Hokkaido Mathematical Journal Vol. 18 (1989) p. 355-361

Structure and commutativity of rings with constraints involving a commutative subset

Dedicated to Professor Tosiro Tsuzuku on his 60th birthday

Hiroaki KOMATSU, Hisao TOMINAGA and Adil YAQUB

(Received November 27, 1987, Revised January 26, 1988)

Throughout, R will represent a ring with center C, N the set of nilpotent elements in R, N^* the subset of N consisting of all x with $x^2=0$. Given a positive integer n, we set $E_n=\{x\in R|x^n=x\}$; in particular, $E=E_2$. For $x, y\in R$, define extended commutators $[x, y]_k$ as follows: let $[x, y]_1$ be the usual commutator $[x, y]=xy-yx$, and proceed inductively $[x, y]_k=[[x, y]_{k-1}, y]$.

A ring R is called *nearly commutative* if R has no factorsubrings isomorphic to $M_\sigma(K)=\{\begin{pmatrix}\alpha & \beta\\ 0 & \sigma(\alpha)\end{pmatrix}|\alpha, \beta\in K\}$, where K is a finite field and σ is a non-trivial automorphism of K. Needless to say, every commutative ring is nearly commutative; every subring and every homomorphic image of a nearly commutative ring are nearly commutative. 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.

Now, let A be a non-empty subset of R, and l a positive integer. We consider the following conditions:

- (I′-A) For each $x\in R$, either $x\in C$ or there exists a polynomial $f(t)$ in $\boldsymbol{Z}[t]$ such that $x-x^2f(x)\in A$.
- (II′-A) If $x, y\in R$ and $x-y\in A$, then either $x^m=y^m$ with some positive integer m or both x and y belong to the centralizer $C_R(A)$ of A in R.
- (II-A)$_l$ If $x, y\in R$ and $x-y\in A$, then either $x^l=y^l$ or x and y both belong to $C_R(A)$.
- (ii-A)′ For each $x\in R$ and $a\in A$, there exists a positive integer m, depending on x and a, such that $[a, x^m]=0$.
- (ii-A)$'_l$ $[a, x^l]=0$ for all $x\in R$ and $a\in A$.
- (ii-A)* For each $x\in R$ and $a\in A$, there exist positive integers k and m, each depending on x and a, such that $[a, x^m]_k=0$.

(ii-A)$^*_{(l)}$ For each $x\in R$ and $a\in A$, there exist positive integers k and m, each depending on x and a, such that $(m, l)=1$ and $[a, x^m]_k=0$.

(jj-A)* For each $x\in R$ and $a\in A$, there exist positive integers k and m, each depending on x and a, such that $[(x+a)^m, x^m]_k=0$.

(jj-A)$^*_l$ For each $x\in R$ and $a\in A$, there exists a positive integer k, depending on x and a, such that $[(x+a)^l, x^l]_k=0$.

(III-A)* For each $x\in R$ and $a\in A$, there exist positive integers k, m and n, each depending on x and a, such that $(m, n)=1$ and $[a, x^m]_k=[a, x^n]_k=0$.

(III-A)$^\#$ For each $x\in R$ and $a\in A$, there exist positive integers k and m, each depending on x and a, 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 k, m and n, each depending on x and a, such that $(m, n)=1$ and $[(x+a)^m, x^m]_k=[(x+a)^n, x^n]_k=0$.

$(A)'_l$ If $a, b\in A$ and $l[a, b]=0$, then $[a, b]=0$.

$(A)^*_l$ If $x\in R$, $a\in A$ and $l[a, x]=0$, then $[a, x]=0$.

Our present objective is to prove the following commutativity theorem, which improves several early results obtained in [3, 4, 5 and 6]. (Note that the conditions (ii-A)$'_l$ and (III-A)* are denoted as (ii-A)$^*_l$ and (III*-A) in [6] and [3], respectively.)

THEOREM 1. *The following conditions are equivalent:*

1) *R is commutative.*

2) *R is nearly commutative and there exists a commutative subset A of R for which R satisfies* (I$'$-A) *and* (II$'$-A).

3) *There exists a commutative subset A of R for which R satisfies* (I$'$-A), (II$'$-A) *and* (III-A)*.

4) *There exists a commutative subset A of R for which R satisfies* (I$'$-A), (II$'$-A) *and* (III-A)$^\#$.

5) *There exists a commutative subset A of R for which R satisfies* (I$'$-A), (II$'$-A) *and* (JJJ-A)*.

6) *There exists a commutative subset A of R and a positive integer n for which R satisfies* (I$'$-A), (II$'$-A), (jj-A)$^*_n$ *and* $(A)^*_{n!}$.

7) *There exists a commutative subset A of N for which R satisfies* (I$'$-A) *and* (III-A)*.

8) *There exists a commutative subset A of N for which R satisfies* (I$'$-A) *and* (III-A)$^\#$.

9) *There exists a commutative subset A of N for which R satisfies* (I$'$-A) *and* (JJJ-A)*.

10) *There exists a commutative subset A of N and a positive integer n for which R satisfies* (I$'$-A), (jj-A)$^*_n$ *and* $(A)^*_{n!}$.

In preparation for proving our theorem, we state the following lemmas.

LEMMA 1. (1) *If R satisfies* (I$'$-C), *then R is commutative.*

(2) *If R satisfies* (I$'$-A), *then $N \subseteq A^+ + C$ and $N^* \subseteq A \cup C$, where A^+ is the additive subsemigroup of R generated by A.*

(3) *Suppose R satisfies* (I$'$-A). *If R satisfies one of the conditions* (II$'$-A), (ii-A)* *and* (jj-A)*, *then R is normal, that is, $E \subseteq C$.*

(4) *If A is commutative and R satisfies* (I$'$-A), *then N is a commutative nil ideal containing the commutator ideal of R and is contained in $C_R(A)$, and therefore $N[A, R]=[A, R]N=0$ and $[A, R] \subseteq A \cup C$.*

(5) *Let R be a subdirectly irreducible ring. If A is a commutative subset of R (resp. N) for which R satisfies* (I$'$-A) *and* (II$'$-A) (*resp.* (I$'$-A) *and* (ii-A)* (*or* (jj-A)*)), *and x is an element in $R \backslash C_R(A)$, then x is invertible and $\langle x \rangle$ is a finite local ring.*

(6) *If A is a commutative subset of R (resp. N) for which R satisfies* (I$'$-A), (II$'$-A) *and* (jj-A)$^*_n$ (*resp.* (I$'$-A) *and* (jj-A)$^*_n$), *then R satisfies* (ii-A)$'_n$.

(7) *If A is a commutative subset of R (resp. N) for which R satisfies* (I$'$-A), (II$'$-A) *and* (JJJ-A)* (*resp.* (I$'$-A) *and* (JJJ-A)*), *then R satisfies* (III-A)*.

PROOF. (1) This is a well-known theorem of Herstein (see [1]).

(2) See [4, Lemma 1 (2)].

(3) See, e.g., the proofs of [4, Lemma 1 (4)] and [3, Lemma (4)].

(4) See [4, Lemma 1 (5)].

(5) By (3), R is normal. Choose $a \in A$ such that $[a, x] \neq 0$. By (I$'$-A) and (II$'$-A) (resp. (I$'$-A) and $A \subseteq N$), $x^m = x^{2m} f(x)$ with some $f(t) \in \boldsymbol{Z}[t]$ and $m \geq 1$. Since N is contained in $C_R(A)$ by (4), x is not in N, and so $x^m f(x)$ is a non-zero central idempotent. Hence we see that $x^m f(x)=1$ and $x^{-1} \in \langle x \rangle$. Replacing x by x^{-1}, we get $x \in \langle x^{-1} \rangle$, and so $g(x)=0$ with some monic polynomial $g(t)$ in $\boldsymbol{Z}[t]$. This implies that the additive group of $\langle x \rangle$ is finitely generated. Since a cannot commute with both $2x$ and $3x$, there exists an integer $h>1$ such that $[a, hx] \neq 0$. Then, by the above observation, we get $h^{-1}=(hx)^{-1}x \in \langle hx \rangle x \subseteq \langle x \rangle$. Noting that the additive group of $\langle x \rangle$ is Noetherian, we can easily see that $h^{-s}(\boldsymbol{Z}\cdot 1) = h^{-(s+1)}(\boldsymbol{Z}\cdot 1)$ with some positive integer s. Hence $h\boldsymbol{Z}\cdot 1 = \boldsymbol{Z}\cdot 1$, which implies that $\langle x \rangle$ is a finite local ring.

(6) Let $x\in R$ and $a\in A$. By (4), $[A, R]^2=0$ and $[A, R]\subseteq A\cup C$. Hence, by (jj-A)$_n^*$, there exists a positive integer k such that

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

Now, in order to see that $[a, x^n]=0$, we may assume that R is subdirectly irreducible. Suppose, to the contrary, that $[a, x^n]\neq 0$. Then, by (5), $\langle\bar{x}\rangle=\mathrm{GF}(q)$ with some $q>1$, where $\bar{x}=x+N$. Since both qx and $x^{nq}-x^n$ are in N and $[a, x^n]_{k-1}\in A\cup C$ (by (4)), $[[[a, x^n]_{k-1}, x^n], x^n]=[a, x^n]_{k+1}=0$ together with (4) implies that

$$[a, x^n]_k=[[a, x^n]_{k-1}, x^n]=[[a, x^n]_{k-1}, x^{nq}]=qx^{n(q-1)}[a, x^n]_k=0.$$

Repeating the same procedure, we obtain eventually a contradiction $[a, x^n]=0$.

(7) By making use of the same argument as in the proof of (6), we can easily see that for each $x\in R$ and $a\in A$, there exist positive integers m, n such that $(m, n)=1$ and $[a, x^m]=[a, x^n]=0$; in particular, R satisfies (III-A)*.

LEMMA 2. *Let R be a non-commutative, subdirectly irreducible ring. Let A be a commutative subset of R (resp. N) for which R satisfies* (I′-A) *and* (II′-A) *(resp.* (I′-A) *and* (ii-A)*). *If $R=\langle a, x\rangle$ with some $x\in R$ and $a\in A$, then there exists a finite field K with a non-trivial automorphism σ such that $M_\sigma(K)$ is homomorphic to a subring of R which meets A.*

PROOF. Let $u=[a, x](\neq 0)$. Then x is invertible and $\langle x\rangle$ is a finite local ring with radical $M=\langle x\rangle\cap N$ nilpotent (Lemma 1 (5)). According to Lemma 1 (4), N is a commutative nil ideal containing the commutator ideal of R with $[A, N]=0$, $M\subseteq C$, $\{(u)\}^2=0$, and $M\cdot(u)=0$. Obviously, M is an ideal of $S=\langle x, u\rangle=\langle x\rangle+\langle x\rangle u\langle x\rangle$. Let $K=\langle x\rangle/M\simeq\mathrm{GF}(q)$, where $q=p^e$ (p a prime and $e>0$). Then $\bar{S}=S/M=K\oplus K\bar{u}K$. We claim that $[\bar{u}, \bar{x}]\neq 0$. Actually, if $[\bar{u}, \bar{x}]=0$, then $[u, x]\in M\subseteq C$. Since both qx and x^q-x are in $M(\subseteq C)$, we see that $[u, x]=[u, x^q]=qx^{q-1}[u, x]\in M\cdot(u)=0$, and so $u=[a, x]=[a, x^q]=qx^{q-1}[a, x]\in M\cdot(u)=0$. This is a contradiction. Now, as is well-known, $K\otimes_{\mathrm{GF}(p)}K$ is the direct sum of e fields isomorphic to K. This enables us to see that $K\bar{u}K=(K\otimes_{\mathrm{GF}(p)}K)\bar{u}=K\bar{u}_1\oplus\cdots\oplus K\bar{u}_{e'}$, where $K\bar{u}_i=\bar{u}_iK$ $(1\leq i\leq e'\leq e)$. Since $[\bar{u}, \bar{x}]\neq 0$, we may assume that $[\bar{u}_1, \bar{x}]\neq 0$, and therefore $u_1\in A$ (Lemma 1 (2)). Then there exists a non-trivial automorphism σ of K such that the subring $K\oplus K\bar{u}_1$ of $\bar{S}$ is isomorphic to $M_\sigma(K)$.

LEMMA 3. *Let $R=M_\sigma(K)$, where K is a finite field with a non-trivial automorphism σ. Let A be a subset of R for which R satisfies* $(\mathrm{I}'\text{-}A)$. *Then R satisfies neither* $(\mathrm{III}\text{-}A)^*$ *nor* $(\mathrm{III}\text{-}A)^\#$.

PROOF. Choose $\gamma\in K$ with $\sigma(\gamma)\neq\gamma$, and put $x=\begin{pmatrix}\gamma & 0\\ 0 & \sigma(\gamma)\end{pmatrix}$, $a=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$. Since $[a, x]\neq 0$ and $a^2=0$, a belongs to A, by Lemma 1 (2). First, suppose that R satisfies $(\mathrm{III}\text{-}A)^*$. Then there exist positive integers m, n and k such that $(m, n)=1$ and $[a, x^m]_k=0=[a, x^n]_k$. Then one can easily see that $[a, x^m]=0=[a, x^n]$. Since $(m, n)=1$ and x is invertible, this forces a contradiction $[a, x]=0$. Next, suppose that R satisfies $(\mathrm{III}\text{-}A)^\#$. Then we can easily see that there exists a positive integer m such that $[a, x^m]=0$ and $x^m=x$, which forces again a contradiction $[a, x]=0$.

We are now ready to complete the proof of Theorem 1.

PROOF OF THEOREM 1. Obviously, 1) implies 2)—10).

2)$\Rightarrow$1). According to Lemma 1 (1), it suffices to show that $A\subseteq C$. Suppose, to the contrary, that $[a, x]\neq 0$ for some $x\in R$ and $a\in A$. Choose an ideal I of $\langle a, x\rangle$ which is maximal with respect to excluding $[a, x]$. Then $S^*=\langle a, x\rangle/I$ is a subdirectly irreducible ring whose heart is $([a^*, x^*])$, where $x^*=x+I$. Obviously, S^* is nearly commutative and satisfies $(\mathrm{I}'\text{-}B^*)$ and $(\mathrm{II}'\text{-}B^*)$, where $B=A\cap\langle a, x\rangle$. But this contradicts Lemma 2.

3) (resp. 7))$\Rightarrow$1). Again, suppose that $[a, x]\neq 0$ for some $x\in R$ and $a\in A$, and consider the same S^* as in the proof of 2)$\Rightarrow$1). Then, by Lemma 2, there exists a finite field K with a non-trivial automorphism σ such that $M_\sigma(K)$ is homomorphic to a subring of S^* which meets B^*. Obviously, $M_\sigma(K)$ satisfies $(\mathrm{I}'\text{-}U)$ and $(\mathrm{III}\text{-}U)^*$ for some subset U. But this contradicts Lemma 3. We have thus seen that $A\subseteq C$. Hence R is commutative, by Lemma 1 (1).

4) (resp. 8))$\Rightarrow$1). The proof is quite similar to the above.

5) (resp. 9))$\Rightarrow$3) (resp. 7)). By Lemma 1 (7).

6) (resp. 10))$\Rightarrow$1). Let σ be a homomorphism of R onto a subdirectly irreducible ring R'. Then R' satisfies $(\mathrm{I}'\text{-}\sigma(A))$ and $(\mathrm{jj}\text{-}\sigma(A))_n^*$. We claim that for each $x'\in R'$ and $a'\in\sigma(A)$

$$\textstyle\sum_{j=1}^{n-1} i^j\binom{n}{j}[a', x'^j]=0 \quad (i=1, 2, \dots, n-1).$$

Actually, in case R' is commutative, there is nothing to prove. If R' is not commutative then R' has an identity element $1'$ and satisfies $(\mathrm{ii}\text{-}\sigma(A))'_n$ (Lemma 1 (1), (5) and (6)), and therefore

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

We have thus seen that for each $x\in R$ and $a\in A$

$$in[a, x]+i^2\binom{n}{2}[a, x^2]+\dots+i^{n-1}n[a, x^{n-1}]=0 \quad (i=1, 2, \dots, n-1),$$

and the usual Vandermonde determinant argument shows, in view of $(A)^*_{n!}$, that $[a, x]=0$. Hence $A\subseteq C$, and R is commutative by Lemma 1 (1).

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

1) *R is commutative.*

2) *There exists a subset A of R and a positive integer n for which R satisfies* (I$'$-A), (II-A)$_n$, (ii-A)$^*_{(n)}$ *and* $(A)'_n$.

3) *There exists a subset A of N and a positive integer n for which R satisfies* (I$'$-A), (ii-A)$'_n$, (ii-A)$^*_{(n)}$ *and* $(A)'_n$.

PROOF. Obviously, 1) implies 2) and 3).

2) (resp. 3))$\Rightarrow$1). By [4, Lemma 1 (3)], (II-A)$_n$ implies (ii-A)$'_n$. Hence, in view of Theorem 1, it suffices to show that if R satisfies (I$'$-A), (II-A)$_n$ (resp. (ii-A)$'_n$) and $(A)'_n$ then A is commutative. Suppose now that there exist $a, b\in A$ such that $[a, b]\neq 0$. Then, by (II-A)$_n$ (resp. $A\subseteq N$), a is nilpotent. 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 $n[a^{k-1}, b]=[(e+a^{k-1})^n, b]=0$, by (ii-$A$)$'_n$. According to (I$'$-$A$), there exists $f(t)\in \boldsymbol{Z}[t]$ such that

$$a^{k-1}-a^{2(k-1)}f(a^{k-1})\in A.$$

Then $n[a^{k-1}-a^{2(k-1)}f(a^{k-1}), b]=0$, which together with $(A)'_n$ implies that

$$[a^{k-1}, b]=[a^{k-1}-a^{2(k-1)}f(a^{k-1}), b]=0.$$

But this contradicts the minimality of k. Hence A has to be commutative.

REMARK 1. Let $R=\left\{\begin{pmatrix} a & b & c\\ 0 & a^2 & 0\\ 0 & 0 & a\end{pmatrix} \middle|\, a, b, c\in \mathrm{GF}(4)\right\}$. Obviously, N is commutative and R satisfies (I$'$-N), (jj-N)$^*_3$ and $(N)^*_3$. But R is not commutative. This shows that, in the statement 10) in Theorem 1, $(A)^*_{n!}$ cannot be replaced by $(A)^*_n$.

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] H. TOMINAGA: A commutativity theorem for rings with constraints involving a commutative subset, Math. Japonica 33 (1988), 809-811.

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

[5] H. TOMINAGA and A. YAQUB: Some commutativity properties for rings. II, Math. J. Okayama Univ. 25 (1983), 173-179.

[6] H. TOMINAGA and A. YAQUB: Commutativity theorems for rings with a commutative subset or a nil subset, Math. J. Okayama Univ. 26 (1984), 119-124.

Okayama University
Okayama University
University of California