Math. J. Okayama Univ. **39** (1997), 45–56

COMMUTATIVITY OF RINGS WITH POWERS COMMUTING ON SUBSETS

HIROAKI KOMATSU

Throughout this paper R will represent a ring with an identity element 1, and the commutator ideal of R will be denoted by $D(R)$. As usual, for x, $y \in R$, we shall write $[x,y] = xy - yx$.

In [5], the author and H. Tominaga proved the following: If, for each x, $y \in R$, there exist relatively prime positive integers m, n such that $[x^m, y^m] = 0 = [x^n, y^n]$, then R is commutative. In [1], H. E. Bell, M. Janjić and E. Psomopoulos established some related commutativity theorems with the commutativity of powers assumed only for elements of some proper subset of R.

The purpose of this paper is to generalize the results of [1]. For example, Theorem 4.3 contains the following: Let A be a proper left ideal of R. Suppose that, for each x, y, $z \in R \backslash A$, there exist relatively prime positive integers m, n such that $[s^k, t^k] = 0$ for all s, $t \in \{x, y, z\}$ and $k \in \{m, n\}$. Then R is commutative.

1. Preliminaries.

A ring R with 1 is called a *unitary ring*, a subring of R containing 1 of R is called a *unitary subring* of R, and a ring homomorphic image of a unitary subring of R is called a *unitary factorsubring* of R.

If R contains the minimum nonzero ideal I, we shall call I the *heart* of R. For $X \subseteq R$, we shall denote by $\langle X \rangle$ the subring of R generated by X.

The next theorem improves [6, Satz] and plays a central role in this paper.

Theorem 1.1. *Let R be a unitary ring. If R is not commutative, then there exists a unitary factorsubring of R which is of type* (i), (ii), (iii), (iv), *or* (v):

(i) $\begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$, *where p is a prime number.*

(ii) $\mathrm{M}_\sigma(K) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} \,\middle|\, \alpha,\ \beta \in K \right\}$, *where K is a finite field with a nontrivial automorphism σ.*

(iii) *A noncommutative division ring.*

(iv) *A domain generated by* 1 *and a simple radical subring.*

(v) *A finite ring $S = \langle 1, x, y \rangle$ such that $D(S)$ is the heart of S and $\langle x, y \rangle$ is nilpotent.*

Proof. [6, Satz] states that there exists a unitary factorsubring of R which is of type (i), (ii), (iii), (iv), (v) or (vi), where

(vi) A ring $S = \langle 1, x, y \rangle$ such that $D(S)$ is the heart of S, $\langle x, y \rangle D(S) = D(S) \langle x, y \rangle = 0$ and the set of all nilpotent elements of $\langle x, y \rangle$ is a commutative ideal of S.

However, by [4, Proposition 2], a ring of type (vi) does not exist.

Remark 1.2. Let R be a ring of type (v), i.e., $R = \langle 1, x, y \rangle$ is a finite ring such that $D(R)$ is the heart of R and $T = \langle x, y \rangle$ is nilpotent. We shall show that

(a) the characteristic of R is a power of a prime number, and

(b) $TD(R) = D(R)T = 0$.

Since R has the heart, R is directly indecomposable, which implies (a). Since T is a nilpotent ideal of R, $TD(R)$ is an ideal properly contained in $D(R)$. Hence we have $TD(R) = 0$; similarly $D(R)T = 0$.

2. *P*-subset. We shall denote by $\mathbf{W}$ the set of all words in X, Y, namely products of factors each of which is X or Y (together with 1). A subset A of R is called a *P-subset* of R if, for each x, $y \in A$, there exist $w_1, \ldots, w_r \in \mathbf{W}$ and positive integers $n_1, \ldots, n_r$ with $(n_1, \ldots, n_r) = 1$ such that either $w_i(x,y)[x^{n_i}, y^{n_i}] = 0$ $(i = 1, \ldots, r)$ or $w_i(x,y)\{(xy)^{n_i} - (yx)^{n_i}\} = 0$ $(i = 1, \ldots, r)$. We assume that an empty set is a P-subset.

Our first result is the following

Theorem 2.1. *Let R be a unitary ring. If R is a union of two P-subsets, then R is commutative.*

In preparation for the proof, we need some lemmas.

Lemma 2.2. *Let* $R = \begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$, *where* p *is a prime number. If* $\alpha \neq \beta \in \mathrm{GF}(p)$, *then neither*

$$\left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \beta \\ 0 & 0 \end{pmatrix} \right\} \text{ nor } \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

are P*-subset.*

Proof. This is obvious.

Lemma 2.3. *Let* $R = \mathrm{M}_\sigma(K)$, *where* K *is a finite field with a nontrivial automorphism* σ. *Put* $x = \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix}$ *and* $y = \begin{pmatrix} \alpha & \gamma \\ 0 & \sigma(\alpha) \end{pmatrix}$, *where* α, β, $\gamma \in K$ *such that* $\sigma(\alpha) \neq \alpha$ *and* $\beta \neq \gamma$. *Then* $\{x, y\}$ *is not a* P*-subset.*

Proof. We can calculate

$$[x^n, y^n] = \left(\sigma(\alpha^n) - \alpha^n\right) \frac{\beta - \gamma}{\sigma(\alpha) - \alpha} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$(xy)^n - (yx)^n = \begin{cases} \left(\sigma(\alpha^{2n}) - \alpha^{2n}\right) \frac{(\sigma(\alpha)-\alpha)(\beta-\gamma)}{\sigma(\alpha^2)-\alpha^2} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & \text{if } \sigma(\alpha^2) \neq \alpha^2 \\ n\alpha^{2(n-1)}(\sigma(\alpha) - \alpha)(\beta - \gamma) \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & \text{if } \sigma(\alpha^2) = \alpha^2. \end{cases}$$

Since x and y are invertible, we get the assertion.

As usual, an element x in R is said to be regular if x is not a divisor of zero.

Lemma 2.4. *Let* x *and* y *be regular elements in* R. *If* $\{x, y\}$ *is a* P*-subset of* R, *then there exists a positive integer* n *such that* $[x^n, y] = 0$.

Proof. There exist positive integers $n_1, \ldots, n_r$ with $(n_1, \ldots, n_r) = 1$ such that either (1) $[x^{n_i}, y^{n_i}] = 0$ $(i = 1, \ldots, r)$ or (2) $(xy)^{n_i} = (yx)^{n_i}$ $(i = 1, \ldots, r)$. There exist nonnegative integers $m_1, \ldots, m_r$ such that $k = m_1 n_1 + \cdots + m_s n_s$, $l = m_{s+1} n_{s+1} + \cdots + m_r n_r$, and $1 = k - l$ $(1 \leq s \leq r)$.

Case (1): Put $n = n_1 \cdots n_r$. Then we have $[x^n, y^{n_i}] = 0$ for all i. Therefore, we have $[x^n, y]y^l = [x^n, y^{1+l}] = [x^n, y^k] = 0$. Hence $[x^n, y] = 0$.
Case (2): Since $[x, (xy)^{n_i}] = x\big((xy)^{n_i} - (yx)^{n_i}\big) = 0$ for all i, we have $x[x, y](xy)^l = [x, xy](xy)^l = [x, (xy)^{1+l}] = [x, (xy)^k] = 0$. Hence $[x, y] = 0$.

Lemma 2.5. *Let R be a unitary ring and T a nilpotent subring of R such that $T[T,T] = 0 = [T,T]T$. Let x, $y \in T$. If $\{1+x, 1+y\}$ is a P-subset of R, then $[x, y] = 0$.*

Proof. Noting that both $1 + x$ and $1 + y$ are invertible, there exist positive integers $n_1, \ldots, n_r$ with $(n_1, \ldots, n_r) = 1$ such that either $[(1+x)^{n_i}, (1+y)^{n_i}] = 0$ $(i = 1, \ldots, r)$ or $\big((1+x)(1+y)\big)^{n_i} = \big((1+y)(1+x)\big)^{n_i}$ $(i = 1, \ldots, r)$. Since $T[T,T] = 0 = [T,T]T$, we see that $[(1+x)^{n_i}, (1+y)^{n_i}] = n_i^2[x, y]$ and $\big((1+x)(1+y)\big)^{n_i} - \big((1+y)(1+x)\big)^{n_i} = n_i[x, y]$. Therefore, we can get the assertion.

Proof of Theorem 2.1. The assumption of Theorem 2.1 is inherited by all unitary factorsubrings. In view of Theorem 1.1, it suffices to show that R is not of type (i), (ii), (iii), (iv), or (v). We assume that $R = A \cup B$, where A and B are P-subsets of R.
Suppose that R is of type (i). Put $F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$. Since $R = A \cup B$, one of $A \cap F$ and $B \cap F$ contains at least two elements. But, this contradicts Lemma 2.2.
Suppose that R is of type (ii). We choose $\alpha \in K$ such that $\sigma(\alpha) \neq \alpha$, and put $F = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ 0 & \sigma(\alpha) \end{pmatrix}, \begin{pmatrix} \alpha & \alpha \\ 0 & \sigma(\alpha) \end{pmatrix} \right\}$. Then one of $A \cap F$ and $B \cap F$ contains at least two elements, which contradicts Lemma 2.3.
Suppose that R is of type (iii) or (iv). Let x and y be arbitrary elements in R. If both x and y belong to A or B, then, by Lemma 2.4, there exists a positive integer n such that $[x^n, y] = 0$. Now, assume that $x \in A$ and $y \in B$. If $x + y \in A$, then, by Lemma 2.4, there exists a positive integer n such that $[x^n, x + y] = 0$, and so $[x^n, y] = 0$. Similarly, if $x + y \in B$, then we have $[y^n, x] = 0$ with some positive integer n. Hence, R is commutative by [3, Theorem], a contradiction.
Finally, suppose that R is of type (v). Then $R = \langle 1, x, y \rangle$, $D(R)$ is the heart of R, and $T = \langle x, y \rangle$ is nilpotent. By Remark 1.2 (b), we have $TD(R) = 0 = D(R)T$. Put $F = \{1 + x, 1 + y, 1 + x + y\}$. Then one of $A \cap F$ and $B \cap F$ contains at least two elements, which contradicts Lemma 2.5.

3. $P(h,r)$**-subset.** A subset A of R is called a P^**-subset* of R if, for each x, $y \in A$, there exist $w_1, \dots, w_r \in \mathbf{W}$ and positive integers $n_1, \dots, n_r$ with $(n_1, \dots, n_r) = 1$ such that $w_i(x,y)\big((xy)^{n_i} - (yx)^{n_i}\big) = 0$ $(i = 1, \dots, r)$.

Let h and r be positive integers. A subset A of R is called a $P(h,r)$-*subset* of R if, for each $F \subseteq A$ consisting at most h elements, there exists a set N of r pairwise relatively prime positive integers and $w_{xy}^{(n)} \in \mathbf{W}$ $(x, y \in F, n \in N)$ such that either $w_{xy}^{(n)}(x,y)[x^n, y^n] = 0$ $(x, y \in F, n \in N)$ or $w_{xy}^{(n)}(x,y)\big((xy)^n - (yx)^n\big) = 0$ $(x, y \in F, n \in N)$.

For a positive integer n, we consider the following condition:

$Q'(n)$ For each x, $y \in R$, $[x,y]$ has the additive order which is relatively prime to n.

In this section, we shall prove the following theorems.

Theorem 3.1. *Let R be a unitary ring satisfying $Q'(2)$. Suppose that A is an additive subgroup of R excluding 1. If $R\backslash A$ is a P^*-subset of R, then R is commutative.*

Theorem 3.2. *Let R be a unitary ring satisfying $Q'(2)$. Suppose that A is an additive subgroup of R excluding 1. If $R\backslash A$ is a $P(2,3)$-subset of R, then R is commutative.*

Theorem 3.3. *Let R be a unitary ring satisfying $Q'(6)$. Suppose that A is an additive subgroup of R excluding 1. If $R\backslash A$ is a $P(3,2)$-subset of R, then R is commutative.*

To prove these, we need some lemmas.

The next lemma is easy and well known.

Lemma 3.4. *Let R be a ring and A a proper additive subgroup of R. If $R\backslash A$ is commutative, then R is commutative.*

Lemma 3.5. *Let φ be a ring homomorphism from a unitary subring R' of R onto a noncommutative ring S. Let A be an additive subgroup of R excluding 1. If $R\backslash A$ is a P-subset of R then $\varphi(A \cap R')$ is a proper additive subgroup of S.*

Proof. Put $B = \varphi(A \cap R')$. If $B = 0$, then S is a union of two P-subsets $\varphi(R' \backslash A)$ and $\{0\}$. But, this is impossible by Theorem 2.1. Hence $B \neq 0$. On the other hand, $1+B$ is a P-subset of S, because $1+(A \cap R') \subseteq R \backslash A$. Therefore, if $B = S$ then S is a P-subset of S, which is impossible again by Theorem 2.1. Hence $B \neq S$.

Lemma 3.6. *Let* $R = \begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$, *where p is a prime number greater than 2. If A is a proper additive subgroup of R, then $R \backslash A$ is not a P-subset of R.*

Proof. Suppose that $R \backslash A$ is a P-subset of R.
Further, suppose that $\begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix} \notin A$ for some $\alpha \in \mathrm{GF}(p)$. Then, by Lemma 2.2, both $\begin{pmatrix} 1 & \alpha+2^{-1} \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & \alpha+1 \\ 0 & 0 \end{pmatrix}$ belong to A. Hence, we have

$$\begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix} = 2\begin{pmatrix} 1 & \alpha+2^{-1} \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & \alpha+1 \\ 0 & 0 \end{pmatrix} \in A,$$

a contradiction. Therefore, all $\begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}$ belong to A.
Since A is a proper additive subgroup of R, A coincides with

$$\begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & 0 \end{pmatrix}.$$

On the other hand, it is easy to see that $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\}$ $(\subseteq R \backslash A)$ is not a P-subset of R, a contradiction.

Lemma 3.7. *Let $R = \mathrm{M}_\sigma(K)$, where K is a finite field with a nontrivial automorphism σ. If A is a proper additive subgroup of R, then $R \backslash A$ is not a P-subset of R.*

Proof. Suppose that $R \backslash A$ is a P-subset of R.
Further, suppose that $\begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix} \notin A$ for some $\alpha \in K$. If $\sigma(\alpha) = \alpha$, then, for $\eta \in K$ with $\sigma(\eta) \neq \eta$, one of $\begin{pmatrix} \eta & 0 \\ 0 & \sigma(\eta) \end{pmatrix}$ and $\begin{pmatrix} \alpha+\eta & 0 \\ 0 & \sigma(\alpha+\eta) \end{pmatrix}$ does

not belong to A. Hence, we may assume that $\sigma(\alpha) \neq \alpha$. By Lemma 2.3, we see that $\begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} \in A$ for all $0 \neq \beta \in K$. It follows that $\begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix} = \begin{pmatrix} \alpha & \alpha \\ 0 & \sigma(\alpha) \end{pmatrix} + \begin{pmatrix} \alpha & 1 \\ 0 & \sigma(\alpha) \end{pmatrix} - \begin{pmatrix} \alpha & \alpha+1 \\ 0 & \sigma(\alpha) \end{pmatrix} \in A$, a contradiction. Hence, we can write

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} \,\middle|\, \alpha \in K,\ \beta \in B \right\},$$

where B is a proper additive subgroup of K.
We can choose two different elements γ and δ in $K \backslash B$. Then, by Lemm 2.3, a subset $\left\{ \begin{pmatrix} \alpha & \gamma \\ 0 & \sigma(\alpha) \end{pmatrix}, \begin{pmatrix} \alpha & \delta \\ 0 & \sigma(\alpha) \end{pmatrix} \right\}$ of $R \backslash A$ is not a P-subset, a contradiction.

Lemma 3.8. *Let x and y be regular elements in R.*
(a) *If $\{x, y\}$ is a P^*-subset of R, then $[x, y] = 0$.*
(b) *If $\{x, y\}$ is a $P(2,3)$-subset of R, then $[x, y] = 0$.*

Proof.
(a) This was proved in Lemma 2.4.
(b) There exist pairwise relatively prime positive integers l, m, n such that either (i) $[x^l, y^l] = [x^m, y^m] = [x^n, y^n] = 0$ or (ii) $(xy)^l = (yx)^l$, $(xy)^m = (yx)^m$, $(xy)^n = (yx)^n$. In case of (ii), $\{x, y\}$ is a P^*-subset, and so $[x, y] = 0$ by (a). We consider the case (i). By the proof of Lemma 2.4, we see that $[x^{lm}, y] = [x^{mn}, y] = [x^{nl}, y] = 0$. Since $(lm, mn, nl) = 1$, the same argument of the proof of Lemma 2.4 shows that $[x, y] = 0$.

Corollary 3.9. *Let R be a domain and A a proper additive subgroup of R. If $R \backslash A$ is a P^*-subset or a $P(2,3)$-subset of R, then R is commutative.*

Proof. This is obvious by Lemmas 3.4 and 3.8.

Lemma 3.10. *Let x, y be invertible elements of R. If $\{x, y, xy\}$ is a $P(3,2)$-subset of R then $[x, y] = 0$.*

Proof. This is a combination of [2, Lemma 1] and Lemma 3.8 (a).

Lemma 3.11. *Let R be a noncommutative division ring and A a proper additive subgroup of R. If $R\backslash A$ is a $P(3,2)$-subset of R, then A is not a subring of R and the additive group R/A has an element of order 2.*

Proof. By Lemma 3.4, there exist $x,\ y \in R\backslash A$ such that $[x,y] \neq 0$. By Lemma 3.10, we have

$$xy \in A.$$

Since $(1+x)y = y+xy \notin A$ and $[1+x,y] \neq 0$, we have $1+x \in A$ again by Lemma 3.10, and similarly $1+y \in A$. Then, we see that $(1+x)(1+y) = (1+x)+xy+y \notin A$. Thus A is not a subring of R.
Since $x \notin A$ and $1+x \in A$, we have $1 \notin A$, and so $2+y \notin A$. Now suppose that $2x \notin A$. Then, we see that $x(2+y) = 2x+xy \notin A$. By Lemma 3.10, this induces a contradiction $[x, 2+y] = 0$. Thus $2x \in A$.

Lemma 3.12. *Let R be a ring of type* (iv) *which has characteristic p greater than 3. If A is a proper additive subgroup of R, then $R\backslash A$ is not a $P(3,2)$-subset of R.*

Proof. $R = \mathrm{GF}(p) \oplus T$ as additive group, where T is a simple radical ring. Suppose that $R\backslash A$ is a $P(3,2)$-subset of R. If $1+T \subseteq A$, then we have $1 \in A$ and $T \subseteq A$, and so $A = R$, a contradiction. Hence, there exists $t \in T$ such that

$$1+t \notin A.$$

Now, suppose that $(1+T)\backslash A$ is commutative. Let x, y be arbitrary elements in T.
Case 1. $1+x \notin A,\ 1+y \notin A$: Our supposition implies that $[x,y] = 0$.
Case 2. $1+x \notin A,\ 1+y \in A$: Since $1+t \notin A$, we have $[x,t] = 0$ by case 1. Further, $2+y+t = (1+y)+(1+t) \notin A$ implies that $1+2^{-1}(y+t) \notin A$. Therefore, we have $[x, y+t] = 0$ by case 1. Hence $[x,y] = 0$.
Case 3. $1+x \in A,\ 1+y \notin A$: Similar to case 2.
Case 4. $1+x \in A,\ 1+y \in A$: Since $1+t \notin A$, we have $[t,y] = 0$ by case 2. By the same way of the proof of case 2, we can see that $1+2^{-1}(x+t) \notin A$ and $[x+t, y] = 0$. Hence $[x,y] = 0$. Thus we have shown that T is commutative, a contradiction.
Therefore, there exist $x,\ y \in T$ such that

$$1+x \notin A,\ 1+y \notin A, \text{ and } [1+x, 1+y] \neq 0.$$

By Lemma 3.10, we have $(1+x)(1+y) \in A$. Since $(2+x)(1+y) = (1+y)+(1+x)(1+y) \notin A$ and $[2+x, 1+y] \neq 0$, we have $2+x \in A$ again by Lemma 3.10; similarly $2+y \in A$. Since $1+x \notin A$, we have $1 \notin A$, and so $3+x \notin A$. On the other hand, since R has characteristic $p > 3$, $1+y \notin A$ implies that $2(1+y) \notin A$. Therefore, we have $(3+x)(1+y) = 2(1+y)+(1+x)(1+y) \notin A$. Hence, by Lemma 3.10, we have $[3+x, 1+y] = 0$, a contradiction.

Lemma 3.13. *Let R be a ring of type* (v)*, and A a proper additive subgroup of R. If $R \backslash A$ is a P-subset of R, then the characteristic of R is a power of 2 and there exists $a \in A$ such that $a^2 \notin A$.*

Proof. R is a finite ring $\langle 1, x, y\rangle$ such that $T = \langle x, y\rangle$ is nilpotent and $TD(R) = 0 = D(R)T$. For $X \subseteq T$, we shall denote by $C(X)$ the centralizer of X in T.
Now, suppose that $1 \in A$. Then $T \nsubseteq A$. By Lemma 3.4, there exists $t \in T \backslash (A \cup C(T))$. Since $1+t \notin A$, we have $1 + (T\backslash C(t)) \subseteq A$ by Lemma 2.5. This together with $1 \in A$ implies that $T \backslash C(t) \subseteq A$, and so $T \subseteq A$, which is a contradiction. Thus we have shown that

$$1 \notin A.$$

Let u and v be elements in T such that $[u, v] \neq 0$. If $1 + (T \backslash C(T)) \subseteq A$, then we have $1+u$, $1+v$, $1+u+v \in A$, which implies a contradiction $1 = (1+u)+(1+v)-(1+u+v) \in A$. Hence, there exists $x \in T\backslash C(T)$ such that $1+x \notin A$. By Lemma 2.5, we have

$$1 + (T\backslash C(x)) \subseteq A.$$

Let $y \in T\backslash C(x)$. Then we have $1+y \in A$. Since $1 \notin A$, we see that $1+2y \notin A$. Hence, we have

$$2y \in C(x)$$

by Lemma 2.5, i.e., $2[x, y] = 0$. Noting Remark 1.2 (a), this shows that the characteristic of R is a power of 2.
We see that $[y^2, x] = y[y, x] + [y, x]x = 0$, i.e., $y^2 \in C(x)$. Hence

$$2y + y^2 \in C(x).$$

Since $y + C(x) \subseteq T\backslash C(x)$, we have $1 + (y + C(x)) \subseteq A$. This together with $1+y \in A$ implies that $C(x) \subseteq A$. Accordingly, $2y+y^2 \in A$. Hence, we have $(1+y)^2 = 1 + (2y+y^2) \notin A$.

Proof of Theorem 3.1. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R satisfying $Q'(2)$ contains a proper additive subgroup A such that $R\backslash A$ is a P^*-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). This was proved by Lemmas 3.6, 3.7, and 3.13 and Corollary 3.9.

Proof of Theorem 3.2. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R satisfying $Q'(2)$ contains a proper additive subgroup A such that $R\backslash A$ is a $P(2,3)$-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). This was proved by Lemmas 3.6, 3.7, and 3.13 and Corollary 3.9.

Proof of Theorem 3.3. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R satisfying $Q'(6)$ contains a proper additive subgroup A such that $R\backslash A$ is a $P(3,2)$-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). This was proved by Lemmas 3.6, 3.7, 3.11, 3.12, and 3.13.

4. Q-subset. A subset A of R is called a *Q^*-subset* of R if, for each x, $y \in A$, there exists a nonnegative integer k and positive integers $n_1, \dots, n_r$ with $(n_1, \dots, n_r) = 1$ such that $x^k\big((xy)^{n_i} - (yx)^{n_i}\big) = 0$ $(i = 1, \dots, r)$.

Let h and r be positive integers. A subset A of R is called a *$Q(h,r)$-subset* of R if, for each $F \subseteq A$ consisting at most h elements, there exists a nonnegative integer k and a set N of r pairwise relatively prime positive integers such that either $x^k[x^n, y^n] = 0$ $(x,\ y \in F,\ n \in N)$ or $x^k\big((xy)^n - (yx)^n\big) = 0$ $(x,\ y \in F,\ n \in N)$.

We shall prove the following theorems.

Theorem 4.1. *Let R be a unitary ring and A an additive subgroup of R excluding* 1. *Suppose that $a^2 \in A$ for all $a \in A$. If $R\backslash A$ is a Q^*-subset of R, then R is commutative.*

Theorem 4.2. *Let R be a unitary ring and A an additive subgroup of R excluding* 1. *Suppose that $a^2 \in A$ for all $a \in A$. If $R\backslash A$ is a $Q(2,3)$-subset of R, then R is commutative.*

Theorem 4.3. *Let R be a unitary ring and A a proper left ideal of R. If $R\backslash A$ is a $Q(3,2)$-subset of R, then R is commutative.*

We need the following lemma. A subset A of R is called a *Q-subset* of R if, for each x, $y \in A$, there exists a nonnegative integer k and positive integers $n_1, \ldots, n_r$ with $(n_1, \ldots, n_r) = 1$ such that either $x^k[x^{n_i}, y^{n_i}] = 0$ $(i = 1, \ldots, r)$ or $x^k((xy)^{n_i} - (yx)^{n_i}) = 0$ $(i = 1, \ldots, r)$.

Lemma 4.4. *Let $R = \begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & \mathrm{GF}(p) \end{pmatrix}$, where p is a prime number. If A is a proper additive subgroup of R and $a^2 \in A$ for all $a \in A$, then $R\backslash A$ is not a Q-subset of R.*

Proof. Suppose that $R\backslash A$ is a Q-subset of R.
We claim that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A$. In fact, if $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin A$, then both $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belong to A by Lemma 2.2. Hence

$$A = \left\{ \begin{pmatrix} \alpha & \alpha \\ 0 & \beta \end{pmatrix} \,\middle|\, \alpha,\ \beta \in \mathrm{GF}(p) \right\}.$$

Accordingly, we have $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \in A$, a contradiction.
Next, we claim that $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in A$. If $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin A$, then we have $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in A$ by Lemma 2.2. Hence $A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \beta \end{pmatrix} \,\middle|\, \alpha,\ \beta \in \mathrm{GF}(p) \right\}$, which induces a contradiction.
We have thus shown that $A = \begin{pmatrix} \mathrm{GF}(p) & \mathrm{GF}(p) \\ 0 & 0 \end{pmatrix}$. However, it is easy too see that $\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ $(\subseteq R\backslash A)$ is not a Q-subset, a contradiction.

Proof of Theorem 4.1. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R contains a proper additive subgroup A such that $a^2 \in A$ for all $a \in A$ and $R\backslash A$ is a Q^*-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). This was proved by Lemmas 3.7, 3.13, and 4.4 and Corollary 3.9.

Proof of Theorem 4.2. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R contains a proper additive subgroup A such that $a^2 \in A$ for all $a \in A$ and $R\backslash A$ is a $Q(2,3)$-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). This was proved by Lemmas 3.7, 3.12, and 4.4 and Corollary 3.9.

Proof of Theorem 4.3. In view of Theorem 1.1 and Lemma 3.5, it suffices to show that if a unitary ring R contains a proper left ideal A such that $R\backslash A$ is a $Q(3,2)$-subset of R then R cannot be of type (i), (ii), (iii), (iv), or (v). By Lemmas 3.7, 3.11, 3.13, and 4.4, R cannot be of type (i), (ii), (iii), or (v). Suppose that R is of type (iv). Then, R is generated by 1 and a simple radical subring T. Since $1+T$ is a subgroup of the unit group of R and A is a proper left ideal of R, we have $1+T \subseteq R\backslash A$. By Lemma 3.10, $1+T$ is commutative, which is a contradiction.

REFERENCES

[1] H. E. BELL, M. JANJIĆ and E. PSOMOPOULOS: On rings with powers commuting on subsets, Resultate Math. **18** (1990), 1–9.

[2] M. HONGAN: A commutativity theorem for s-unital rings. II, Math. J. Okayama Univ. **25** (1983), 19–22.

[3] I. N. HERSTEIN: A commutativity theorem, J. Algebra **38** (1976), 112–118.

[4] H. KOMATSU, T. NISHINAKA and H. TOMINAGA: A commutativity theorem for rings, Bull. Austral. Math. Soc. **44** (1991), 387–389.

[5] H. KOMATSU and H. TOMINAGA: Some commutativity theorems for left s-unital rings, Resultate Math. **15** (1989), 335–342.

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

GRADUATE SCHOOL OF NATURAL SCIENCE AND TECHNOLOGY
OKAYAMA UNIVERSITY
OKAYAMA, 700 JAPAN

(Received December 26, 1997)