

Mathematical Journal of Okayama University

Volume 26, Issue 1

1984

Article 16

JANUARY 1984

Commutativity theorems for rings with a commutative subset or a nil subset

Hisao Tominaga*

Adil Yaqub†

*Okayama University

†University of California

Copyright ©1984 by the authors. *Mathematical Journal of Okayama University* is produced by
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

COMMUTATIVITY THEOREMS FOR RINGS WITH A COMMUTATIVE SUBSET OR A NIL SUBSET

HISAO TOMINAGA and ADIL YAQUB

Throughout, R will represent a ring with center C , and N the set of nilpotent elements in R . As usual, $[x, y]$ will denote the commutator $xy - yx$. Given a subset S of R , we denote by $V_R(S)$ the set of all elements of R which commute with all elements in S . Following [2], R is called *s-unital* if for each x in R , $x \in Rx \cap xR$. As stated in [2], if R is an *s-unital* ring, then for any finite subset F of R there exists an element e in R such that $ex = xe = x$ for all x in F . Such an element e will be called a *pseudo-identity* of F .

Let l be a fixed positive integer, q a fixed integer greater than 1, and E_q the set of elements x in R such that $x^q = x$. Let A be a non-empty subset of R , and A^+ the additive subsemigroup of R generated by A . We consider the following properties :

- (I-A) For each $x \in R$, there exists a polynomial $f(\lambda)$ in $\mathbf{Z}[\lambda]$ such that $x - x^2 f(x) \in A$.
- (II-A)_q If $x, y \in R$ and $x - y \in A$, then either $x^q = y^q$ or x and y both belong to $V_R(A)$.
- (ii-A)_q If $x, y \in R$ and $x - y \in A$, then either $x^q - y^q \in C$ or x and y both belong to $V_R(A)$.
- (ii-A)_q^{*} $[a, x^q] = 0$ for any $a \in A$ and $x \in R$.
- (iii-A)_q For any $x \in R$, either $x \in C$ or $x = x' + x''$ with some $x' \in A$ and $x'' \in E_q$.
- (A)_q If $a, b \in A$ and $q[ka, b] = 0$ for some positive integer k , then $[ka, b] = 0$.
- (A)_q' If $a, b \in A$ and $q[a, b] = 0$, then $[a, b] = 0$.
- (A)_l^{*} If $a \in A$, $x \in R$ and $l[a^k, x] = 0$ for some positive integer k , then $[a^k, x] = 0$.

Our present objective is to prove the following theorems.

Theorem 1. *The following statements are equivalent :*

- 1) R is commutative.
- 2) There exists a commutative subset A for which R satisfies (I-A), (ii-A)_q and (iii-A⁺)_q.
- 2)^{*} There exists a commutative subset A for which R satisfies (I-A),

$(ii-A)_q^*$ and $(iii-A^+)_q$.

3) There exists a commutative subset A of N for which R satisfies $(ii-A)_q$ and $(iii-A^+)_q$.

3)* There exists a commutative subset A of N for which R satisfies $(ii-A)_q^*$ and $(iii-A^+)_q$.

Theorem 2. Let R be an s -unital ring. Then the following statements are equivalent :

1) R is commutative.

2) There exists a subset A for which R satisfies $(I-A)$, $(II-A)_q$, $(iii-A^+)_q$ and $(A)'_q$.

3) There exists a subset A of N for which R satisfies $(ii-A)_q$, $(iii-A)_q$ and $(A)'_q$.

3)* There exists a subset A of N for which R satisfies $(ii-A)_q^*$, $(iii-A)_q$ and $(A)'_q$.

4) R satisfies the polynomial identity $[X^q, Y] = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$ and $(A)'_q$.

5) R satisfies the polynomial identity $(XY)^q - (YX)^q = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$ and $(A)'_q$.

6) R satisfies the polynomial identity $[X^q, Y] - [X, Y^q] = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$ and $(A)'_q$.

7) R satisfies the polynomial identity $[X, (X+Y)^q - Y^q] = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$ and $(A)'_q$.

8) R satisfies the polynomial identity $(XY)^q - X^q Y^q = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$, $(A)'_q$ and $(A)_{q-1}^*$.

9) R satisfies the polynomial identity $[X^q, Y^q] = 0$ and there exists a subset A of N for which R satisfies $(iii-A)_q$ and $(A)_q^*$.

Proof of Theorem 1. Obviously, 1) implies both 2) and 3). Next, the proof of [4, Lemma 1 (3)] shows that $(ii-A)_q$ implies $(ii-A)_q^*$, and therefore 2) and 3) imply 2)* and 3)*, respectively.

2)* \Leftrightarrow 1). Since A is commutative and $A \subseteq V_R(E_q)$, $(iii-A^+)_q$ shows that $A \subseteq V_R(A) \cap V_R(E_q) \subseteq V_R((A^+ + E_q) \cup C) = C$. Hence, by $(I-A)$ and [1, Theorem 19], R is commutative.

3)* \Leftrightarrow 1). As was shown just above, A is a subset of C . We claim next that $N \subseteq C$. Suppose, to the contrary, that there exists $u \in N \setminus C$. Then $u = u' + u''$ with some $u' \in A^+$ and $u'' \in E_q$. As is easily seen, $u'' = u - u' \in E_q \cap N = 0$, and hence $u = u' \in A^+ \subseteq C$, a contradiction. Thus,

N is an ideal of R contained in C . Now, let $x \in R \setminus C$, and $x = x' + x''$ ($x' \in A^+$, $x'' \in E_q$). Then $x^q \equiv x''^q = x'' \equiv x \pmod{N}$. This proves that $x - x^q \in C$ for all $x \in R$. Hence, R is commutative again by [1, Theorem 19].

Proof of Theorem 2. It is clear that 1) implies 2)–9) and 4) does 3)*. Furthermore, [3, Proposition 3] shows that 5) implies 4) and 6) is equivalent to 7). As was claimed in the proof of Theorem 1, (ii- A) $_q$ implies (ii- A) $_q^*$, and hence 3) implies 3)*.

2) \Rightarrow 1). Suppose that there exist $a, b \in A$ such that $ab \neq ba$. Then, by (II- A) $_q$, $a^q = 0$. Let $k (> 1)$ be the least positive integer such that $[a^i, b] = 0$ for all $i \geq k$, and let e be a pseudo-identity of $\{a, b\}$. Then $q[a^{k-1}, b] = [(e + a^{k-1})^q, b] = 0$, since as remarked in the proof of Theorem 1, (II- A) $_q \Leftrightarrow$ (ii- A) $_q \Leftrightarrow$ (ii- A) $_q^*$. In view of (I- A), there exists $f(\lambda) \in \mathbf{Z}[\lambda]$ such that $a^{k-1} - a^{2(k-1)}f(a^{k-1}) \in A$. Then, by (A) $_q$, $q[a^{k-1} - a^{2(k-1)}f(a^{k-1}), b] = 0$ implies that $0 = [a^{k-1} - a^{2(k-1)}f(a^{k-1}), b] = [a^{k-1}, b]$, which contradicts the minimality of k . Hence, A has to be commutative, and therefore R is commutative by Theorem 1.

3)* \Rightarrow 1). Let $u \in N \setminus C$, and $u = u' + u''$ ($u' \in A$, $u'' \in E_q$). Then, noting that $A \subseteq V_R(E_q)$, we can easily see that $u'' = u - u' \in E_q \cap N = 0$; $u = u' \in A$. This proves that $N \subseteq A \cup C$. Suppose now that there exist $a, b \in A$ such that $ab \neq ba$. Let $k (> 1)$ be the least positive integer such that $[a^i, b] = 0$ for all $i \geq k$. Since $N \subseteq A \cup C$, a^{k-1} must belong to A . Let e be a pseudo-identity of $\{a, b\}$. Then $q[a^{k-1}, b] = [(e + a^{k-1})^q, b] = 0$, and so (A) $_q$ gives $[a^{k-1}, b] = 0$, which contradicts the minimality of k . We have thus seen that A is commutative. Hence, R is commutative by Theorem 1.

Combining those above, we see that 1)–5) are all equivalent.

6) \Rightarrow 1). In view of [3, Proposition 3], R satisfies the polynomial identity $[X^q, Y] = 0$ for some positive integer q . It is easy to see that R satisfies (iii- A) $_{q^a}$ and (A) $'_{q^a}$. Hence R is commutative by 4).

8) \Rightarrow 3)*. Let $a \in A$ and $x \in R$. Let e be a pseudo-identity of $\{a, x\}$. If a_0 is the quasi-inverse of a then we can easily see that

$$\begin{aligned} 0 &= (e - a)^q \{ (e - a_0)^q x^q (e - a)^q \} (e - a_0) - x^q (e - a)^{q-1} \\ &= (e - a)^q \{ (e - a_0) x (e - a) \}^q (e - a_0) - x^q (e - a)^{q-1} \\ &= [(e - a)^{q-1}, x^q]. \end{aligned}$$

Choose the minimal positive integer k such that $[a^i, x^q] = 0$ for all $i \geq k$.

Suppose $k > 1$. Then, by the above, $[(e - a^{k-1})^{q-1}, x^q] = 0$. Combining this with $[a^i, x^q] = 0$ for all $i \geq k$, we get $(q-1)[a^{k-1}, x^q] = 0$, and hence $[a^{k-1}, x^q] = 0$ by $(A)_{q-1}^*$. But this contradicts the minimality of k . Thus, $k = 1$, and hence $[a, x^q] = 0$.

9) \Rightarrow 3)*. Let $a \in A$ and $x \in R$. Choose the minimal positive integer k such that $[a^i, x^q] = 0$ for all $i \geq k$. Suppose $k > 1$. Then $0 = [(e + a^{k-1})^q, x^q] = q[a^{k-1}, x^q]$, and hence $[a^{k-1}, x^q] = 0$ by $(A)_q^*$. This contradiction shows that $[a, x^q] = 0$.

Corollary 1. *Let R be an s -unital ring. Then the following statements are equivalent :*

- 1) R is commutative.
- 2) R satisfies the polynomial identity $[X^q, Y] = 0$ and there exists a subset A of N for which R satisfies $(iii-A^+)_q$ and $(A^+)'_q$.
- 3) R satisfies the polynomial identity $(XY)^q - (YX)^q = 0$ and there exists a subset A of N for which R satisfies $(iii-A^+)_q$ and $(A^+)'_q$.
- 4) R satisfies the polynomial identity $[X^q, Y] - [X, Y^q] = 0$ and there exists a subset A of N for which R satisfies $(iii-A^+)_q$ and $(A^+)'_q$.
- 5) R satisfies the polynomial identity $[X, (X+Y)^q - Y^q] = 0$ and there exists a subset A of N for which R satisfies $(iii-A^+)_q$ and $(A^+)'_q$.

Proof. Notice that N forms an ideal provided R satisfies one of the polynomial identities cited in 2)–5) (see, e.g., [3, Proposition 2]).

Corollary 2. *Let R be an s -unital ring. Then the following statements are equivalent :*

- 1) R is commutative.
- 2) R satisfies the polynomial identity $[X^q, Y] = 0$ and there exists a subset A for which R satisfies $(II-A)_q$, $(iii-A)_q$ and $(A)'_q$.
- 3) R satisfies the polynomial identity $(XY)^q - (YX)^q = 0$ and there exists a subset A for which R satisfies $(II-A)_q$, $(iii-A)_q$ and $(A)'_q$.
- 4) R satisfies the polynomial identity $[X^q, Y] - [X, Y^q] = 0$ and there exists a subset A for which R satisfies $(II-A)_q$, $(iii-A)_q$ and $(A)'_q$.
- 5) R satisfies the polynomial identity $[X, (X+Y)^q - Y^q] = 0$ and there exists a subset A for which R satisfies $(II-A)_q$, $(iii-A)_q$ and $(A)'_q$.
- 6) R satisfies the polynomial identity $[X^q, Y^q] = 0$ and there exists a subset A for which R satisfies $(II-A)_q$, $(iii-A)_q$ and $(A)'_q$.

Proof. Obviously 1) \Rightarrow 2)–6) and 2) \Rightarrow 6).ⁿ Furthermore,

[3, Proposition 3] shows that 3) implies 2) and 4) is equivalent to 5).

6) \Rightarrow 1). Suppose A is not commutative. Let $a \in A$ and $b \in A \setminus V_R(A)$. Then, by $(\text{II-}A)_q$, $a^q = 0$, which tells us that $A \subseteq N$. As was remarked in the proof of Theorem 2, $(\text{II-}A)_q$ implies $(\text{ii-}A)_q^*$. Hence the statement 3)* of Theorem 2 holds, and therefore R is commutative. This contradiction shows that A is commutative. Suppose now that there exist $x, y \in R$ such that $xy \neq yx$. Then, by $(\text{iii-}A)_q$, $x = x' + x''$ and $y = y' + y''$ with some $x', y' \in A$ and $x'', y'' \in E_q$. Since $[x'', y''] = 0$ and $A \subseteq V_R(E_q \cup A)$, we see that $[x, y] = 0$, a contradiction. Hence R is commutative.

5) \Rightarrow 1). By [3, Proposition 3 (ii)], R satisfies the polynomial identity $[X^{q^\alpha}, Y^{q^\alpha}] = 0$ for some positive integer α . It is easy to see that R satisfies $(\text{II-}A)_{q^\alpha}$, $(\text{iii-}A)_{q^\alpha}$ and $(A)_{q^\alpha}$. Hence R is commutative, by 6).

We conclude this paper with the following examples :

$$(1) \text{ Let } R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in \text{GF}(3) \right\}, A = N = R, \text{ and } q =$$

4. This example shows that Theorem 2 need not be true if R is not s -unital.

$$(2) \text{ Let } R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \mid a, b, c, d \in \text{GF}(3) \right\}, A = N, \text{ and } q = 3.$$

This example shows that we cannot drop the hypothesis that A is commutative in Theorem 1 3) and that $(A)_q$ cannot be deleted in Theorem 2 3).

(3) Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \text{GF}(2) \right\}$, $A = N$, and $q = 3$. This example shows that $(\text{ii-}A)_q$ cannot be deleted in Theorem 1 3) and Theorem 2 3).

$$(4) \text{ Let } R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a^2 & 0 \\ 0 & 0 & a \end{pmatrix} \mid a, b, c \in \text{GF}(4) \right\}, A = N, \text{ and } q = 6.$$

This example shows that $(\text{iii-}A)_q$ cannot be deleted in Theorem 2 3).

(5) Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & a^2 \end{pmatrix} \mid a, b \in \text{GF}(4) \right\}$. Then $C = \{0, 1\}$, $E_7 = \left\{ \begin{pmatrix} a & b \\ 0 & a^2 \end{pmatrix} \mid a \neq 0 \right\} \cup \{0\}$, and $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = 1 + \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ for any b ; hence R satisfies $(\text{II-C})_7$, $(\text{iii-C})_7$ and $(C)_7$. This example shows that the hypothesis that $A \subseteq N$ cannot be deleted in Theorem 1 3) and Theorem 2 3).

REFERENCES

- [1] I.N. HERSTEIN : The structure of a certain class of rings, *Amer. J. Math.* **75** (1953), 864 – 871.
- [2] Y. HIRANO, M. HONGAN and H. TOMINAGA : Commutativity theorems for certain rings, *Math. J. Okayama Univ.* **22** (1980), 65 – 72.
- [3] Y. HIRANO, Y. KOBAYASHI and H. TOMINAGA : Some polynomial identities and commutativity of s -unital rings, *Math. J. Okayama Univ.* **24** (1982), 7 – 13.
- [4] H. TOMINAGA and A. YAQUB : Some commutativity properties for rings, *Math. J. Okayama Univ.* **25** (1983), 81 – 86.

OKAYAMA UNIVERSITY, OKAYAMA, JAPAN
UNIVERSITY OF CALIFORNIA, SANTA BARBARA, U.S.A.

(Received October 12, 1983)