $R = GF(p)\,[\eta_1, \eta_2, \ldots]$ (p prime). Another example is obtained by taking

$$R = \left\{ \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ & a_1 & \ddots & \vdots \\ & & \ddots & a_2 \\ 0 & & & a_1 \end{pmatrix} \;\middle|\; a_i \in GF(p^k) \ , \quad i = 1, \ldots, n \right\} .$$

Here the nilpotent elements consist of the *strictly* upper triangular matrices in R . It is readily verified that the rings in both of these two examples satisfy all the hypotheses of the theorem.

Reference

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

University of California,
Santa Barbara, California.

https://doi.org/10.1017/S0004972700041630 Published online by Cambridge University Press