Math. J. Okayama Univ. 21 (1979), 15—19

STRUCTURE AND COMMUTATIVITY OF RINGS WITH CONSTRAINTS ON NILPOTENT ELEMENTS

DAVID L. OUTCALT and ADIL YAQUB

Recently [3] the authors proved the following :

Theorem 1. *Let R be an associative ring with a left identity, and let N be the set of nilpotent elements in R. Suppose that* (P) *for every x in R, there exists a positive integer $n = n(x)$ and an element x' in the subring, $\langle x \rangle$, generated by x such that $x^n = x^{n+1}x'$, and* (M) $x - y \in N$ *implies $x^2 = y^2$ or both x and y commute with all elements of N. Then R is a subdirect sum of local commutative rings and nil commutative rings.*

As was noted in the final section of [3], Theorem 1 need *not* be true if the prime 2 in hypothesis (M) is replaced by *any prime* $q > 2$, *even if we were to replace hypothesis* (M) *by the stronger hypothesis*: $x - y \in N$ implies $x^2 = y^2$. This naturally gives rise to the following question: What hypotheses, in addition to hypothesis (P) and the hypothesis that $x - y \in N$ implies $x^q = y^q$, should be added in order to guarantee the commutativity of the ground ring R? It turns out that one such hypothesis is to assume that the set N is commutative. In fact, by assuming this additional hypothesis on N, it turns out that *we do not need to assume that the ground ring R has a left identity* — an assumption which is absolutely essential for Theorem 1 to be true (see [3]). Our theorem, then may be stated as follows :

Theorem 2. *Let R be an associative ring and let N be the set of nilpotent elements of R. Suppose q is a fixed prime. Suppose, further, that* (i) *N is commutative,* (ii) *for every x in R there exists an element x' in $\langle x \rangle$ and a positive integer $n = n(x)$ such that $x^n = x^{n+1}x'$,* (iii) *$x - y \in N$ implies $x^q = y^q$. Then R is a subdirect sum of local commutative rings and nil commutative rings.*

In preparation for the proof of Theorem 2 we first establish the following lemmas.

Lemma 1. *Let R, N, q be as in Theorem 2. Then,*

(a) *Hypothesis* (ii) *of Theorem 2 is equivalent to the following: For every $x \in R$, there exists an element x' in $\langle x \rangle$ such that $x - x^2x' \in N$.*

(b) *Hypothesis* (iii) *of Theorem* 2 *implies that*

$$ab^q = b^q a, \quad \text{for all } a \in N \text{ and all } b \in R,$$

and necessarily all of the idempotent elements of R *are in the center of* R.

Proof. (a) is almost trivial. We shall prove (b). Since $(a+b)-b \in N$, therefore by hypothesis (iii),. $(a+b)^q = b^q$. Hence,

$$b^q(a+b) = (a+b)^q(a+b) = (a+b)(a+b)^q = (a+b)b^q,$$

which simplifies to $b^q a = ab^q$. As is well known, every idempotent element commuting with all nilpotent elements is central.

Lemma 2. *In the notation, and under the hypotheses, of Theorem* 2, *we have*

(a) N *is a commutative nil ideal of* R.

(b) *If* f *is a homomorphism of* R *onto* R^*, *then* $f(N)$ *coincides with the set of all nilpotent elements of* R^*.

Proof. The proof is obvious from the proof of Lemma [1]. However, for the sake of selfcontainedness, we shall give here the proof.

(a): Let a be an arbitrary element of N, and let $b \in R$. Suppose $a^h = 0$. By hypothesis (ii), there exists a $c \in \langle ab \rangle$ such that $(ab)^n = (ab)^{n+1}c$. Let $e = (ab)^n d$, where $d = c^n$. Then, as is readily verified,

$$(1) \qquad (ab)^n = (ab)^n e \text{ and } e^2 = e.$$

By Lemma 1 (b), e is in the center of R, and hence

$$e = e^2 = e(ab)^n d = aeb(ab)^{n-1}d = a^h e\{b(ab)^{n-1}d\}^h = 0,$$

since $a^h = 0$. Thus, $e = 0$ and hence by (1), $(ab)^n = 0$. Therefore, ab is nilpotent. Similarly, ba is nilpotent. We have thus shown that ab and ba are nilpotent, for all $a \in N$ and $b \in R$. Combining this and hypothesis (i), we conclude that N is a commutative nil ideal of R.

(b): Let d^* be an arbitrary nilpotent element of R^*, and let $(d^*)^k = 0$. Choose d in R such that $f(d) = d^*$. By Lemma 1 (a), there exists $d' \in \langle d \rangle$ such that $d - d^2 d' \in N$. Since N is an ideal [by part (a)], we obtain

$$d - d^{k+1}(d')^k = (d - d^2 d') + dd'(d - d^2 d') + \ldots + (dd')^{k-1}(d - d^2 d') \in N.$$

Recall that $f(d) = d^*$, $(d^*)^k = 0$, and hence it follows that $d^* \in f(N)$. This proves part (b).

Corollary 1. *If R satisfies the hypotheses* (i), (ii), (iii) *of Theorem* 2, *then any subring of R and any homomorphic image of R satisfy* (i), (ii), (iii).

Proof. The statement is obvious for subrings. Now, let f be a homomorphism of R onto R^*. By Lemma 2 (b), it follows at once that R^* satisfies (i). Clearly, R^* satisfies (ii). To prove that R^* satisfies (iii), suppose that $x^* - y^* \in f(N)$ [= set of nilpotents of R^*, by Lemma 2 (b)]. Then $x^* - y^* = n^* = f(n)$, for some n in N. Let $x^* = f(x)$, $y^* = f(y)$. Since $x-(x-n) \in N$, $x^q = (x-n)^q$, by (iii), and hence $(x^*)^q = (x^* - n^*)^q = (y^*)^q$. Thus, R^* satisfies (iii).

We are now in a position to prove Theorem 2.

Proof of Theorem 2. Since, as is well known, the ground ring R is isomorphic to a subdirect sum of subdirectly irreducible rings, we may in view of Corollary 1 assume that R is subdirectly irreducible. Recall that, by hypothesis (ii), $x^n = x^{n+1}x'$, and hence, as is readily verified, $e = x^n(x')^n$ is idempotent and $x^n = x^n e$. Also, by Lemma 1 (b), e is a central idempotent in R, and hence $e = 0$ or $e = 1$ (if $1 \in R$). Now, if R does not have an identity, then $x^n = x^n e = 0$, and hence $R = N$ is commutative, by hypothesis (i). Next, suppose $1 \in R$. In this case, $e = 0$ or $e = 1$ implies that, for every x in R, x is nilpotent or x is a unit in R; that is, R is a local ring. To prove that R is commutative, we may further assume that R is finitely generated. By Lemma 1 (a) and Corollary 3.5 of [4], it readily follows that, for every x in R, there exists a positive integer n such that $x - x^{n+1} \in N$. Hence, by Jacobson's Theorem (see, e. g., [2]), R/N is a field. In fact, since R is finitely generated, R/N is a finite field, say,

$$(2) \qquad R/N = \mathrm{GF}(r), \quad \text{where } r = p^{\alpha}, \quad p \text{ prime}, \ \alpha \geq 1.$$

Clearly, if $N = \{0\}$, then R is commutative. So, suppose $N \neq 0$, and let a be an arbitrary element of N. Suppose that $a^k = 0$ but $a^{k-1} \neq 0$, $(k \geq 2)$. Since by hypothesis (iii), $(1 + a)^q = 1$, we have

$$(3) \qquad qa^{k-1} = \{(1 + a)^q - 1\} a^{k-2} = 0.$$

On the other hand, by (2), the characteristic of R is equal to p^β for some positive integer β, and hence $p^\beta a^{k-1} = 0$. Combining this with (3), we get $qa^{k-1} = 0 = p^\beta a^{k-1}$. Now, if $p \neq q$, then the last implies that $a^{k-1} = 0$, which is a contradiction. This contradiction shows that $p = q$. Hence, by Lemma 1 (b), we have

$$(4) \qquad ab^r = b^r a, \quad (a \in N, \ b \in R).$$

Moreover, by (2), $b^r - b \in N$, and hence by hypothesis (i), we conclude that

$$(5) \qquad a(b^r - b) = (b^r - b)a, \quad (a \in N, \ b \in R).$$

Combining (4) and (5), we see that

$$(6) \qquad ab = ba, \quad (a \in N, \ b \in R).$$

Also, by (2), the multiplicative group of nonzero elements of R/N is cyclic. Combining this fact with (6), we can easily see that R is commutative. Note that in the above proof, we have shown that the ground ring R has the structure described in Theorem 2. This completes the proof.

It is well known that Theorem 2 need not be true if any of the hypotheses (i), (ii) is deleted (see [3]). In the subring $R = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right\}$ of $(GF(2))_2$, all the hypotheses of Theorem 2 hold except (iii). Observe that R is not commutative, and hence hypothesis (iii) cannot be deleted. We conclude this paper with the following

Remark. Let $q = 3$. Let R be an algebra over $GF(2)$ of dimension 4 with $\{1, \xi, \eta, \eta'\}$ as a basis, and with the following multiplication table:

$$\xi\eta = \eta', \quad \xi\eta' = \eta + \eta' = \eta\xi, \quad \eta'\xi = \eta,$$
$$\xi^2 = 1 + \xi, \quad \eta\eta' = \eta'\eta = \eta^2 = (\eta')^2 = 0.$$

It can be verified that $(R, +, \times)$ is an associative ring, and that all the hypotheses of Theorem 2 hold *except* that hypothesis (iii) is now replaced by that $x - y \in N$ implies $x^q = y^q$ or both x and y commute with all elements of N (where $q = 3$). In verifying this, observe that, for x in R, $x^2 = x^8$. Note, however, that R is not commutative. This example shows, then, that Theorem 2 need not be true if we replace hypothesis (iii) by the weaker hypothesis that $x - y \in N$ implies $x^q = y^q$ or both x and y commute with all elements of N.

In conclusion, we would like to express our indebtedness and gratitude to the referee for his helpful suggestions and valuable comments.

REFERENCES

[1] S. IKEHATA and H. TOMINAGA: A commutativity theorem, Math. Japonica **24** (1979), 29—30.
[2] T. NAGAHARA and H. TOMINAGA: Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson, Abh. Math. Sem. Univ. Hamburg **41** (1974), 72—74.
[3] D. L. OUTCALT and ADIL YAQUB: Commutativity and structure theorems for rings with polynomial constraints, Math. Japonica **23** (1978), 217—226.
[4] P. N. STEWART: Semi-simple radical classes, Pacific J. Math. **32** (1970), 249—259.

DEPARTMENT OF MATHEMATICS AND
INSTITUTE FOR THE INTERDISCIPLINARY APPLICATION OF
ALGEBRA AND COMBINATORICS
UNIVERSITY OF CALIFORNIA, SANTA BARBARA
SANTA BARBARA, CALIFORNIA 93106, U. S. A.

(*Received October 22, 1978*)