The identity \((xy)^n = x^ny^n\) and commutativity of rings

Yuji Kobayashi*
THE IDENTITY \((xy)^n = x^ny^n\) AND COMMUTATIVITY OF RINGS

YUJI KOBAYASHI

We shall give a commutativity theorem for rings with identity element. It contains some known results which have been obtained by several authors. Throughout this paper \(R\) represents a ring with 1, and \(N\) denotes the set of all positive integers.

1. Statement of Theorem. Let \(S\) be a semigroup or a ring. The subset \(E(S)\) of \(N\) defined by

\[
E(S) = \{ n \in N \mid (xy)^n = x^ny^n \text{ for all } x, y \in S \}
\]

forms a multiplicative subsemigroup of \(N\) and is called the exponent semigroup of \(S\) (Tamura [9]). The purpose of this paper is to prove the following

**Theorem.** Let \(R\) be a ring with 1. If \(E(R)\) contains integers \(n_1, \ldots, n_r \geq 2\) such that \((n_1(n_1-1), \ldots, n_r(n_r-1)) = 2\) and some of \(n_i\) is even, then \(R\) is commutative.

The theorem contains the following well-known result: If \(E(R)\) contains three consecutive positive integers, \(R\) is commutative. This was proved by Luh [7] under the additional condition that \(R\) is a primary ring. Ligh and Richoux [6] removed the condition and gave a complete and elementary proof. Our theorem contains also the following more general result: If \(E(R)\) contains \(m, m+1, n\) and \(n+1\) such that \((m, n)\) is either 1 or 2, then \(R\) is commutative. In case \((m, n) = 1\), this result was proved by Bell [1, Theorem 2]. In case \((m, n) = 2\), this was first proved by Yen [10, Theorem 2] under the condition that \(R\) is primary, and Mogami [8] removed the condition (even in a localized version).

As the simplest case of the theorem we have the following: If \(2 \in E(R)\), \(R\) is commutative. This was given by Johnsen, Outcalt and Yaqub [3]. Let us consider the case \(3 \in E(R)\). Then, \(R\) is commutative, if \(E(R)\) contains some \(n\) such that \(n \equiv 2 \pmod{6}\). Note that the commutativity of \(R\) need not follow only from the condition \(3 \in E(R)\).
exponent semigroups (Kobayashi [4, Theorem 3]). However, for the convenience of the reader, we shall give a direct proof of it in the last section.

**Lemma 1.** Let $S$ be a cancellative semigroup. If $E(S)$ contains integers $n_1, \ldots, n_r \geq 2$ such that $(n_1(n_1-1), \ldots, (n_r(n_r-1)) = 2$, then $S$ is commutative.

**Lemma 2.** Let $x, y \in R$. Then under the assumption in Theorem, $xy = 0$ implies $yx = 0$.

*Proof.* Let $n \in E(R)$ and $n \geq 2$. Assume that $xy = 0$. Then we have

$$y^n + y^nx = (y + yx)^n = y^n(1 + x)^n.$$ 

It follows that

$$(n-1) y^nx = -y^n x \sum_{i=2}^{n} \binom{n}{i} x^{i-1}.$$ 

Using this equality $n-1$ times, we get

$$(n-1)^{n-1} y^nx = (-1)^{n-1} y^n x \sum_{i=2}^{n} \binom{n}{i} x^{i-1}.$$ 

Since $y^nx = (yx)^n = 0$, we obtain $(n-1)^{n-1} y^nx = 0$. By the assumption there are integers $n_1, \ldots, n_r \geq 2$ in $E(R)$ such that $(n_1-1, \ldots, n_r-1) = 1$. Thus we get the equalities

$$(n_i-1)^{n_i-1} y^{m_i} x = 0 \quad (i = 1, \ldots, r),$$

where $m_i = \max \{n_1, \ldots, n_r\}$. It follows that $y^{m_i} x = 0$. A similar argument starting with the equation $(x + yx)^n = (1 + y)^n x^n$ yields $yx^{m_i} = 0$.

On the other hand, we have

$$(1 + x)^n + (1 + y)^n - 1 = (1 + x)^n(1 + y)^n = (1 + x + y)^n = (1 + x)^n + (1 + y)^n - 1 + \sum_{i+j=n} \binom{n}{i+j} y^i x^j.$$

It follows that

$$\binom{n}{2} yx = -\sum_{n \neq i+j \geq 3} \binom{n}{i+j} y^i x^j.$$ 

Using this equality repeatedly, we obtain

$$\binom{n}{2} yx = \sum_{i+j \geq 1} a_{i,j} y^i x^j,$$

where $m_0 = \min \{n \mid n \in E(R), n \geq 2\}$ and $a_{i,j}$ are integers. Since $y^{m_0} x^{m_0} = yx^{m_1} = y^{m_1} x = 0$, it follows that $\binom{n}{2} yx = 0$. By the
assumption that there are integers \( n_1, \ldots, n_r \geq 2 \) in \( E(R) \) such that \( \left( \begin{array}{c} n_1 \\ 2 \end{array} \right), \ldots, \left( \begin{array}{c} n_r \\ 2 \end{array} \right) = 1 \), we conclude that \( yx = 0 \).

**Proof of Theorem.** Let us assume the condition in Theorem is satisfied. By Lemma 2 there is no distinction between left and right zero-divisors in \( R \), and for any subset \( S \) of \( R \), the left and the right annihilator of \( S \) coincide and form a two-sided ideal of \( R \), which we denote by \( \text{Ann}(S) \). Let \( D \) be the set of all zero divisors of \( R \) (together with 0). To prove the theorem we may assume that \( R \) is subdirectly irreducible. Let \( H \) be the unique nonzero minimal ideal of \( R \). We claim that \( D = \text{Ann}(H) \). Clearly \( D \supset \text{Ann}(H) \). Conversely, let \( d \) be any element in \( D \). Since \( \text{Ann}(d) \) is a nonzero ideal of \( R \), it contains \( H \). This means \( d \in \text{Ann}(H) \), proving the claim. In particular we see that \( D \) is an ideal of \( R \). It follows that \( R \setminus D \) generates \( R \). Since \( R \setminus D \) is a cancellative semigroup by multiplication, it is commutative by Lemma 1. Therefore \( R \) is also commutative.

3. **Remarks.** In Theorem the existence of 1 in \( R \) is essential, because there is a non-commutative ring without 1 whose exponent semigroup contains all positive integers ([3, Example 1]).

The condition that \( (n_1(n_1 - 1), \ldots, n_r(n_r - 1)) = 2 \) is also indispensable as the following example shows.

**Example** (c.f. Kobayashi [5, Example 4]). Let \( q \geq 2 \) be an integer and \( \mathbb{Z}_q \) the residue class ring of integers modulo \( q \). Let \( N \) be a non-commutative algebra over \( \mathbb{Z}_q \) such that \( N^3 = 0 \). We consider the ring \( R \) whose additive group is the direct sum \( \mathbb{Z}_q \oplus N \) with multiplication given by \( (a + x) \cdot (b + y) = ab + (ay + bx + xy) \) for \( a, b \in \mathbb{Z}_q \) and \( x, y \in N \). Then, \( R \) is a ring with 1 and satisfies the identity \((xy)^n = x^n y^n\) for any positive integer \( n \) such that \( n(n - 1)/2 \equiv 0 \pmod{q} \). But, \( R \) is not commutative.

The second condition that some of \( n_i \) is even can be removed when \( R \) is a primary ring. In fact, let \( R \) be a primary ring, that is, the Jacobson radical \( J \) of \( R \) is maximal, and assume that there are integers \( n_1, \ldots, n_r \geq 2 \) in \( E(R) \) such that \( (n_1(n_1 - 1), \ldots, n_r(n_r - 1)) = 2 \). Then, \( R/J \) is commutative by Herstein [2, Theorem 1], so it is a field. It follows that \( R \) is generated by its units. Hence, \( R \) is commutative by Lemma 1.

We do not know if Theorem remains true in general after removing the second condition.
4. Proof of Lemma 1. Let $S$ be a cancellative semigroup satisfying the condition in Lemma 1. Let $\iota$ denote the equality relation on $S$. For $n \in \mathbb{N}$ we define the relation $\pi_n$ on $S$ as follows: For $x, y \in S$, $x \pi_n y$ if $x^n = y^n$ for some $e \in \mathbb{N}$. $S$ is called $n$-power cancellative if $\pi_n = \iota$. If $n \in E(S)$, it is readily seen that $\pi_n$ is a congruence on $S$ and the quotient semigroup $S/\pi_n$ is an $n$-power cancellative, cancellative semigroup. We set $P(S) = \{n \in E(S) \mid \pi_n = \iota\}$.

We claim that if $m_1, \ldots, m_s$ are positive integers such that $(m_1, \ldots, m_s) = 1$, then $\pi_{m_1} \cap \cdots \cap \pi_{m_s} = \iota$. Let $x, y \in S$ and suppose that $x \pi_{m_i} y$ for $i = 1, \ldots, s$, that is, $x^{k_i} = y^{k_i}$ for some power $k_i$ of $m_i$ $(i = 1, \ldots, s)$. Since $(k_1, \ldots, k_s) = 1$, by renumbering $k_i$ if necessary, we can find non-negative integers $l_1, \ldots, l_s$ such that $l_1k_1 + \cdots + l_sk_s = l_{t+1}k_{t+1} + \cdots + l_sk_s + 1$ $(1 \leq t < s)$. Then we have

$$x^{l_1k_1} = \prod_{i=1}^{s} x^{l_1k_1} = \prod_{i=1}^{s} y^{l_1k_1} = (\prod_{i=1}^{s} y^{l_1k_1}) y = (\prod_{i=1}^{s} x^{l_1k_1}) y.$$

By the cancellation law we then get $x = y$, proving the claim.

Now, we set $R(S) = \{n \in \mathbb{N} \mid (xy)^n = y^n x^n \text{ for all } x, y \in S\}$. If $n \geq 2$ is in $E(S)$, then $n-1 \in R(S)$ by cancellation. So, if $2 \in E(S)$, then $1 \in R(S)$ and $S$ is commutative. Let $n \geq 3$ and $n \in E(S)$. Then $(n-1)^2 \geq 4$ and $(n-1)^2 \in E(S)$. Since $(n, (n-1)^2) = 1$, we get $\pi_n \cap \pi_{n-1} = \iota$ by the claim above. Thus $S$ is isomorphic to a subdirect product of $S/\pi_n$ and $S/\pi_{n-1}$. To show the commutativity of $S$, it suffices to show it for $S/\pi_n$ and $S/\pi_{n-1}$, which are $n$-power cancellative and $(n-1)^2$-power cancellative respectively. So we may assume from the first that $P(S) \setminus \{1\} \neq \emptyset$.

We claim that if $m \geq 2$ is in $P(S)$, then $m-1 \in E(S)$ and $x^{m-1}$ is in the center of $S$ for every $x \in S$. If $m \in P(S)$, then $(m-1)^2 \in E(S)$ as above. Hence $m(m-2) = (m-1)^2 - 1 \in R(S)$. Since $m \in P(S)$, it follows that $m-2 \in R(S)$. Thus we find $m-1 \in E(S)$. So we have $x^n y^m = (xy)^n = x y x^{m-1} y^{m-1}$ for any $x, y \in S$. By cancellation we obtain $x^{m-1} y = y x^{m-1}$, proving the claim.

Let $m$ be the smallest integer in $P(S) \setminus \{1\}$. We proceed by induction on $m$. If $m = 2$, $S$ is commutative. Let assume that $m \geq 3$ and the assertion of the lemma holds for any cancellative semigroup $S'$ for which $P(S')$ contains an integer $m'$ such that $m > m' \geq 2$. Let $n_1, \ldots, n_r$ be in $E(S)$ and $(n_1(n_1-1), \ldots, n_r(n_r-1)) = 2$. If $m-1$ divides $n_i$ or $n_i - 1$ for every $i = 1, \ldots, r$, then $m-1$ is either 1 or 2. In either case $2 \in E(S)$ and consequently $S$ is commutative. Henceforth, assume that there is $n \in E(S)$ such that $n \equiv 0, 1 \pmod{m-1}$. Let $n = l(m-1) + k$, $2 \leq k \leq
m - 2. Since \( m - 1 \in E(S) \) and \( x^{m-1} \) and \( y^{m-1} \) are in the center for any \( x, y \in S \), we have

\[
x^n y^n = (xy)^{l(m-1)+k} = (x^{m-1} y^{m-1})^{l} (xy)^{k} = x^{l(m-1)} (xy)^{k} y^{l(m-1)}.
\]

The cancellation law gives \( x^k y^k = (xy)^k \), showing \( k \in E(S) \). Since \( m - 2, k - 1 \in R(S) \), we see that \( (m-2)(k-1) = (k-2)(m-1) + (m-k) \in E(S) \).

In the same way as above we find that \( m - k \in E(S) \). Note that \( m > m - 1, k, m - k \geq 2 \) and \( (m-1, k, m-k) = 1 \). Thus by the first claim we see that \( \pi_{m-1} \cap \pi_k \cap \pi_{m-k} = \emptyset \), that is, \( S \) is isomorphic to a subdirect product of \( S/\pi_{m-1}, S/\pi_k \) and \( S/\pi_{m-k} \), which are \( (m-1), k \)- and \( (m-k) \)-power cancellative respectively. By the induction hypothesis they are all commutative. Consequently \( S \) is also commutative, this completes the proof.

REFERENCES


FACULTY OF EDUCATION

TOKUSHIMA UNIVERSITY

TOKUSHIMA, JAPAN

(Received April 28, 1981)