East-West J. of Mathematics: Vol. 7, No 1 (2005) pp. 79-91

NORMALITY CONDITIONS AND COMMUTATIVITY THEOREMS FOR RINGS

Takasi Nagahara[1] and **Adil Yaqub**[2]

[1] *Professor Emeritus of Okayama University*
Present address: Wakamiya 12-24,
Hayashima-cho, Okayama-ken 701-0302, Japan

[2] *Department of Mathematics*
University of California,
Santa Barbara, CA 93106, USA
e-mail:yaqub@math.ucsb.edu

Abstract

Let R be a ring with center C, and let N the set of nilpotent elements. Suppose that for each $x,\ y \in R\backslash N, x^n y - xy^n \in N \cap C$, where $n > 1$ is a fixed integer. We shall present conditions for R to be commutative, non-commutative, normal and periodic.

Throughout, R will represent a ring with center C. Let N, E be the set of nilpotent elements of R and the set of idempotents of R, respectively; let N^* be the subset of N consisting of all elements x such that $x^2 = 0$. The ring R is called *normal* if $E \subseteq C$. For $x,\ y$ in R, let $[x,y]_1 = [x,y] = xy - yx$, and define, recursively $[x,y]_k = [[x,y]_{k-1}, y]$ for all integers $k > 1$.

Before stating and proving the main theorems of this paper, we first establish the following basic lemma.

Lemma 1. *Let $n > 1$ be a fixed integer. Then*

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} ((n-i)^n - (n-i)) = n!.$$

Key words:
2000 AMS Mathematics Subject Classification:

Proof We start with a polynomial $f(X)$ in $Z[X]$, and define recursively:

$$\Delta^1 f(X) = f(X+1) - f(X),$$
$$\Delta^k f(X) = \Delta^1(\Delta^{k-1} f(X)).$$

Then we can easily see that $\Delta^k f(X) = \sum_{i=0}^{k}(-1)^i\binom{k}{i}(f(X+(k-i)))$. In particular,

$$\Delta^n(X^n) = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(X+(n-i))^n,$$
$$\Delta^n(X) = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(X+(n-i)).$$

Combining these with [8, Lemma 1], we obtain

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(X+(n-i))^n = n!,$$
$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(X+(n-i)) = 0.$$

So putting $X = 0$ in the above, we obtain

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^n = n!,$$
$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i) = 0.$$

Hence $\sum_{i=0}^{n}(-1)^i\binom{n}{i}((n-i)^n - (n-i)) = n!$. □

We now proceed to prove the main theorems.

Theorem 1. *A ring R is normal if and only if there exists an integer $n > 1$ for which R satisfies the following conditions:*

(i) *For each $x \in R\backslash N$ and $e \in E$, $[x^n - x, e] \in C$.*

(ii) *For each $a \in N^*$ and $e \in E$, $n![a,e] = 0$ implies $[a,e]_k = 0$ with some positive integer k.*

Proof It suffices to prove the if part only. Let $e \in E$, and $x \in R$. Obviously, $a = ex - exe \in N^*$ and $f = e + a \in E$. Further, noting that $[a,e] = -a$, we see that $[a,e]_k = (-1)^{k-1}[a,e]$. Now, we shall prove that $a = 0$. First, suppose that there exists an integer i with $2 \leq i \leq n$ such that $if \in N$, namely $i^m f = (if)^m = 0$ for some positive integer m. Then $i^m[a,e] = i^m[f,e] = [i^m f, e] = 0$, and so $(n!)^m[a,e] = 0$. Hence, by (ii), $(-1)^{k-1}(n!)^{m-1}[a,e] = (n!)^{m-1}[a,e]_k = 0$ for some positive integer k, namely $(n!)^{m-1}[a,e] = 0$. Therefore, we obtain eventually $-a = [a,e] = 0$, namely $a = 0$. On the other hand, if $if \notin N$ for all i with $2 \leq i \leq n$, then by (i)

$$(i^n - i)[a,e] = (i^n - i)[f,e] = [(if)^n - if, e] = 0 \quad (0 \leq i \leq n).$$

Hence, by Lemma 1, we obtain $n![a,e] = 0$. Then, by (ii), $(-1)^k a = [a,e]_k = 0$ for some positive integer k. We have thus seen that $ex = exe$. Similarly, $xe = exe$, and therefore $ex = xe$. □

Corollary 1. *Suppose that there exists an integer $n > 1$ for which R satisfies the following conditions:*

(i)′ *For each $x, y \in R \backslash N$, $[x^n, y] - [x, y^n] \in C$.*

(ii) *For each $a \in N^*$ and $e \in E$, $n![a,e] = 0$ implies $[a,e]_k = 0$ with some positive integer k.*

Then R is a normal ring.

Proof If $x \in R \backslash N$ and $e \in E$, then $[x^n - x, e] = [x^n, e] - [x, e^n] \in C$. Hence R is normal by Theorem 1. □

Another corollary to Theorem 1 involves periodic rings. A ring R is called *periodic* if for each x in R, there exist distinct positive integers n, m for which $x^n = x^m$. If $0 < n < m$ then $x^{n(m-n)} \in E$. By [3, Proposition 2], R is periodic if and only if for each x in R, there exists $f(X) \in X^2 Z[X]$ such that $x - f(x) \in N$. We are now in a position to prove the following:

Corollary 2. *Suppose that there exists a fixed integer $n > 1$, and R is a ring which satisfies the following conditions:*

(i)″ *For each $x, y \in R \backslash N$, $x^n y - x y^n \in N \cap C$.*

(ii) *For each $a \in N^*$ and $e \in E$, $n![a,e] = 0$ implies $[a,e]_k = 0$ with some positive integer k.*

Then R is a normal periodic ring.

Proof In fact, if $x \in R \backslash N$ and $e \in E$, then $[x^n - x, e] = (x^n e - x e^n) - (e x^n - e^n x) \in C$ and $x^{n+1}(x - x^n) = x^n x^2 - x x^{2n} \in N$. Since $(x - x^n)^{n+3} = (x - x^n)(1 - x^{n-1})^{n+1} x^{n+1}(x - x^n)$, it follows that $x - x^n \in N$. Hence, R is normal and periodic by Theorem 1 and [3, Proposition 2]. □

For the conditions (i), (i)′ and (i)″, we have the implications (i)″⇒(i)′⇒(i). Hence the condition (ii)″ is most strong.

Another theorem which follows at once from Theorem 1 is the following:

Theorem 2. *Suppose that there exists an integer $n > 1$ for which R satisfies the following conditions:*

(i) *For each $x \in R\backslash N$ and $e \in E$, $[x^n - x, e] \in C$.*

(ii) *For each $a \in N^*$ and $e \in E$, $n![a, e] = 0$ implies $[a, e]_k = 0$ with some positive integer k.*

If R is generated, as a ring, by E, then R is commutative, and isomorphic to a subdirect sum of rings isomorphic to $Z/(p^k)$ for some prime p and some positive integer k.

This follows by writing R as a subdirect sum of subdirectly irreducible rings, and by recalling that Z is isomorphic to a subdirect sum of prime fields $Z/(p)'s$.

Our next result gives a sufficient condition for a ring R to be commutative and periodic. This result makes an essential use of Corollary 2.

Theorem 3. *Suppose that $n > 1$ is a fixed integer, R is a ring which satisfies the following conditions:*

(i)$''$ *For each $x, y \in R\backslash N$, $x^n y - xy^n \in N \cap C$.*

(ii)$'$ *For each $a \in N$ and $x \in R$, $n![a, x] = 0$ implies $[a, x]_k = 0$ with some positive integer k.*

(iii) *For each $a, b \in N$, there exists an integer $m = m(a, b) > 1$ such that $[a, b] = [a, b]^m$.*

Then R is a commmutative periodic ring.

Proof By Corollary 2, R is a normal periodic ring. Then, for each $x \in R$, there exists a positive integer r such that $x^r \in E \subseteq C$. Hence, by [5, Theorem 4], the commutator ideal of R is nil, and so N forms an ideal of R. Further, in view of (iii), [6, Theorem 6] shows that N is commutative.

Claim 1. *If R contains 1, then it is commutative.*

Proof Let $a \in N$. Then both $1 + a$ and 1 are in $R\backslash N$. Then, by (i)$''$, $(1 + a)^n \cdot 1 - (1 + a) \cdot 1^n \in C$. As was noted above, N is a commutative ideal, and so $N^2 \subseteq C$. Hence $1 + na - (1 + a) \in C$, namely $(n - 1)[a, x] = 0$ for all $x \in R$. Then $n![a, x] = 0$, so that $[a, x]_k = 0$ with some positive integer k. Now, the commutativity of R is clear by [2, Theorem]. □

We now proceed to the general case ($1 \notin R$). Let $\sigma : R \to R'$ be a homomorphism of R onto a subdirectly irreducible ring R'. To complete the proof of Theorem 3, it suffices to show that R' is commutative. By [1,(c)], $\sigma(N)$ coincides with the set N' of nilpotents in R'. Further, by [8, Lemma 1],

R' is a normal periodic ring. Since R' is subdirectly irreducible, 1 and 0 are the only idempotents in R'. If $1 \notin R'$, then $R' = N'$ is commutative. In what follows, we may restrict our attention to the case that R' contains 1. Then, as is easily seen, there exists a (central) idempotent e in R such that $\sigma(e) = 1$. Obviously, e is the unity of eR and eR satisfies all the conditions (i)$''$, (ii)$'$ and (iii) in Theorem 3. Hence eR is commutative, by Claim 1; and so $R' = \sigma(eR)$ is commutative. This completes the proof of Theorem 3. □

Related work also appears in [4].

Next, we shall present a classification theorem of rings which satisfies the conditions (i)$''$ and (ii) in Corollary 2.

Theorem 4. *For a ring R and an integer $n > 1$, the following conditions* (1) and (2) are equivalent.

(1)

(i)$''$ For each $x,\ y \in R\backslash N$, $x^n y - xy^n \in N \cap C$.

(ii) For each $a \in N^*$ and $e \in E$, $n![a, e] = 0$ implies $[a, e]_k = 0$ with some positive integer k.

(2) R is a ring which is one of the following types (a)-(d).

(a) $R = N$.

(b) $R = C$ and $x^n - x \in N$ for each $x \in R$.

(c) (c_1) $\{0\} \neq RE \subset C$ and $R = RE + N$.
(c_2) N is a non-commutative ideal of R.
(c_3) $x^n - x \in N$ for each $x \in RE$.
(c_4) $x^n y - xy^n \in C$ for each $x, y \in N$.

(d) (d_1) $RE \not\subset C$, $E = \{e, 0\} \subset C$ and $R = Re + R(1 - e)$.
(d_2) N is an ideal of R containing $R(1 - e)$.
(d_3) The factor ring $Re/(Re \cap N)$ is a finite field $GF(p^s)$ such that $p^s - 1$ is a divisor of $n - 1$.
(d_4) $x^n y - xy^n \in C$ for each $x, y \in R\backslash N$.

Proof (1)⇒(2): For each $x \in R$, by (i)$''$, we have

$$x^{n+1}(x - x^n) = x^n x^2 - x x^{2n}, \quad \text{and}$$
$$(x - x^n)^{n+3} = (x - x^n)(1 - x^{n-1})^{n+1} x^{n+1}(x - x^n).$$

If $x \notin N$ then $x^{n+1}(x - x^n) \in N \cap C$, whence $x - x^n \in N$. Hence

$$x^n - x \in N \quad \text{for all} \quad x \in R.$$

We assume that $R \neq N$ and $R \neq C$. We shall distinguish two cases:

Case 1. $RE \subset C$: By Corollary 2, R is normal and periodic. Hence, for each $x \in R$, there exists an integer $r > 0$ such that $x^r \in E \subset C$. If $RE = \{0\}$

then $R = N$, and this is a contradiction. Thus, we have $\{0\} \neq RE \subset C$. Now, we set

$$A = \{x \in R \mid x(RE) = \{0\}\}.$$

Clearly A is an ideal of R. If $A \not\subset N$ then, for each $x \in A \backslash N$, $0 \neq x^r \in E \cap A$ for some integer $r > 0$ and $A(RE) \ni x^r x^r = x^r \neq 0$, which is a contradiction. Hence we have $A \subset N$. Next, let $b_1,\ b_2 \in N$. Then $b_1^{m_1} = 0$ and $b_2^{m_2} = 0$ for some integers $m_1 > 0$ and $m_2 > 0$. For each $e \in E$, we have $b_1 e, b_2 e \in RE \subset C$, and so

$$(b_1 - b_2)^{m_1+m_2} e = (b_1 e - b_2 e)^{m_1+m_2} = 0.$$

Hence $(b_1 - b_2)^{m_1+m_2} \in A \subset N$, and so $b_1 - b_2 \in N$. By a similar way, we have $b_1 x,\ x b_1 \in N$ for all $x \in R$. Thus, N is an ideal of R. Next, we shall prove $R = RE + N$. Let $x \in R \backslash N$. Then $0 \neq x^r \in E \subset C$ for some integer $r > 0$. We set $e = x^r$ and consider $R = Re + R(1 - e)$. Then $x = x_1 + x_2$ where $x_1 \in Re$ and $x_2 \in R(1 - e)$. Since $e, x_1 \in C$, we have $x^r = x_1^r + x_2^r$. Since $x^r = e$ and $x_1^r \in Re$, it is easily seen that $x_2^r = 0$ and so $x_2 \in N$. Thus, we obtain $x = x_1 + x_2 \in RE + N$. Therefore, it follows that $R = RE + N$. Since $R \neq C$ and $RE \subset C$, N is a non-commutative ideal of R. Now, we shall prove (c$_4$). Let $b_1, b_2 \in N$ and $e \neq 0 \in E$. Then $e + b_1, e + b_2 \notin N$. Obviously $RE \cap N$ is an ideal of R. Moreover

$$\begin{aligned} &(e + b_1)^n (e + b_2) - (e + b_1)(e + b_2)^n \\ &= (e + b_1^n)(e + b_2) - (e + b_1)(e + b_2^n) \qquad (\text{mod } RE \cap N) \\ &= b_1^n b_2 - b_1 b_2^n \qquad (\text{mod } RE \cap N). \end{aligned}$$

Hence $C \cap N \ni (e + b_1)^n (e + b_2) - (e + b_1)(e + b_2)^n = b_1^n b_2 - b_1 b_2^n + c$ for some $c \in RE \cap N$. Since $RE \cap N \subset C \cap N$, we obtain $b_1^n b_2 - b_1 b_2^n \in C \cap N \subset C$. Thus, we obtain (c$_4$) and the assertion (c).

Case 2. $RE \not\subset C$: In this case, we shall prove the assertion (d). Let a be an element of $RE \backslash C$. Then, there are elements $e_1, \ldots, e_m \in E$ and $a_1, \ldots, a_m \in R$ such that

$$a_1 e_1 + \cdots + a_m e_m = a.$$

Since $E \subset C$, there exists an element $f \neq 0$ in E such that $f \geq e_i$, that is, $e_i f = e_i$ for $i = 1, \ldots, m$. Then $a \in Rf$. We consider the Peirce decomposition

$$R = Rf + R(1 - f).$$

Since $a \notin C$, there exists an element b in R such that $ab \neq ba$. We write here

$$b = b_1 + b_2,\ b_1 \in Rf \text{ and } b_2 \in R(1 - f).$$

Since $a \in Rf$, we have $ab = ab_1$ and $ba = b_1 a$, whence $ab_1 \neq b_1 a$. Thus, Rf is a non-commutative ring, and so is RE. Now, let $x \in RE \backslash (RE \cap N)$. Then, there is an element g in E such that $xg = x$. Since $g \in RE \backslash (RE \cap N)$, we have

$x^n g - xg^n = x^n - x \in N \cap C$ by (i)$''$. Hence, it follows that $x^n - x \in C \cap RE$ for all $x \in RE \backslash (RE \cap N)$. Since $E \subset C \cap RE$, RE is a ring of Type (b) in [7, Theorem]. Thus, we obtain that $E = \{e, 0\}$ and $Re \cap N$ is an ideal of Re. We consider the Peirce decomposition

$$R = Re + R(1-e), \qquad Re = RE.$$

Since R is periodic and $E \cap R(1-e) = \{0\}$, it follows that

$$R(1-e) \subset N, \qquad N = (Re \cap N) + R(1-e)$$

and so, it is an ideal of R. Thus, we obtain (d_2). Next, we shall prove (d_3). By [7, Theorem, Type (b)], the factor ring $Re/(Re \cap N)$ is a field which is algebraic over $GF(p)$, where p is a positive prime integer. Since $x^n - x \in Re \cap N$ for all $x \in Re$ and n is fixed, one will easily see that the factor ring $Re/(Re \cap N)$ is a finite field $GF(p^s)$ for an integer $s > 0$. Let $\bar{b} = b + (Re \cap N)$ be a generating element of the multiplicative cyclic group of non-zero elements in $Re/(Re \cap N)$. Then

$$b^{p^s - 1} = e + c, \qquad c \in Re \cap N.$$

On the other hand, since $b \in Re \backslash (Re \cap N)$, we have $b^n - b \in Re \cap N$, and so

$$b^{n-1} = e + d, \qquad d \in Re \cap N.$$

Since $p^s - 1$ is the order of $\bar{b} = b + (Re \cap N)$, it follows that $p^s - 1$ is a divisor of $n - 1$. Thus, we obtain (d_3). The assertion (d_4) follows from (i)$''$ immediately. Therefore, for Case 2, we have the assertion (d). Next, we shall prove the converse (2) (a,b,c,d) $\Rightarrow$ (1) in our theorem. Since the implications (a), (b), (c), (d) $\Rightarrow$ (ii) in (1) (resp) are trivial, it suffices to prove that (a), (b), (c), (d) $\Rightarrow$ (i)$''$ in (1) (resp).

(a) $\Rightarrow$ (i)$''$: It is trivial.

(b) $\Rightarrow$ (i)$''$: For each $x, y \in R \backslash N$, we have

$$x^n y - xy^n = (x^n - x)y - x(y^n - y) \in N = N \cap R = N \cap C.$$

(c) $\Rightarrow$ (i)$''$: Let $x = x_1 + x_2,\ y = y_1 + y_2 \in R \backslash N$ where $x_1, y_1 \in RE$ and $x_2, y_2 \in N$. Then $x_1, y_1 \in RE \backslash N$. Hence, by ($\mathrm{c}_2$), ($\mathrm{c}_3$) and ($\mathrm{c}_4$), we have

$$\begin{aligned} &x_1^n y_1 - x_1 y_1^n \in RE \cap N \subset C \cap N, \\ &x_2^n y_2 - x_2 y_2^n \in C \cap N. \end{aligned}$$

Moreover

$$\begin{aligned} x^n y - xy^n &= (x_1 + x_2)^n (y_1 + y_2) - (x_1 + x_2)(y_1 + y_2)^n \\ &= (x_1^n + x_2^n)(y_1 + y_2) - (x_1 + x_2)(y_1^n + y_2^n) \qquad (\mathrm{mod}\ RE \cap N) \\ &= (x_1^n y_1 - x_1 y_1^n) + (x_2^n y_2 - x_2 y_2^n) \qquad (\mathrm{mod}\ RE \cap N). \end{aligned}$$

Therefore, it follows that $x^n y - xy^n \in C \cap N$.

(d) $\Rightarrow$ (i)$''$: Let $x, y \in R\backslash N$. Then, we can write as it follows:

$$x = x_1 + x_2, \qquad y = y_1 + y_2,$$
$$x_1, y_1 \in Re\backslash(Re \cap N) \quad \text{and} \quad x_2, y_2 \in R(1-e).$$

Since $Re/(Re \cap N) = GF(p^s)$, we have

$$x_1^{p^s-1} = e + c, \qquad c \in Re \cap N,$$
$$y_1^{p^s-1} = e + d, \qquad d \in Re \cap N.$$

Since $p^s - 1$ is a divisor of $n-1$, we have $n - 1 = m(p^s - 1)$ for some integer $m > 0$. Hence

$$\begin{aligned} x_1^n &= x_1 x_1^{n-1} = x_1(x_1^{m(p^s-1)}) = x_1(x_1^{p^s-1})^m = x_1(e+c)^m = x_1(e+c') \\ &= x_1 e + x_1 c' = x + c'', \qquad c', c'' = x_1 c' \in Re \cap N, \\ y_1^n &= y_1 + d'', \qquad d'' \in Re \cap N. \end{aligned}$$

Then, since $x_1,\ y_1,\ e + x_2,\ e + y_2 \in R\backslash N$, we have

$$\begin{aligned} x_1^n y_1 - x_1 y_1^n &= (x_1 + c'')y_1 - x_1(y_1 + d'') \\ &= c'' y_1 - x_1 d'' \in Re \cap N \cap C \quad (\text{by } (d_2, d_4)), \quad \text{and} \\ x_2^n y_2 - x_2 y_2^n &= (e + x_2)^n (e + y_2) - (e + x_2)(e + y_2)^n \in C \cap N \quad (\text{by } (d_2, d_4)). \end{aligned}$$

Therefore, it follows that

$$x^n y - xy^n = x_1^n y_1 - x_1 y_1^n + x_2^n y_2 - x_2 y_2^n \in C \cap N.$$

Thus, we obtain the condition (i)$''$. □

Lemma 2. *Let R be a ring of Type (d) in Theorem 4 for an integer $n > 1$, that is, R a ring which satisfies the conditions* (d$_1$)-(d$_4$):

(d$_1$) $RE \not\subset C$, $E = \{e, 0\} \subset C$ and $R = Re + R(1-e)$.

(d$_2$) N is an ideal of R containing $R(1-e)$.

(d$_3$) The factor ring $Re/(Re \cap N)$ is a finite field $GF(p^s)$ such that $p^s - 1$ is a divisor of $n - 1$.

(d$_4$) $x^n y - xy^n \in C$ for each $x, y \in R\backslash N$.

Then, there hold the following (1) and (2).

(1) If $s = 1$ then N is non-commutative.

(2) If $s > 1$ and p is not a divisor of $n - 1$ then N is non-commutative.

Proof (1) We assume that $s = 1$. The, since $e \in Ce\backslash(Ce \cap N)$, we have

$$Re/(Re \cap N) = GF(p) = Ce/(Ce \cap N).$$

Hence, it follows that $Re = Ce + (Re \cap N)$, and so, $R = C + N$ by (d_1) and (d_2). Since $Re \not\subset C$, R is non-commutative. This implies that N is non-commutative. (See Examples (3)).

(2) We assume that p is not a divisor of $n-1$ and N is commutative. Then, one will easily see that $N^2 \subset C$. Moreover, we have $R(1-e) \subset C$ by (d_1) and (d_2). Let $g + (Re \cap N)$ be a generating element of the multiplicative (cyclic) group of non-zero elements of $Re/(Re \cap N)$. Then Re is generated by g and $Re \cap N$. Hence any subring of Re containing g and $Re \cap N$ coincides with Re. Let C_0 be the center of Re, and $N_0 = Re \cap N$. Since

$$R = Re + R(1-e) \quad \text{and} \quad R(1-e) \subset C$$

we have $C_0 = Re \cap C$. First, we shall prove that $N_0 \cap C_0$ is an ideal of Re. We set

$$A = \{x \in Re \mid (N_0 \cap C_0)x \subset N_0 \cap C_0\}.$$

Obviously A is a subring of Re. Since $N_0(N_0 \cap C_0) \subset N_0^2 \subset C_0$, we have $N_0 \subset A$. Let $x \in N_0 \cap C_0$. Then $xg \in N_0$. We set

$$B = \{y \in Re \mid y(xg) = (xg)y\}.$$

Since N_0 is commutative, we have $N_0 \subset B$. Moreover, since $x \in C_0$, we have $g \in B$. Hence $B = Re$, and $xg \in C_0 \cap N_0$. Therefore, it follows that $(N_0 \cap C_0)g \subset C_0 \cap N_0$, and so, $g \in A$. Since $N_0 \subset A$, we obtain $A = Re$. Thus, $N_0 \cap C_0$ is an ideal of Re. Now, since $Re/N_0 \cong GF(p^s)$ and p is not a divisor of $n-1$, we have $(n-1)e \in Re\backslash N_0$, and so, $(n-1)^t e \in E = \{e, 0\}$ for some integer $t > 1$. Hence $(n-1)^t e = e$. Now, let $v \in N_0$. Then $v^2 \in N_0^2 \subset N_0 \cap C_0$, and $e + v \in Re\backslash(Re \cap N)$. Hence

$$Re \cap N \cap C \ni (e+v)^n e - (e+v)e^n = (n-1)v \pmod{N_0 \cap C_0}.$$

Hence $(n-1)v = 0 \pmod{N_0 \cap C_0}$, and so

$$v = (n-1)^{t-1}(n-1)v = 0 \pmod{N_0 \cap C_0}.$$

Therefore, it follows that $N_0 \subset N_0 \cap C_0 \subset C_0$. Since Re is generated by g and N_0, Re is generated by g and C_0. Hence Re is commutative, and so, R is commutative. This is a contradiction. Thus, we obtain our assertion (2). □

Now, by virtue of Theorem 4 and Lemma 2, we shall prove a commutativity theorem in which the condition of R is weaker than that of R in Theorem 3.

Theorem 5. *Suppose that there exists an integer $n > 1$ for which R satisfies the following conditions:*

(i)″ *For each* $x, y \in R\backslash N$, $x^n y - xy^n \in N \cap C$.

(ii) *For each* $a \in N^*$ *and* $e \in E$, $n![a, e] = 0$ *implies* $[a, e]_k = 0$ *with some positive integer* k.

(iii) *For each* $a, b \in N$, *there exists an integer* $m = m(a, b) > 1$ *such that* $[a, b] = [a, b]^m$.

Then, R *is normal periodic and* N *is commutative. Moreover,*

(1) R *is commutative, provided that* n *is in the following: {2, 3, 4, 5, 6/8, 9, 10, 11, 12/14/16, 17, 18/20, 21, 22, 23, 24/26, 27, 28/30, and integers* t *such that* $t - 1$ *is not a multiple of* $p(p^s - 1)$ *for all positive prime divisors* p *of* $t - 1$ *and all positive integers* $s > 1$*}.*

(2) R *is not always commutative, that is, there exists an example of* R *which is a non-commutative ring, provided that* n *is in the following: {7, 13, 15, 19, 25, 29, and integers* t' *such that* $t' - 1$ *is a multiple of* $p(p^s - 1)$ *for some positive prime divisor* p *of* $t' - 1$ *and some positive integer* $s > 1$*} (Examples (1) and (4)).*

Proof By Corollary 2, R is a normal periodic ring. Moreover, by Theorem 4, N is an ideal of R. Let $a, b \in N$. Then, we have $[a, b] \in N$. Hence, it follows from (iii) that

$$[a, b] = [a, b]^m = [a, b]^{m^2} = \cdots = [a, b]^{m^u} = 0$$

for some positive integers $m > 1$ and u, and so, $ab = ba$. Thus, N is commutative. By Examples (1) and (4), it suffices to prove the assertion (1). Let n be an integer such that $n - 1$ is not a multiple of $p(p^s - 1)$ for all positive prime divisors p of $n - 1$ and all positive integers $s > 1$. Now, we assume that R is non-commutative. Then, since N is commutative, it is easily seen that R is a ring of the Type (d) in Theorem 4. Hence

$$E = \{e, 0\} \subset C, \quad Re \not\subset C, \quad R = Re + R(1 - e), \quad R(1 - e) \subset N,$$

and the factor ring $Re/(Re \cap N)$ is a finite field $GF(p^s)$ such that $p^s - 1$ is a divisor of $n - 1$. Hence $n - 1 = q(p^s - 1)$ for some integer q. If $s = 1$ then N is non-commutative by Lemma 2(1). Hence we have $s > 1$. By the condition on n, p is not a divisor of q. This implies that p is not a divisor of $n - 1$. Therefore, it follows from Lemma 2(2) that N is non-commutative. This is a contradiction. Thus, R is commutative. □

Examples 1. We shall present some examples of rings of Types (b), (c) and (d) in Theorem 4. In what follows, $\{e_{ij} \mid 1 \le i,\ j \le 3\}$ means the set of matrix units in $(GF(2))_3$, the complete matrix ring of order 3 over $GF(2)$.

(1) Type (b) for any integer $n > 1$: $R = GF(2)$ where $N = \{0\}$.

(2) Type (c) for any integer $n > 2$: $R = GF(2) \oplus GF(2) \oplus N$ where $N = \{e_{12}x + e_{13}y + e_{23}z \mid x, y, z \in GF(2)\}$.

(3) Type (d) for $n = 5$ (the case such that N is non-commutative): $R = \{(e_{11} + e_{22} + e_{33})u + e_{12}x + e_{13}y + e_{23}z \mid u, x, y, z \in GF(2)\}$ where $N = \{e_{12}x + e_{13}y + e_{23}z \mid x, y, z \in GF(2)\}$.

(4) Type (d) for $n = rp(p^s - 1) + 1$ with any positive prime integer p and any positive integers r and $s > 1$ (the case such that N is commutative): We shall present an example which is a non-commutative ring of Type (d) and satisfies the condition (i)$''$, (ii) and (iii) in Theorem 5 for $n = rp(p^s - 1) + 1$ with the above p, r and s. Now, we set $h = p^s$ ($s > 1$), and consider the finite field $GF(h)$. It is well known that $GF(h)\backslash\{0\}$ is a multiplicative cyclic group of order $h - 1$. Hence $v^{h-1} = 1$ for each $v \in GF(h)\backslash\{0\}$. We set

$$T = GF(h) \otimes_{GF(p)} GF(h) \quad \text{(tensor product)}.$$

Then T is a right $GF(h)$-module by the multiplication

$$(a \otimes b)v = a \otimes (bv), \quad v \in GF(h).$$

Moreover, T is a left $GF(h)$-module by the multiplication

$$v(a \otimes b) = (va) \otimes b, \quad v \in GF(h).$$

Next, we consider the module

$$R = GF(h) \times T; \qquad (v, t) + (v', t') = (v + v', t + t').$$

Since T is a left-right-$GF(h)$-module, we can define a product in R by the following

$$(v, t)(v', t') = (vv', vt' + tv').$$

Then R is a non-commutative ring such that for any $v \in GF(h)\backslash GF(p)$ ($\neq \emptyset$),

$$(v, 0)(1, 1 \otimes 1) = (v, v \otimes 1) \neq (v, 1 \otimes v) = (1, 1 \otimes 1)(v, 0).$$

Obviously, $(1, 0)$ is the identity of R. Now, we set $N = \{(0, t) \mid t \in T\}$. Then N is a commutative ideal of R such that $N^2 = \{(0, 0)\}$. If $(v, t) \in R\backslash N$ then $v \neq 0$ and

$$(v, t)^{p(h-1)} = ((v, t)^{h-1})^p = (v^{h-1}, t')^p = (1, t')^p = (1, pt') = (1, 0)$$

for some $t' \in N$. Now, let r be a positive integer, and $d = rp(h - 1)$. Let $x, y \in R\backslash N$. Then $x^d = (1, 0)$, $x^{d+1} = x$ and $y^{d+1} = y$. Therefore, it follows that

$$x^n y - xy^n = x^{d+1}y - xy^{d+1} = xy - xy = (0, 0) \in N \cap C.$$

Moreover, it is easily seen that N is the set of all nilpotent elements of R and $\{(1, 0), (0, 0)\}$ is the set E of all idempotent elements of R. Further, $N^* = N$ and it is commutative. Therefore, one will see that R satisfies the conditions (i)$''$, (ii) and (iii) in Theorem 5 for $n = d + 1 = rp(h - 1) + 1$.

Remark. We shall present an alternative proof of Theorem 3 in virtue of Theorem 4. Let R be a ring which satisfies the conditions (i)$''$, (ii)$'$ and (iii) in Theorem 3. Obviously R satisfies the conditions (i)$''$ and (ii) in Corollary 2. Hence R is normal and periodic. By Theorem 4, N is an ideal of R. Hence by (iii), N is commutative and $N^2 \subset C$. Now, we assume that R is non-commutative. Then, it follows that R is a ring of Type (d) in Theorem 4 such that

$$E = \{e, 0\} \subset C, \quad R = Re + R(1-e) \ \text{ and } \ R(1-e) \subset N \cap C.$$

Let $a \in Re \cap N$. Then $e + a$, $e \in Re \backslash (Re \cap N)$. Hence

$$C \ni (e+a)^n e - (e+a)e^n = (n-1)a + c, \quad c \in C.$$

This implies that $(n-1)a \in C$, and so, $(n-1)[a, x] = 0$ for all $x \in Re$. Then $n![a, x] = 0$, so that $[a, x]_k = 0$ for some positive integer k (by (ii)$'$). Hence by [2, Theorem], Re is commutative, and so, R is commutative. This is a contradiction. Thus, R is commutative.

In Example 1(4), we set $n = 7 = 2(2^2-1)+1$ and $GF(2^2) = \{0,\ g,\ g^2,\ g^3 = 1\}$. Then, one will easily see that $7![(0,\ 1 \otimes 1),\ (g,\ 0)] = 0$ and

$$0 \neq (0,\ 1 \otimes g - g \otimes 1) = [(0,\ 1 \otimes 1),\ (g,\ 0)]_{1+3n}$$

Hence, this example does not satisfy (ii)$'$, while it satisfies (ii).

Acknowledgment

The authors would like to thank Prof. Taichi Nakamoto, Kurashiki Univ. of Science and the Arts, Prof. Miguel Ferrero, Universidade Federal, and the referee for their valuable comments and suggestions.

References

[1] H. E. Bell, *Some commutativity results for periodic rings,* Acta Math. Acad. Sci. Hung. **28**(1976), 279–283.

[2] H. E. Bell, *A commutativity theorem for periodic rings,* Math. Japonica **33**(1988), 661–662.

[3] M. Chacron, *On a theorem of Herstein,* Canad. J. Math. **21**(1969), 1348–1353.

[4] J. Grosen, H. Tominaga and A. Yaqub, *On weakly periodic rings, periodic rings and commutativity theorems,* Math. J. Okayama Univ. **32**(1990), 77-81.

[5] I. N. Herstein *A theorem on rings,* Canad. J. Math. **5**(1953), 238–241.

[6] I. N. Herstein *A condition for the commutativity of rings,* Canad. J. Math. **9**(1957), 583–586.

[7] T. Nagahara and A. Yaqub, *Classification of rings satisfying some Herstein's condition on the set of all non-nilpotents,* Communications in Algebra **30(7)**(2002), 3087–3105

[8] H. Tominaga and A. Yaqub, *Some commutativity conditions for left s-unital rings satisfying certain polynomial identities,* Resultate Math. **6**(1983), 217–219.