Math. J. Okayama Univ. 31 (1989), 101−120

CHACRON'S CONDITION AND COMMUTATIVITY THEOREMS

Dedicated to Professor Hiroyuki Tachikawa on his 60th birthday

HIROAKI KOMATSU and HISAO TOMINAGA

In his paper [1], M. Chacron observed the commutativity of rings R satisfying the following condition :

(C) For each x, y in R, there exist $f(X)$, $g(X)$ in $X^2\mathbf{Z}[X]$ such that $[x-f(x), y-g(y)]=0$.

He defined the *cohypercenter* $C'=C'(R)$ of a ring R as the set of all elements a in R such that for each $x\in R$ there holds $[a, x-f(x)]=0$ with some $f(X)$ in $X^2\mathbf{Z}[X]$, which is a commutative subring of R ([1, Remark 12]). We summarize the results of [1] as follows (as for notations used without mention, see the below):

Theorem C. *Suppose that R satisfies* (C).

(1) *C' is a commutative subring of R containing N.*

(2) *N is a commutative ideal of R containing D.*

(3) $N[C', R]=[C', R]N=0$ and $[C', R]\subseteq N^*$.

In the present paper, we shall study rings satisfying (C) by making use of the recent result of W. Streb [11].

In § 1, we shall state the results of [11]. Without doubt, Streb gave his mind to applying his result to commutativity theorems. In the present paper, too, Proposition 1 and Corollary 1 will play essential roles. In § 2, we shall characterize the class of rings satisfying (C) and the polynomial identity $[X^n, Y^n]=0$ (Theorem 1), and improve the main theorem of [8] (Corollary 2). § 3 contains two commutativity theorems for rings satisfying (C) (Theorem 2 and Theorem 3), which include the main theorem of [9] and Theorem 3 of [6], respectively. The theorem of [13] are the jumping-off place for the work in § 4 ; § 4 deals with commutativity of rings satisfying some related conditions (Theorems 4 and 5).

Throughout, R will represent a ring with center $C=C(R)$. Let $N=N(R)$ denote the set of nilpotent elements in R, and $N^*=N^*(R)$ the subset of N consisting of all elements in R which square to zero. In case $N=0$, R is called *reduced*. Let $D=D(R)$ be the commutator ideal of R. Given a positive integer n, we put $E_n = \{x \in R \mid x^n = x\}$. In case $E = E_2 \subseteq C$, R is called *normal*. If q (>1) is a power of a prime and $r > 1$ and s are integers with $(r, s) = 1$, we put

$$R(q, r, s) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{q^s} \end{pmatrix} \middle| \alpha, \beta \in \mathrm{GF}(q^r) \right\}.$$

Obviously, $\alpha \mapsto \alpha^{q^s}$ induces a (non-trivial) automorphism of $\mathrm{GF}(q^r)$ whose fixed field is $\mathrm{GF}(q)$. For $x, y \in R$, define $[x, y] = xy - yx$ and define extended commutators $[x, y]_k$ as follows: let $[x, y]_0 = x$, and proceed inductively $[x, y]_k = [[x, y]_{k-1}, y]$. Finally, for a subset S of R, we use the following notations: $\langle S \rangle$ (resp. (S)) is the subring (resp. ideal) of R generated by S. $C_R(S) = \{r \in R \mid [r, S] = 0\}$. $l_R(S) = \{r \in R \mid rS = 0\}$. $\mathrm{Ann}(S) = \{r \in R \mid rS = Sr = 0\}$.

1. Streb's theorem. The main theorem of [11] is the next

Theorem S. *Let R be a non-commutative ring $(R \neq C)$. Then there exists a factorsubring of R which is of type* a), b), c), d), e) *or* f):

a) $\begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & 0 \end{pmatrix}$ *or* $\begin{pmatrix} 0 & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$, *$p$ a prime.*

b) $R(q, r, s)$.

c) *A non-commutative division ring.*

d) *A simple radical ring with no non-zero divisors of zero.*

e) *A finite nilpotent ring S such that $D(S)$ is the heart of S and $SD(S) = D(S)S = 0$.*

f) *A ring S generated by two elements of finite additive order such that $D(S)$ is the heart of S, $SD(S) = D(S)S = 0$ and $N(S)$ is a commutative nilpotent ideal of S.*

The proof of Theorem S can be completed by the reduction to the following proposition. For the sake of completeness, we shall give its proof.

Proposition 1. *Let R be a non-commutative ring.*

(1) *If R is semi-primitive, then there exists a factorsubring of R which is of type* a) *or* c).

(2) *If $D \subseteq C$, then there exists a factorsubring of R which is of type* e) *or* f).

(3) *If $xy \neq 0 = yx$ for some $x, y \in R$, then there exists a factorsubring*

of R which is of type a), e) *or* f).

(4) *If R contains a non-central element y such that* $(y)^2 = 0$, *then there exists a factorsubring of R which is of type* a), b), e) *or* f).

Proof. (1) This can be easily seen, by the structure theorem of primitive rings.

Claim 1. Let x, y be elements of R with $[x, y] \neq 0$. Choose an ideal M of $\langle x, y\rangle$ which is maximal with respect to $[x, y] \notin M$, and put $S = \langle x, y\rangle/M$. Then $D(S) = ([\bar{x}, \bar{y}])$ is the heart of S and $S/D(S)$ is a commutative Noetherian ring.

Proof. Obviously, $D(S)$ is the heart of S and $S/D(S)$ is homomorphic to the subring $\langle X, Y\rangle$ of $\boldsymbol{Z}[X, Y]$. Noting that every ideal of $\langle X, Y\rangle$ is an ideal of $\boldsymbol{Z}[X, Y]$, we see that $\langle X, Y\rangle$ is Noetherian, and therefore so is $S/D(S)$.

Claim 2. Every factorfield of $\boldsymbol{Z}[X_1, \cdots, X_n]$ is a finite field. Therefore, if a field is finitely generated as ring then it is finite.

Proof. Let $L = K[a_1, \cdots, a_n]$ be a factorfield of $\boldsymbol{Z}[X_1, \cdots, X_n]$, where K is the prime field of L. By Noether normalizing theorem, every a_i is algebraic over K, namely there exists a non-zero $f_i(X) \in \boldsymbol{Z}[X]$ such that $f_i(a_i) = 0$. Let m_i be the leading coefficient of $f_i(X)$. If $K = \boldsymbol{Q}$ then L is integral over $\boldsymbol{Z}[m_1^{-1}, \cdots, m_n^{-1}]$, and therefore $\boldsymbol{Z}[m_1^{-1}, \cdots, m_n^{-1}]$ must be the field $\boldsymbol{Q}$. But this is impossible. Hence K is a finite field, and therefore so is L.

(2) In view of Claim 1, without loss of generality, we may assume that R is generated by two elements and $D(R)$ is the heart of R. First, we shall show that $A = l_R(D(R))$ is not commutative. Suppose, to the contrary, that A is commutative. Then, noting that $A \neq R$ and $D(R)$ is a minimal left ideal of R, we see that A is a primitive ideal of R. If $A = 0$ then, by the structure theorem of primitive rings, R has a non-commutative simple factorsubring R'. But then $D(R') = R' \not\subseteq C(R')$, which is a contradiction. Hence $A \neq 0$ and $D(R) \subseteq A$. Now, R/A is a field, which is isomorphic to some GF(q) by Claim 2. Since $D(R) \subseteq C(R)$ and $x^q - x \in A$, $qx \in A$ for all $x \in R$, we get $[x, y] = qx^{q-1}[x, y^q - y] - qy^{q-1}[x, y] + [x, y] = [x^q, y^q - y] - [x, y^q] + [x, y] = [x^q - x, y^q - y] = 0$ for all $x, y \in R$. This contradiction shows that A is not commutative, so that, by Claim 1, there exists a factorsubring S of A generated by two elements such that $D(S)$ is the heart of S and $S/D(S)$ is Noetherian. Obviously, $SD(S) = D(S)S = 0$, and so $D(S) \simeq \boldsymbol{Z}/p\boldsymbol{Z}$ with some prime p, as additive group. Since S is subdirectly irreducible and $pD(S) = 0$, the torsion ideal T of S is p-primary and $p^kT = 0$ for some

positive integer k. If $p^kS \neq 0$ then $D(S) \subseteq p^kS$, and so $D(S) \subseteq p^kS \cap T = p^kT = 0$, which is a contradiction. Hence $p^kS = 0$. Further, noting that $N(S/D(S)) = N(S)/D(S)$ is a nilpotent ideal of the commutative Noetherian ring $S/D(S)$, we see that $N(S)$ is a nilpotent ideal of S. If $N(S)$ is commutative then S is of type f). Suppose now that $N(S)$ is not commutative. Then, again by Claim 1, there exists a factorsubring S' of $N(S)$ generated by two elements such that $D(S')$ is the heart of S'. Obviously, $S'/D(S')$ is a finite nilpotent ring and $D(S')$ is finite. Therefore S' is of type e).

(3) If $x^2y = xy^2 = 0$ then $D(\langle x, y\rangle) \subseteq C(\langle x, y\rangle)$, and so there exists a factorsubring of $\langle x, y\rangle$ which is of type e) or f), by (2). Next, if $x^2y \neq 0$ then $x(xy) \neq 0 = (xy)x = (xy)^2$, and so we may, and shall, assume that $xy \neq 0 = yx = y^2$. Consider $S = \langle x, y\rangle/M$ as in Claim 1. In case $\bar{x}^2\bar{y} = 0$, by the above, there exists a factorsubring of S which is of type e) or f). We assume therefore $\bar{x}^2\bar{y} \neq 0$. Since $D(S)$ is the heart of S, the ideal $D(S)$ is generated by $\bar{x}^2\bar{y} = [\bar{x}, \bar{x}\bar{y}]$. Since $D(S) = \boldsymbol{Z}\bar{x}^2\bar{y} + \langle\bar{x}\rangle\bar{x}^2\bar{y} = D(\langle\bar{x}, \bar{x}\bar{y}\rangle)$, we have $\bar{x}\bar{y} = [\bar{x}, \bar{y}] \in D(\langle\bar{x}, \bar{x}\bar{y}\rangle)$. Consider again $S' = \langle\bar{x}, \bar{x}\bar{y}\rangle/M'$ as in Claim 1, and put $a = \bar{x}+M'$ and $b = \bar{x}\bar{y}+M'$. Then $D(S') = (b)$. Further, noting that $bS' = 0$, we see that (b) is an irreducible left $\langle a\rangle$-module. Since $l_{\langle a\rangle}((b))$ is an ideal of S', $l_{\langle a\rangle}((b)) \neq 0$ forces a contradiction $(b) \subseteq l_{\langle a\rangle}((b)) \subseteq \langle a\rangle$. Therefore $l_{\langle a\rangle}((b)) = 0$, and hence $\langle a\rangle$ is a field, which is isomorphic to some $\mathrm{GF}(q)$, by Claim 2. Hence $S' = \langle a\rangle \oplus \langle a\rangle b \simeq \begin{pmatrix} \mathrm{GF}(q) & \mathrm{GF}(q) \\ 0 & 0 \end{pmatrix}$. Finally, if $xy^2 \neq 0$, we can apply the above argument to see that there exists a factorsubring of R which is of type e) or f), or isomorphic to $\begin{pmatrix} 0 & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$.

(4) In view of Claim 1, we may assume that $R = \langle x, y\rangle$ and $D(R)$ is the heart of R. In view of (2), we may assume further that $[x, [x, y]] \neq 0$. Consider $S = \langle x, [x, y]\rangle/M$ as in Claim 1, and put $a = x+M$ and $b = [x, y]+M$. Then $D(R) = ([x, [x, y]]) = D(\langle x, [x, y]\rangle)$ implies that $D(S) = (b)$. In view of (3), we may assume that S is completely reflexive, namely $st = 0$ implies $ts = 0$ for any $s, t \in S$. We can easily see that $l_{\langle a\rangle}((b))$ is an ideal of S, and therefore $l_{\langle a\rangle}((b))$ must be zero. Now, let a_L and a_R be the additive group endomorphisms of (b) induced by the left multiplication and the right multiplication effected by a, respectively. The left $\langle a_L, a_R\rangle$-module (b) is irreducible, and therefore $\langle a_L, a_R\rangle$ is a field, which is finite by Claim 2. Since the subfields $\langle a_L\rangle$ and $\langle a_R\rangle$ have the same order, $\langle a_L\rangle$ coincides with

$\langle a_R \rangle$. Hence $S = \langle a \rangle \oplus \langle a \rangle b$ is of type (b).

Proof of Theorem S. Let R be a non-commutative ring. In view of Claim 1 in the proof of Proposition 1, we may assume that $R = \langle x, y \rangle$ and D is the heart of R. In case $D^2 = 0$, we can apply Proposition 1 (2) and (4). Henceforth, we assume therefore that $D^2 \neq 0$. Then D is a simple ring. Now, in view of Proposition 1 (1) and (3), we may assume that R is a completely reflexive non-semiprimitive ring. Then D is contained in the Jacobson radical of R, and so D is a radical ring. Furthermore, for every non-zero x in D, the ideal $l_D(x)$ must be zero ; D is of type (d).

Corollary S.1. *Suppose that R satisfies the following condition considered in* [10] :

(SC) *For each $x, y \in R$, there exists a polynomial $f(X, Y)$ in $\mathbf{Z}\langle X, Y\rangle [X, Y]\mathbf{Z}\langle X, Y\rangle$ each of whose monomials is of length ≥ 3 such that $[x, y] = f(x, y)$.*

Then there exists no factorsubring of R which is of type e) *or* f). *Therefore, if R is non-commutative, then there exists a factorsubring of R which is of type* a), b), c) *or* d).

By a theorem of Herstein [2] (signified as Theorem H), a ring R is commutative if (and only if) R satisfies the condition

(H) For each $x \in R$, there exists $f(X)$ in $X^2\mathbf{Z}[X]$ such that $x - f(x) \in C$.

Obviously, Corollary S.1 enables us to reduce the proof of Theorem H to the case that R is a division ring. By making use of Theorem H, we can prove Theorem C (see [3]).

Now, the next which is crucial in our subsequent study is immediate by Corollary S.1 and Theorem C.

Corollary 1. *Suppose that R satisfies* (C). *Then there exists no factorsubring of R which is of type* c), d), e) *or* f). *Therefore, if R is non-commutative, then there exists a factorsubring of R which is of type* a) *or* b).

2. Condition (C) and the identity $[X^n, Y^n] = 0$. First, as preliminary, we shall establish fundamental results for rings R with (C).

Lemma 1. *Let $x \in R$, $a \in C'$ and n a positive integer.*

(1) *If $x^n[a, x] = [a, x]x^n = 0$ then $[a, x] = 0$.*

(2) *Suppose that R satisfies* (C). *If $[a, x]_n = 0$ then $[a, x] = 0$.*

Proof. (1) There exists $f_1(X)$ in $X^2\mathbf{Z}[X]$ such that $[a, x-f_1(x)] = 0$. Again there exists $f_2(X)$ in $X^2\mathbf{Z}[X]$ such that $[a, f_1(x)-f_2(f_1(x))] = 0$. Repeating the same procedure, we can choose a positive integer r such that $g(X) = f_r(\cdots f_2(f_1(X))\cdots) \in X^{2^n}\mathbf{Z}[X]$. Then, by hypothesis, we can easily see that $[a, g(x)] = 0$. Hence $[a, x] = 0$.

(2) Suppose, to the contrary, that $[a, x] \neq 0$. Then, without loss of generality, we may assume that $[a, x]_{n-1} \neq 0$. Suppose $n > 1$, and consider the non-commutative subring $T = \langle [a, x]_{n-2}, x \rangle$. Then $D(T) = ([a, x]_{n-1})$. Noting that $[C', R] \subseteq N^* \subseteq C'$ and C' is commutative by Theorem C, we see that $[a, x]_{n-1} \in C(T)$. Hence $[D(T), T] = [[a, x]_{n-1}T, T] = [a, x]_{n-1}[T, T] \subseteq [C', R]N = 0$, namely $D(T) \subseteq C(T)$, again by Theorem C. Then, by Proposition 1 (2), there exists a factorsubring of T which is of type e) or f). But this is impossible by Corollary 1.

Lemma 2. *If R satisfies* (C), *then* $\mathrm{Ann}([C', R]) = \mathrm{Ann}([N^*, R])$ *is the largest commutative ideal of R and is contained in the commutative subring $C_R(C') = C_R(N^*)$ of R, and $R/\mathrm{Ann}([N^*, R])$ is a commutative reduced ring.*

Proof. Since $D \subseteq C' \subseteq C(C_R(C'))$ by Theorem C, in view of Proposition 1 (2) and Corollary 1, $C_R(C')$ is commutative. Put $I = \mathrm{Ann}([C', R])$. By making use of Lemma 1 (1), we can easily see that $I \subseteq C_R(C')$. Now, let K be an arbitrary commutative ideal of R. For each $x \in K$ and $a \in C'$, there exists $f(X)$ in $X^2\mathbf{Z}[X]$ such that $[a, x-f(x)] = 0$. Since $K^2 \subseteq C$, we get $[a, x] = 0$. Then, we can easily see that $K \subseteq I$. Hence, I is the largest commutative ideal of R. In particular, $D \subseteq I$ by Theorem C. We define an ideal M of R by $M/I = N(R/I)$. Then, using Lemma 1 (1), we get $M \subseteq C_R(C')$, and hence $M = I$, which means that R/I is reduced.

Now, obviously $I \subseteq \mathrm{Ann}([N^*, R])$. Let $x \in \mathrm{Ann}([N^*, R])$ and $a \in C'$. Since $[a, x] \in N^*$ by Theorem C, we have $x[[a, x], x] = [[a, x], x]x = 0$. Hence $[[a, x], x] = 0$ by Lemma 1 (1), and therefore $[a, x] = 0$ by Lemma 1 (2). This shows that $\mathrm{Ann}([N^*, R]) \subseteq C_R(C')$. As proved above, I is the largest commutative ideal. Hence $I = \mathrm{Ann}([N^*, R])$. Similarly, we can show that $C_R(C') = C_R(N^*)$.

Lemma 3. *Let n be a power of a prime p. Suppose that R satisfies* (C) *and the identity* $[X^n, Y^n] = 0$. *If $p[N^*, R] = 0$, then R is commutative.*

Proof. Suppose, to the contrary, that R is not commutative. In view of Corollary 1, R has a factorsubring R' isomorphic to some $R(q, r, s)$. Since

pR is commutative by Lemma 2, pR' is also commutative. This means that $p|q$. On the other hand, R' satisfies $[X^n, Y^n] = 0$. But this is impossible, since n is a power of the characteristic of R'.

Now, we consider the following conditions, where A is a non-empty subset of R and n is a positive integer:

$(\text{ii-}A)_n$ $[a, x^n] = 0$ for all $x \in R$ and $a \in A$.

$(\text{ii-}A)_n^*$ For each $x \in R$ and $a \in A$, there exists a positive integer k such that $[a, x^n]_k = 0$.

$(\text{jj-}A)_n^*$ For each $x \in R$ and $a \in A$, there exists a positive integer k such that $[(x+a)^n, x^n]_k = 0$.

$Q(n\,;\,A)$ If $x \in R$, $a \in A$ and $n[a, x] = 0$, then $[a, x] = 0$.

(Note that the condition $Q(n\,;\,A)$ is denoted as $(A)_n^*$ in [9].)

Lemma 4. *Let A be a subset of C' containing N^*, and n a positive integer. Suppose that R satisfies* (C). *Then the following are equivalent:*

1) *R satisfies the identity $[X^n, Y^n] = 0$.*
2) *R satisfies $(\text{jj-}A)_n^*$.*
3) *R satisfies $(\text{ii-}A)_n^*$.*
4) *R satisfies $(\text{ii-}A)_n$.*

Proof. Obviously, 1) implies 2), and 3) does 4) by Lemma 1 (2).

2) ⇨ 3). Let $x \in R$ and $a \in A$. Noting that $[A, R] \subseteq N^*$ and N is a commutative ideal of R by Theorem C, there exists a positive integer k such that

$$\begin{aligned}[a, x^n]_{k+1} &= [\textstyle\sum_{i=0}^{n-1} x^i[a, x]x^{n-i-1}, x^n]_k \\ &= [(x+[a, x])^n, x^n]_k \\ &= 0.\end{aligned}$$

4) ⇨ 1). Since $C_R(A)$ is commutative by Lemma 2, R satisfies the identity $[X^n, Y^n] = 0$.

We are now in a position to state our first theorem.

Theorem 1. *Let n be a positive integer. Then the following conditions are equivalent:*

1) *R satisfies the identity $[X-X^m, Y-Y^m] = 0$ for some integer $m > 1$, and satisfies the identity $[X^n, Y^n] = 0$.*

2) *R satisfies* (C) *and the identity $[X^n, Y^n] = 0$.*

3) *R satisfies* (C) *and* (ii-$N^*)_n^*$.

4) *R satisfies* (C) *and* (jj-$N^*)_n^*$.

5) *R is a subdirect sum of a commutative ring and* $R(q, r, s)$*'s such that* $(q^r-1)/(q-1)\mid n$.

Proof. Obviously, 1) implies 2) and 2)−4) are equivalent by Lemma 4.

5) ⇒ 1). Let Q be the (finite) set of all integers $q>1$ such that q is a power of a prime and $(q^r-1)/(q-1)\mid n$ with some integer $r>1$, and let $m = n\prod_{q\in Q}(q-1)+1$. Now, let $q>1$ be a power of a prime such that $(q^r-1)/(q-1)\mid n$ with an integer $r>1$. Then, for any $\alpha\in \mathrm{GF}(q^r)$, we have $\alpha^m=\alpha$ and $\alpha^n\in \mathrm{GF}(q)$. Hence we can easily see that $R(q, r, s)$ satisfies the identities $[X-X^m, Y-Y^m]=[X^n, Y^n]=0$, proving 1).

2) ⇒ 5). We assume that R is a non-commutative subdirectly irreducible ring satisfying (C) and the identity $[X^n, Y^n]=0$. By Lemma 4, R satisfies (ii-$N^*)_n$.

If R contains x, y such that $xy=0\neq yx$ then, by Proposition 1 (3), there exists a factorsubring of R which is of type a), e) or f). But this is impossible by Corollary 1. Hence, R is completely reflexive. Now, let H be the heart of R, and B the set of all zero-divisors of R (together with 0). Then, as is well-known, $B=\mathrm{Ann}(H)$, which is an ideal of R.

Since R is subdirectly irreducible, the torsion ideal of R is a p-primary additive group for some prime p. We let $n=p^t n'$, where $t\geq 0$ and $n'>0$ are integers and $(p, n')=1$. Put $S=\{x^{p^t}\mid x\in R\}$ and $k=p^{\varphi(n')}-1$, where φ is Euler's function.

Claim 1. $p[N^*, R]=0$, $n'>1$ and $k>1$.

Proof. Let $x\in R$ and $a\in N^*$ with $[a, x]\neq 0$. For any $i=1,2,\cdots, n-1$, we have

$$\sum_{j=1}^{n-1} i^j\binom{n}{j}[a, x^{n(n-j)+j}]=[a,(x^n+ix)^n]-[a, x^{n^2}]-[a,(ix)^n]=0.$$

Therefore, the usual Vandermonde determinant argument shows that $d[a, x]x^{n(n-1)}=d[a, x^{n(n-1)+1}]=0$ for some positive integer d. Hence $d[a, x]=0$ by Lemma 1 (1). Suppose now that the additive order of $[a, x]$ is p^s for some integer $s>1$, and put $y=p^{s-1}x$. Then, there exists $f(X)\in X^2\mathbf{Z}[X]$ such that $[a, y-f(y)]=0$, which forces a contradiction $[a, y]=0$. Hence $p[N^*, R]=0$. Combining this with Lemma 3, we get $n'>1$ and therefore $k>1$.

Claim 2. $\mathrm{Ann}([N^*, S])=\mathrm{Ann}([N^*, R])$.

Proof. For any $x \in \mathrm{Ann}([N^*, S])$ and $a \in N^* \cap \mathrm{Ann}([N^*, S])$, we have $[a, x^{p^t}]x = 0$, and so $[a, x^{p^t}] = 0$ by Lemma 1 (1). Therefore, by Lemmas 4 and 3, $\mathrm{Ann}([N^*, S])$ is commutative. Hence, by Lemma 2, we obtain $\mathrm{Ann}([N^*, S]) = \mathrm{Ann}([N^*, R])$.

Claim 3. $[a, x]y^{k^2+k} = [a, x]x^k y^k = [a, x]y^k x^k$ for any $x, y \in S$ and $a \in N^*$.

Proof. Let $x, y \in S$, and $a \in N^*$. Since $n'|k$ by Euler's Theorem, we have $[a, x^k] = 0$. Furthermore, $k+1 = p^{\varphi(n')}$ and $[N^*, D] = [N^*, R]D = p[N^*, R] = 0$ by Theorem C and Claim 1. Now, noting that $x+y^k \in S+pR+D$ and $(x+y^k)^{k+1}-(x^{k+1}+y^{k^2+k}) \in pR+D$, we can easily see that

$$\begin{aligned}[a, x](x^{k+1}+y^{k^2+k}) &= [a, x](x+y^k)^{k+1} \\ &= [a, x+y^k](x+y^k)^{k+1} \\ &= [a, (x+y^k)^{k+1}](x+y^k) \\ &= [a, x^{k+1}+y^{k^2+k}](x+y^k) \\ &= [a, x^{k+1}](x+y^k) \\ &= [a, x](x^{k+1}+x^k y^k).\end{aligned}$$

Hence, we obtain $[a, x]y^{k^2+k} = [a, x]x^k y^k = [a, x]y^k x^k$ by $[N^*, R]D = 0$.

Claim 4. $L = R/B$ is a finite field of characteristic p and B is commutative.

Proof. Let $x, y \in S$ and $a \in N^*$. By Claim 3, we have

$$\begin{aligned}[a, x]y^{2k^2+k} &= [a, x]y^k x^k y^{k^2} = [a, x]y^{k^2+k}x^k \\ &= [a, x]y^k x^{2k} = [a, x]x^{2k}y^k.\end{aligned}$$

Repeating the same procedue, we get $[a, x]y^{(k+1)k^2+k} = [a, x]x^{(k+1)k}y^k$. Setting $x = y$ in Claim 3, we have $[a, x]x^{(k+1)k} = [a, x]x^{2k}$. Hence $[a, x]y^{k^3+k^2+k} = [a, x]x^{2k}y^k = [a, x]y^{2k^2+k}$. By Claim 2, $z^{p^t(k^3+k^2+k)} - z^{p^t(2k^2+k)} \in \mathrm{Ann}([N^*, R])$ for any $z \in R$. But $\bar{R} = R/\mathrm{Ann}([N^*, R])$ is reduced by Lemma 2, and hence $\bar{R}$ satisfies the identity $X^{p^t(k^3-k^2)+1} = X$.

Since $\mathrm{Ann}([N^*, R])$ is commutative by Lemma 2, $[N^*, R]R$ is a non-zero ideal of R. Hence $H \subseteq [N^*, R]R$. Now, let $\sum a_i x_i$ be an arbitrary element of H, where $a_1, \cdots, a_n \in [N^*, R]$ and $x_1, \cdots, x_n \in R$. Then, as $\bar{R}$ is a regular ring, there exists $e \in R$ such that $\bar{x}_i\bar{e} = \bar{x}_i$ in $\bar{R}$ for $i = 1, \cdots, n$. Therefore $\sum a_i x_i e = \sum a_i x_i$. Hence $HR = H$ and $B \neq R$. Since $pR \subseteq \mathrm{Ann}([N^*, R]) \subseteq B$ and L has no non-zero divisors of zero, L is a finite field of characteristic p.

Let $x \in B$ and $a \in N^* \cap B$. For an arbitrary $z \in R \backslash B$, we can choose $e \in R$ such that $\bar{x}\bar{e} = \bar{x}$, $\bar{z}\bar{e} = \bar{z}$ and $\bar{e}^2 = \bar{e}$ in $\bar{R}$. Then $e \notin B$. By Claim 3, we see $[a, x^{p^t}]e = [a, x^{p^t}]e^{p^t(k^2+k)} = [a, x^{p^t}]x^{p^tk}e^{p^tk} = [a, x^{p^t}]x^{p^tk}$, and so $[a, x^{p^t}](e-x^{p^tk}) = 0$. Since $e-x^{p^tk} \notin B$, we get $[a, x^{p^t}] = 0$. Hence B is commutative by Lemmas 4 and 3.

Claim 5. $H = \mathrm{Ann}(B)$ and $[H : L] = 1$.

Proof. As is well-known, $L \otimes_{\mathrm{GF}(p)} L$ is the direct sum of $[L : \mathrm{GF}(p)]$ copies of L. Regarding $\mathrm{Ann}(B)$ as a left $L \otimes_{\mathrm{GF}(p)} L$-module, we can easily see that $[\mathrm{Ann}(B) : L] = 1$, and therefore $H = \mathrm{Ann}(B)$.

Claim 6. No non-zero ideal of R is contained in C.

Proof. It suffices to show that $H \not\subseteq C$. Suppose, to the contrary, that $H \subseteq C$. By Claim 4 and Lemma 2, we have $B \subseteq \mathrm{Ann}([N^*, R])$, and so $[N^*, R] \subseteq \mathrm{Ann}(B) = H \subseteq C$ by Claim 5. But, by Lemma 1 (2), this forces a contradiction $[N^*, R] = 0$.

We are now in a position to complete the proof of Theorem 1. Since $B^2 \subseteq C$ by Claim 4, we get $B^2 = 0$ by Claim 6, and so $B \subseteq \mathrm{Ann}(B) = H$ by Claim 5. Hence H is the only proper ideal of R (Claim 4). By Theorem C, D is a proper ideal of R, and therefore $pD = pH = 0$, which means $pR \subseteq C$. Hence $pR = 0$ by Claim 6, and R is a finite algebra with 1 over $\mathrm{GF}(p)$. Now, by Wedderburn factor theorem (see, e.g., [7, p.116, Theorem 5.37]), R contains a subfield L' isomorphic to L such that $R = L'+H$ and $L' \cap H = 0$. Hence R is isomorphic to some $R(q, r, s)$. Put $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q^s} \end{pmatrix}$ in $R(q, r, s)$, where α is a generating element of the multiplicative group of $\mathrm{GF}(q^r)$. Since $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is in $N^*(R(q, r, s))$, we have $(\alpha^{nq^s} - \alpha^n)a = [a, x^n] = 0$, which means that $\alpha^n \in \mathrm{GF}(q)$. Hence $q^r-1 \mid n(q-1)$, and so $(q^r-1)/(q-1) \mid n$.

The next improves [8, Theorem].

Corollary 2. *Let R be an s-unital ring, and $n > 1$ an integer. Then the following conditions are equivalent:*

1) *R satisfies the identity $[X^n, Y^n] = 0$ and $\mathrm{Q}(n) = \mathrm{Q}(n ; R)$.*

2) *R satisfies (C), (ii-N^*)$_n^*$ and $\mathrm{Q}(n ; N^*)$.*

3) *R satisfies (C), (jj-N^*)$_n^*$ and $\mathrm{Q}(n ; N^*)$.*

4) *R is a subdirect sum of a commutative ring and $R(q, r, s)$'s such that* $(q^r-1)/(q-1) \mid n$ and $(q, n) = 1$.

Proof. Obviously, 4) implies 1), and 2) and 3) are equivalent.

1) $\Rightarrow$ 2). It suffices to show that R satisfies (C). Put $f(X) = X-\{(1+nX)^n-1\}/n^2 \in X^2\mathbf{Z}[X]$. For each $x, y \in R$, we choose a pseudo identity e

of $\{x, y\}$ (see [4]). Then $0 = [(e+nx)^n, (e+ny)^n] = n^4[x-f(x), y-f(y)]$. Hence $[x-f(x), y-f(y)] = 0$ by Q(n).

2) ⇨ 4). R is a subdirect sum of a commutative ring R_0 and $R_i = R(q_i, r_i, s_i)$ such that $(q_i^{r_i}-1)/(q_i-1)\,|\,n$ ($i \in I$). Now, we suppose that $(q_k, n) \neq 1$ for some $k \in I$. Let $\alpha \in \mathrm{GF}(q_k^{r_k})\backslash\mathrm{GF}(q_k)$. Then, we can choose $x = (x_0, (x_i)_{i\in I})$ and $a = (a_0, (a_i)_{i\in I})$ in $R \subseteq R_0 \times \prod_{i\in I} R_i$ such that $x_k = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q_k^{s_k}} \end{pmatrix}$ and $a_k = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Let m be the product of all primes p such that $p\,|\,q_i$ for some $i \in I$ and $(p, q_k) = 1$ (if there exists no such prime, we set $m = 1$). Setting $y = mx$, we can easily see that $b = [a, y]$ is in N^* and $nb = 0$. But $[b, y] \neq 0$ and $n[b, y] = 0$, which is a contradiction.

3. Condition (C) and commutativity theorems. We shall examine commutativity of a ring satisfying (C).

First, we consider the following conditions, where A is a non-empty subset of R:

(III-A)* For each $x \in R$ and $a \in A$, there exist positive integers $m_1, \cdots, m_n$ and k such that $(m_1, \cdots, m_n) = 1$ and $[a, x^{m_i}]_k = 0$ for $i = 1, \cdots, n$.

(III-A)$^\sharp$ For each $x \in R$ and $a \in A$, there exist positive integers m and k such that $[a, x^m]_k = 0$ and $x = x' + x''$ with some $x' \in E_m$ and $x'' \in N$.

(JJJ-A)* For each $x \in R$ and $a \in A$, there exist positive integers $m_1, \cdots, m_n$ and k such that $(m_1, \cdots, m_n) = 1$ and $[(x+a)^{m_i}, x^{m_i}]_k = 0$ for $i = 1, \cdots, n$.

(iii-A)* For each $x \in R$ and $a \in A$, there exist positive integers $m_1, \cdots, m_n$, $m_1', \cdots, m_n'$ and k such that $(m_1m_1', \cdots, m_nm_n') = 1$ and $[(x^{m_i}(x+a)^{m_i})^{m_i'}, ((x+a)^{m_i}x^{m_i})^{m_i'}]_k = 0$ for $i = 1, \cdots, n$.

The conditions (III-A)* and (JJJ-A)* are weaker than those considered in [9], respectively.

By brief computation, we can easily see the next

Lemma 5. *Let* $x = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ *and* $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *be in* $\mathrm{M}_2(K)$, *where K is a field. Let $f(X)$ be in $XZ[X]$, and let k, m, n, m' and n' be positive integers with* $mn = m'n'$.

(1) $[a, f(x)]_k = (f(\beta)-f(\alpha))^k a$.

(2) $[f(x+a), f(x)]_k = -[f(x), f(x+a)]_k = (f(\beta)-f(\alpha))^{k+1}$

$(\beta-\alpha)^{-1}a$, *provided* $\alpha\neq\beta$.

(3) $[(f(x)^m f(x+a)^m)^n, (f(x+a)^{m'} f(x)^{m'})^{n'}]_k = (f(\beta)^{2mn} - f(\alpha)^{2mn})^{k+1} (f(\beta)^{m+m'} - f(\alpha)^{m+m'})(\alpha-\beta)^{-1}(f(\alpha)^m + f(\beta)^m)^{-1}(f(\alpha)^{m'} + f(\beta)^{m'})^{-1}a$, *provided* $f(\alpha)^{2m}\neq f(\beta)^{2m}$ *and* $f(\alpha)^{2m'}\neq f(\beta)^{2m'}$.

The next improves [9, Theorem 1].

Theorem 2. *The following conditions are equivalent:*

0) *R is commutative.*

1) *R satisfies* (C) *and* (III-N^*)*.

2) *R satisfies* (C) *and* (III-N^*)$^\#$.

3) *R satisfies* (C) *and* (JJJ-N^*)*.

4) *R satisfies* (C) *and* (iii-N^*)*.

5) *R satisfies* (C) *and there exists a positive integer n for which R satisfies* (ii-N^*)$_n^*$ *and* Q($n!$; N^*).

6) *R satisfies* (C) *and there exists a positive integer n for which R satisfies* (jj-N^*)$_n^*$ *and* Q($n!$; N^*).

Proof. Obviously, 0) implies 1)−6).

4) ⇒ 0). Suppose that there exists a homomorphism ψ of a subring of R onto some $R(q, r, s)$. Let α be a generating element of the multiplicative group of GF(q^r) and choose $x, y\in R$ such that $\psi(x) = \begin{pmatrix}\alpha & 0\\ 0 & \alpha^{q^s}\end{pmatrix}$ and $\psi(y) = \begin{pmatrix}0 & (\alpha^{q^s}-\alpha)^{-2}\\ 0 & 0\end{pmatrix}$. Since $a=[y, x]_2$ is in N^* by Theorem C, there exist positive integers $m_1,\cdots,m_n,m_1',\cdots,m_n'$ and k such that $(m_1m_1',\cdots,m_nm_n')=1$ and $[(x^{m_i}(x+a)^{m_i})^{m_i'}, ((x+a)^{m_i}x^{m_i})^{m_i'}]_k=0$ for $i=1,\cdots,n$. Noting that $\psi(a) = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, by Lemma 5 (3), we get $\alpha^{2m_im_i'}\in$ GF(q) for $i=1,\cdots,n$, and hence $\alpha^2\in$ GF(q). But this means that $(q^r-1)/(q-1)\,|\,2$, which is impossible. By a similar argument, R has no factorsubring of type a). Hence, by Corollary 1, R is commutative.

Similarly, by making use of Lemma 5 (1) and (2) instead of Lemma 5 (3), we can easily see that each of 1)−3) implies 0).

5) or 6) ⇒ 0). Suppose that R is non-commutative. By Theorem 1, R is a subdirect sum of a commutative ring and $R(q_i, r_i, s_i)$'s such that $(q_i^{r_i}-1)/(q_i-1)\,|\,n$ $(i\in I)$. Let m be the product of all primes p such that $p\,|\,q_i$ for some $i\in I$. Then $mD=0$. Since $m\,|\,n!$, we get $[N^*, R]=0$ by Q($n!$; N^*). Hence R is commutative by Lemma 2, which is a contradiction.

Next, we consider the following conditions which are stronger than (C) :

(C)$_1$ For each x, y in R, there exist $f(X)$, $g(X)$, $h(X)$ in $X^2\mathbf{Z}[X]$ and a positive integer k such that $[x-f(x), y-g(y)] = [f(x+y-h(y)), f(x)]_k = 0$.

(C)$_2$ For each x, y in R, there exist $f(X)$, $g(X)$, $h(X)$ in $X^2\mathbf{Z}[X]$ and a positive integer k such that $[x-f(x), y-g(y)] = [f(x), f(x+y-h(y))]_k = 0$.

(C)$_3$ For each x, y in R, either $[x, y] = 0$ or there exist $f(X)$ in $X\mathbf{Z}[X]$, $g(X)$, $h(X)$ in $X^2\mathbf{Z}[X]$ and positive integers k, n such that $f(X)^n \in X^2\mathbf{Z}[X]$, $x-f(x)^n \in N$ and $[x-f(x)^n, y-g(y)] = [(f(x)f(x+y-h(y)))^n, (f(x+y-h(y))f(x))^n]_k = 0$.

(C)$_4$ For each x, y in R, either $[x, y] = 0$ or there exist $g(X)$, $h(X)$ in $X^2\mathbf{Z}[X]$ and positive integers k, m, n, m' and n' such that $mn = m'n' > 1$, $(m+m', mn-1)\,|\,2mn$, $x-x^{mn} \in N$ and $[x-x^{mn}, y-g(y)] = [(x^m(x+y-h(y))^m)^n, ((x+y-h(y))^{m'}x^{m'})^{n'}]_k = 0$.

Theorem 3. *The following conditions are equivalent*:

0) *R is commutative.*

1) *R satisfies* (C)$_1$.

2) *R satisfies* (C)$_2$.

3) *R satisfies* (C)$_3$.

4) *R satisfies* (C)$_4$.

Proof. Obviously, 0) implies 1)$-$4).

1) $\Rightarrow$ 0). First, suppose that $\begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & 0 \end{pmatrix}$ satisfies (C)$_1$. For $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, there exists $f(X)$ in $X^2\mathbf{Z}[X]$ and a positive integer k such that $[x-f(x), a] = [f(x+a), f(x)]_k = 0$. But $f(1) = 1$ ($\in \mathrm{GF}(p)$) by $[x-f(x), a] = 0$, and hence $[f(x+a), f(x)]_k \neq 0$ by Lemma 5 (2). This is a contradiction. Similarly, $\begin{pmatrix} 0 & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$ does not satisfy (C)$_1$.

Next, suppose that $R = R(q, r, s)$ satisfies (C)$_1$. Let $\alpha \in \mathrm{GF}(q^r)\setminus \mathrm{GF}(q)$, and put $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q^s} \end{pmatrix}$ and $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. There exists $f(X)$ in $X^2\mathbf{Z}[X]$ and a positive integer k such that $[x-f(x), a] = [f(x+a), f(x)]_k = 0$. Then, in virtue of Lemma 5 (2), $f(\alpha) \in \mathrm{GF}(q)$. Since $\alpha-f(\alpha) \in \mathrm{GF}(q)$ by $[x-f(x), a] = 0$, we get $\alpha \in \mathrm{GF}(q)$, which is a contradiction. We conclude therefore that R is commutative by Corollary 1.

By similar argument, we can easily see that 2) implies 0).

4) $\Rightarrow$ 0). First, suppose that $\begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}$ satisfies $(C)_4$. For $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, there exist positive integers k, m, n, m' and n' such that $mn = m'n'$ and $[(x^m(x+a)^m)^n, ((x+a)^{m'}x^{m'})^{n'}]_k = 0$. But this is impossible. Similarly, $\begin{pmatrix} 0 & GF(p) \\ 0 & GF(p) \end{pmatrix}$ does not satisfy $(C)_4$.

Next, suppose that $R = R(q, r, s)$ satisfies $(C)_4$. Let α be a generating element of the multiplicative group of $GF(q^r)$, and put $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q^s} \end{pmatrix}$ and $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. There exist positive integers k, m, n, m', n', μ and ν such that $mn = m'n'$, $2mn = (m+m')\mu-(mn-1)\nu$, $x-x^{mn} \in N$ and $[(x^m(x+a)^m)^n, ((x+a)^{m'}x^{m'})^{n'}]_k = 0$. Then $\alpha = \alpha^{mn}$, and $\alpha^{2mn} \in GF(q)$ by Lemma 5(3). (If $\alpha^{m+m'} \in GF(q)$ then $\alpha^{2mn} = \alpha^{(m+m')\mu}(\alpha^{mn-1})^{-\nu} \in GF(q)$.) Hence $\alpha^2 = \alpha^{2mn} \in GF(q)$, which means that $(q^r-1)/(q-1)\,|\,2$. But this is impossible. We conclude therefore that R is commutative by Corollary 1.

By similar argument, we can easily see that 3) implies 0).

The next which includes Theorem 3 of [6] is immediate by Theorem 3 4).

Corollary 3. *Let R be a ring satisfying the identity $(X-X^n)(Y-Y^n) = 0$ $(n > 1)$. If for each $x, y \in R$, either $(xy)^n-(yx)^n \in C$, or $x^ny^n-y^nx^n \in C$ or $(xy)^n-y^nx^n \in C$, then R is commutative.*

Example 1. Let $R = R(q, 2, 1)$ and let $A = N$. Then $x-x^{q^2} \in A$ and $(x(x+a))^{q^2} = ((x+a)^q x^q)^q$ for all $x \in R$ and $a \in A$. This example shows that, in Theorem 3 4), the hypothesis $(m+m', mn-1)\,|\,2mn$ cannot be deleted.

Example 2. Let $R = R(2, 2, 1)$ and let $A = C + N$. Then $(1+2, 1\cdot 2-1)\,|\,2\cdot 1\cdot 2$, $x-x^2 \in A$ and $[(x(x+a))^2, (x+a)^2x^2] = 0$ for all $x \in R$ and $a \in A$. This example shows that, in Theorem 3 4), the hypothesis $x-x^{mn} \in N$ cannot be deleted.

4. Condition (I'-A) and commutativity theorems. In this section, A will denote a non-empty subset of R. In the previous papers ([9], [12]), we considered the following condition :

(I'-A) For each $x \in R$, either $x \in C$ or there exists $f(X)$ in $X^2\mathbf{Z}[X]$ such that $x-f(x) \in A$.

By definition, we can easily see

Lemma 6. *If A is commutative and R satisfies* (I'-A), *then R satisfies* (C) *and $N^* \subseteq A \cup C \subseteq C'$.*

Now, the next is immediate by Lemmas 4 and 6.

Corollary 4. *A ring R is commutative if and only if there exists a commutative subset A of R for which R satisfies* (I'-A) *and* (ii-A)$_1^*$.

If A is a commutative subset of N, the next is a special case of $(C)_4$ by Lemma 6 :

(1-A) For each $x \in R$ and $a \in A$, either $x \in C$ or there exists an integer $n > 1$ such that $x-x^n \in A$ and either $(x(x+a))^n-((x+a)x)^n \in C$, or $x^n(x+a)^n-(x+a)^nx^n \in C$ or $(x(x+a))^n-(x+a)^nx^n \in C$.

Theorems 1, 2 and 3 of [13] are now included in the following

Corollary 5. *A ring R is commutative if and only if there exists a commutative subset A of N for which R satisfies* (1-A).

Next, we consider the following conditions which are stronger than (I'-A) :

(2-A) For each $x \in R$ and $a \in A$, either $x \in C$ or there exist positive integers k, m and n such that $mn > 1$, $x-x^{mn} \in A$ and $[(x^m(x+a)^m)^n, ((x+a)^mx^m)^n]_k = 0$.

(3-A) For each $x \in R$, either $x \in C$ or there exists an integer $n > 1$ such that

1) $x-x^n \in A$,
2) $[x^ny^n-(xy)^n, x] = [y^nx^n-(yx)^n, x] = 0$ for all $y \in R$,
3) for all $a \in A$, $(n-1)[a, x] = 0$ implies $[a, x] = 0$.

(4-A) For each $x \in R$, either $x \in C$ or there exists an integer $n > 1$ such that $x-x^n \in A$ and $[(xy)^{n+1}-x^{n+1}y^{n+1}, x] = [(yx)^{n+1}-y^{n+1}x^{n+1}, x] = 0$ for all $y \in R$.

Theorem 4. *A ring R is commutative if and only if there exists a commutative subset A of R for which R satisfies* (2-A^+), *where A^+ is the additive subsemigroup of R generated by A.*

In advance of proving Theorem 4, we state next

Lemma 7. *Let $L \supsetneq K$ be a field extension. Suppose that for each $x \in L$ there exists an integer $n > 1$ such that both $x - x^n$ and x^{2n} belong to K. If K is not of characteristic 2 (in particular, if L/K is separable), then $L = \mathrm{GF}(9)$. Conversely, for each $x \in \mathrm{GF}(9)$, there exists an integer $n > 1$ such that both $x - x^n$ and x^{2n} belong to $\mathrm{GF}(3)$.*

Proof. Let x be an arbitrary element of $L \backslash K$. Then there exists an integer $n > 1$ such that both $x - x^n$ and x^{2n} belong to K. (If K is of characteristic 2, then we can easily see that $x^2 \in K$, which implies that L/K is inseparable.) Let a be an arbitrary non-zero element of K. Then $ax^n - (ax^n)^m \in K$ for some $m > 1$. Since $x^n \notin K$ and $x^{2n} \in K$, m has to be odd, and $ax^n - (ax^n)^m = (1 - (ax^n)^{m-1})ax^n \in K \cap Kx^n = 0$. Hence $(ax^n)^{m-1} = 1$. In particular, $x^{nm'} = 1$ for some positive integer m', and therefore $a^{(m-1)m'} = 1$. Hence K is periodic. Let Φ be the prime field of K, and let $q = 2^e r - 1$ be the order of $K \cap \Phi(x)$, where $e > 0$ and r is odd. Noting that $(x - (x - x^n))^2 = x^{2n}$ and both $x - x^n$ and x^{2n} belong to K, we see that $\Phi(x)$ is a quadratic extension of $K \cap \Phi(x)$. Since the multiplicative group of $\Phi(x)$ is the cyclic group of order $q^2 - 1$, it contains an element y of order $r(q-1)$. Choose an integer $l > 1$ such that $y - y^l$ and y^{2l} are in K. Then $y^{2l} \in K$ implies that $r(q-1) \mid 2l(q-1)$. But r is odd, and so we get $r \mid l$. This means that $y^l \in K$, and hence $y \in K$. We obtain therefore $r = 1$ and $q = 2^e - 1$. Now, we shall show that $q = 3$, which will complete the proof. Suppose, to the contrary, that $e > 2$. Then, the multiplicative group of $\Phi(x)$ contains an element z of order 16. Obviously, z is not in K. Again by hypothesis, there exists an integer $k > 1$ such that both $z - z^k$ and z^{2k} belong to K. Since $(z^{2k})^8 = 1$ and $(q-1)/2$ is odd, $z^{2k} \in K \cap \Phi(x)$ implies that $(z^{2k})^2 = 1$. If $z^{2k} = 1$ then we have $z^k = \pm 1$, which forces a contradiction $z \in K$. Hence z^{2k} has to be -1. Putting $b = z - z^k$, we have

$$
\begin{aligned}
z^2 &= (z^k + b)^2 = 2bz^k + b^2 - 1, \\
z^4 &= (z^2)^2 = 4b(b^2-1)z^k + (b^2-1)^2 - 4b^2, \\
z^8 &= (z^4)^2 \\
&= 8b(b^2-1)((b^2-1)^2 - 4b^2)z^k + ((b^2-1)^2 - 4b^2)^2 - 16b^2(b^2-1)^2.
\end{aligned}
$$

Since $z^4 \notin K$ and $z^8 = -1$, we get $(b^2-1)^2 = 4b^2$ and $16b^2(b^2-1)^2 = 1$. Then $(8b^2)^2 = 16b^2 4b^2 = 16b^2(b^2-1)^2 = 1$, and hence $8b^2 = \pm 1$. Furthermore, $(8b^2 - 8)^2 = 64(b^2-1)^2 = 64 \cdot 4b^2 = 32 \cdot 8b^2$. In this equation, $8b^2 =$

± 1 implies that either $17=0$ or $113=0$. But, in either case, we can easily see that $q=4s+1$ with some positive integer s, which contradicts $q=2^e-1$. We have thus seen that $e=2$.

Conversely, let x be an arbitrary element of $\mathrm{GF}(9)\backslash\mathrm{GF}(3)$. If $x^2+1=0$ then $x-x^5=0$ and $x^{10}=-1$. If $x^2-x-1=0$ then $x-x^2=-1$ and $x^4=-1$. Finally, if $x^2+x-1=0$ then $x-x^6=1$ and $x^{12}=-1$.

Proof of Theorem 4. Only if part is clear. In order to prove if part, by Corollary 1 and Lemma 5, it suffices to show that $R=R(q, r, s)$ does not satisfy $(2\text{-}A)$, where A is an additively closed commutative subset of R. Since $N^*\subseteq A$ by Lemma 6, the commutativity of A implies that $A\subseteq C+N$. Suppose, to the contrary, that R satisfies $(2\text{-}A)$. Let α be an arbitrary element of $\mathrm{GF}(q^r)$, and put $x=\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{q^s}\end{pmatrix}$. Since $a=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$ is in A, there exist positive integers k, m and n such that $x-x^{mn}\in A$ and $[(x^m(x+a)^m)^n, ((x+a)^m x^m)^n]_k=0$. Then, in view of Lemma 5 (3), $\alpha^{2mn}\in\mathrm{GF}(q)$. Since $\alpha-\alpha^{mn}\in\mathrm{GF}(q)$ by $x-x^{mn}\in A\subseteq C+N$, Lemma 7 shows that $q=3$ and $r=2$.

Now, let α be a generating element of the multiplicative group of $\mathrm{GF}(9)$. Without loss of generality, we may assume that $\alpha^3-\alpha-1=0$; $\beta=\alpha^2\notin\mathrm{GF}(3)$ and $\beta^2=-1$. Let $x=\begin{pmatrix}\alpha & 0\\ 0 & \alpha^3\end{pmatrix}$. Then, as was shown above, there exist positive integers m, n such that $x-x^{mn}\in A$, $\alpha-\alpha^{mn}\in\mathrm{GF}(3)$ and $\alpha^{2mn}\in\mathrm{GF}(3)$. Since $\alpha^{2mn}=(\alpha-(\alpha-\alpha^{mn}))^2=(\beta-(1+(\alpha-\alpha^{mn})))^2=-1+(1+(\alpha-\alpha^{mn}))^2-2(1+(\alpha-\alpha^{mn}))\beta$, we obtain $-1=\alpha-\alpha^{mn}$ and $-1=x-x^{mn}\in A$. Let $y=\begin{pmatrix}\beta & 0\\ 0 & \beta^3\end{pmatrix}$ and $b=-1+a\in A$. If $y-y^{m'n'}\in A$ for some positive integers m', n', then $\beta-\beta^{m'n'}\in\mathrm{GF}(3)$, and so $m'n'$ has to be odd. But, for any positive integer k' we have

$$\begin{aligned}&[(y^{m'}(y+b)^{m'})^{n'}, ((y+b)^{m'}y^{m'})^{n'}]_{k'}\\&=(\alpha^{9m'n'}-\alpha^{3m'n'})^{k'+1}(\alpha^{6m'}-\alpha^{2m'})(\alpha^{9m'}-\alpha^{3m'})^{-1}(\alpha^2-\alpha^6)^{-1}a\\&\neq 0.\end{aligned}$$

This is a contradiction.

Example 3. Let $R=R(3,2,1)$ and let $A=C\cup N$. Then R satisfies $(2\text{-}A)$. Actually, by Lemma 7, for each $\alpha\in\mathrm{GF}(9)$ there exists an integer $n>1$ such that $\alpha-\alpha^n\in\mathrm{GF}(3)$ and $\alpha^{2n}\in\mathrm{GF}(3)$. Noting that $(\alpha-\alpha^n)^3=$

$\alpha-\alpha^n$ implies $\alpha^n-\alpha^{3n}=\alpha-\alpha^3$, we can easily see that for each $x \in R$ there exists an integer $n>1$ such that $x-x^n \in A$ and $[(x(x+a))^n, ((x+a)x)^n]=0$ for all $a \in A$. We have thus seen that, in Theorem 4, $(2\text{-}A^+)$ cannot be replaced by $(2\text{-}A)$.

Finally, we improve [13, Theorems 4, 5].

Lemma 8. *Suppose that R satisfies $(\text{I}'\text{-}N)$. Let ψ be a homomorphism of R onto R'. If R is normal, then every idempotent e' of R' is in $\psi(C)$.*

Proof. Let $\psi(x)=e'$. If x is not central, then there exists a positive integer k and $g(X)$ in $\boldsymbol{Z}[X]$ such that $x^k=x^{2k}g(x)$. Obviously, $x^kg(x)$ is a central idempotent and $\psi(x^kg(x))=e'\psi(g(x))=\psi(x^{2k}g(x))=\psi(x^k)=e'$.

Theorem 5. *Let R be a normal ring. Then the following conditions are equivalent :*

0) *R is commutative.*

1) *There exists a commutative subset A of N for which R satisfies* $(3\text{-}A)$.

2) *There exists a commutative subset A of N for which R satisfies* $(4\text{-}A)$.

Proof. Obviously, 0) implies 1) and 2).

1) $\Rightarrow$ 0). By Lemma 8, every factorsubring of R is normal. Hence, by Corollary 1, it suffices to show that R has no factorsubring isomorphic to some $R(q, r, s)$. Suppose, to the contrary, that there exists a homomorphism ψ of a subring S of R onto $R'=R(q, r, s)$, where we may assume that $S=R$. Now, let $x'=\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{q^s}\end{pmatrix}$ $(\alpha \notin \mathrm{GF}(q))$ and $a'=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$. Choose $x \in R$, $a \in A$ and $e \in C$ such that $\psi(x)=x'$, $\psi(a)=a'$ and $\psi(e)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ (Lemma 8). There exists an integer $n>1$ satisfying 1), 2), 3) of $(3\text{-}A)$. Then, noting that $N^2 \subseteq C$ by Theorem C, we see that

$$\begin{aligned}&(n-1)[[e^{n-1}a, x^n], x]\\ &= [\{(x(e+a))^n-x^n(e+a)^n\}-\{((e+a)x)^n-(e+a)^nx^n\}, x]\\ &= 0.\end{aligned}$$

Since $[N, R] \subseteq N^*$ by Theorem C and $N^* \subseteq A \cup C$ by Lemma 6, we get $[[e^{n-1}a, x^n], x]=0$, and therefore $[[a', x'^n], x']=0$. Combining this with $[a', x'^n]=[a', x']$, we get $[[a', x'], x']=0$. But this is impossible.

2) $\Rightarrow$ 0). Again by Lemma 8 and Corollary 1, it suffices to show that $R = R(q, r, s)$ cannot satisfy (4-A), A a commutative subset of N. Suppose, to the contrary, that R satisfies (4-A). Then A coincides with N. Let α be a generating element of the multiplicative group of $GF(q^r)$, and put $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q^s} \end{pmatrix}$, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $y = 1+a$. Then there exists an integer $n > 1$ such that $x-x^n \in A$ and $[a_1, x] = [a_2, x] = 0$, where $a_1 = (xy)^{n+1}-x^{n+1}y^{n+1} \in A\,(=N)$ and $a_2 = (yx)^{n+1}-y^{n+1}x^{n+1} \in A$. Noting that $x^2-x^{n+1} = x(x-x^n) \in A$, we obtain $n[[a, x^2], x] = n[[a, x^{n+1}], x] = [a_1-a_2, x] = 0$. Further

$$\begin{aligned}(n+1)[[a, x], x] &= (n+1)[[a, x^n], x] \\ &= [\{(yx)^n-x^ny^n\}-\{(xy)^n-y^nx^n\}, x] \\ &= [x^{-1}a_1y^{-1}-y^{-1}a_2x^{-1}, x] \\ &= [x^{-1}a_1(1-a)-(1-a)a_2x^{-1}, x] \\ &= [x^{-1}(a_1-a_2), x] \\ &= 0.\end{aligned}$$

Combining this with $n[[a, x^2], x] = 0$, we get $[[a, x^2], x] = 0$. But this is impossible.

Lemma 9. *Let R be an s-unital ring. Suppose that for each $x \in R$, either $x \in C$ or there exists an integer $n > 1$ such that $[x^ny^n-(xy)^n, x] = [y^nx^n-(yx)^n, x] = 0$ for all $y \in R$. Then R is normal.*

Proof. Let $e = e^2$ and x be in R, and choose a pseudo identity e' of $\{e, x\}$. If $e'-e$ is central, then $ex-exe = ex(e'-e) = e(e'-e)x = 0$; similarly, $xe-exe = 0$. If $e'-e$ is not central, then there exists an integer $n > 1$ such that

$$-xe+exe = [(e'-e)^n(e+(e'-e)xe)^n-((e'-e)xe)^n, e'-e] = 0,$$

and similarly $ex-exe = 0$. We have thus seen that $ex = xe$ in either case.

Combining Theorem 5 with Lemma 9, we readily obtain

Corollary 6. *Let R be an s-unital ring. Then the following conditions are equivalent :*

0) *R is commutative.*

1) *There exists a commutative subset A of N for which R satisfies (3-A).*

2) *There exists a commutative subset A of N for which R satisfies* (4-A).

REFERENCES

[1] M. CHACRON : A commutativity theorem for rings, Proc. Amer. Math. Soc. 59 (1976), 211−216.

[2] I. N. HERSTEIN : The structure of a certain class of rings, Amer. J. Math. 75 (1953), 864−871.

[3] Y. HIRANO and H. TOMINAGA : Two commutativity theorems for rings, Math. J. Okayama Univ. 20 (1978), 67−72.

[4] Y. HIRANO and H. TOMINAGA : Some commutativity theorems for rings, Hiroshima Math. J. 11 (1981), 457−464.

[5] Y. HIRANO, Y. KOBAYASHI and H. TOMINAGA : Some polynomial identities and commutativity of s-unital rings, Math. J. Okayama Univ. 24 (1983), 7−13.

[6] Y. HIRANO and A. YAQUB : Rings satisfying the identity $(X-X^n)(Y-Y^n)=0$, Math. J. Okayama Univ. 29 (1987), 185−189.

[7] N. JACOBSON : The Theory of Rings, Amer. Math. Soc. Math. Surveys 2, Amer. Math. Soc., New York, 1943.

[8] Y. KOBAYASHI : Rings with commuting n-th powers, Arch. Math. 47 (1986), 215−221.

[9] H. KOMATSU, H. TOMINAGA and A. YAQUB : Structure and commutativity of rings with constraints involving a commutative subset, Hokkaido Math. J. 18 (1989), 355−361.

[10] W. STREB : On commutativity conditions for rings, Math. J. Okayama Univ. 28 (1986), 105−108.

[11] W. STREB : Zur Struktur nichtkommutativer Ringe, Math. J. Okayama Univ. 31 (1989), 135−140.

[12] H. TOMINAGA and A. YAQUB : Some commutativity properties for rings, Math. J. Okayama Univ. 25 (1983), 81−86.

[13] A. YAQUB : Commutativity of rings with conditions on commutators, nilpotent and potent elements, Resultate Math. 14 (1988), 375−381.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY
OKAYAMA, 700 JAPAN

(*Received September 10, 1988*)