On rings satisfying the identity \((X - X^n)^2 = 0\)

Hisao Tominaga\(^*\) \hspace{1cm} Adil Yaqub\(^†\)

\(^*\)Okayama University  
\(^†\)University Of California
ON RINGS SATISFYING THE IDENTITY  
\[(X - X^n)^2 = 0\]

HISAO TOMINAGA and ADIL YAQUB

Throughout, \( R \) will represent a ring with center \( C \), and \( N \) the set of nilpotent elements in \( R \). Let \( n \) be a positive integer greater than 1, and \( E_n \) the set of elements \( x \) in \( R \) such that \( x = x^n \).

We consider the following properties:

(i) \( N \) is commutative.
(ii) \( (x - x^n)(y - y^n) = 0 \) for all \( x, y \in R \).
(iii) \( (x - x^n)^2 = 0 \) for all \( x \in R \).
(iv) \( (x - x^n)^n = 0 \) for all \( x \in R \).
(v) Any \( x \in R \) may be written in at most one way in the form \( x = b + a \), where \( b \in E_n \) and \( a \in N \). (There may be elements \( x \) in \( R \) which cannot be written in the given form.)

If \( R \) satisfies (ii) and (v), then \( R \) is called a generalized \( n \)-ring. Following [4], \( R \) is called a generalized \( n \)-like ring if \( (xy)^n - x^n y^n + xy \)

Following [4], \( R \) is called a generalized \( n \)-like ring if \( (xy)^n - x^n y^n + xy \)

The major purpose of this paper is to prove the following

**Theorem 1.** If \( R \) satisfies (i), (ii) and (v), then \( R \) is commutative.

In preparation for proving Theorem 1, we state the next lemma.

**Lemma 1.** (1) Let \( R \) be a ring satisfying (i) and (ii). Then \( N \) is a commutative nil ideal of bounded index at most 2. If there exists an integer \( m > 1 \) such that \( m^2 x^4 = 0 \) for all \( x \in R \), then \( x^{m^2} \in E_n \) for all \( x \in R \).

(2) If \( R \) satisfies (i) and (ii), then there exists a finite set \( P \) of prime numbers such that \( R = \sum_{p \in P} R^{(p)} \), where \( R^{(p)} = \{ x \in R \mid px \in N \} \).

(3) Let \( R \) be a ring satisfying (i), (ii) and (v). If there exists an integer \( m > 1 \) such that \( m^2 x^4 = 0 \) for all \( x \in R \), then \( x^{m^2} \in E_n \) for all \( x \in R \) and \( a \in N \).

**Proof.** (1) By (ii), there holds \( x^{2n} = 2x^{n+1} - x^2 \). Hence, \( N \) is a commutative nil ideal of bounded index at most 2 by [2, Lemma 2 (2)]. Furthermore, an easy induction shows that \( x^{m^2 + 2} = \mu x^{n+1} - (\mu - 1)x^2 \), and so \( x^{m^2} = \mu(x^{n+1} - x^2) + x^2 \) for any positive integer \( \mu \); in particular, \( x^{m^2} = 181 \)
Let $m=(2^n-2)^2$. Since $N$ is an ideal of $R$ by (1), we see that 
$(2^n-2)x=2^n(x-x^n)-(2x-(2x)^n)\in N$ for all $x \in R$, i.e., $m(R/N)=0$. As is well known, the factor ring $R/N$ satisfying the polynomial identity $X-X^n=0$ is a subdirect sum of finite fields (see, e.g., [1, Theorem 19]). Noting here that $m(R/N)=0$, we can easily see the assertion. Needless to say, every $R^{(p)}$ is an ideal of $R$ containing $N$.

(3) Let $x \in R$, and $a \in N$. According to (1), we have $(x+a)^m=x^{m^2}+a'+a''$, where $x^{m^2} \in E_n$, $a'=\sum_{t=0}^{n-1} x^{m^2-t} ax^t \in N$, and $a'' \in N^2 \subseteq C$. Since $(x+a)^m$ is also in $E_n$, (iii)$_n$ shows that $a'+a''=0$. Hence, $[x^{m^2},a]=[x,a']+[x,a'']=0$.

Proof of Theorem 1. In view of Lemma 1 (2), there exists a finite set $P$ of prime numbers such that $R=\sum_{p \in P} R^{(p)}$, where $R^{(p)}$ is the ideal of $R$ containing $N$ defined by $\{x \in R \mid px \in N \}$. Obviously, (i)$_n$, (ii)$_n$ and (iii)$_n$ are inherited by the ideal $R^{(p)}$. Since $N$ is a nil ideal of bounded index at most 2 (Lemma 1 (1)), we see that $p^2x^2=0$ for all $x \in R^{(p)}$, and so $[x^{p^2},a]=0$ for all $x \in R^{(p)}$ and $a \in N$ (Lemma 1 (3)). As is well known, the factor ring $R^{(p)}/N$ satisfying the polynomial identity $X-X^n=0$ is a subdirect sum of finite fields of characteristic $p$, and hence we can find a positive integer $k$ such that $x^{pk}-x \in N$ for all $x \in R^{(p)}$. Now, let $x \in R^{(p)}$ and $a \in N$. Since $[x^{pk},a]=0$ and $x^{pk}-x \in N$, we get $[x,a]=0$ by (i)$_n$, which shows that $N$ is in the center of $R^{(p)}$. Hence, $N$ is contained in the center of $R$, and therefore $R$ is commutative by [1, Theorem 19].

If $R$ is a generalized $n$-ring, it is easy to see that $N^2=0$, and so $N$ is commutative. Thus, as a direct consequence of Theorem 1, we have

**Corollary 1.** Every generalized $n$-ring is commutative. In particular, every generalized $n$-like ring satisfying (iii)$_n$ is commutative.

**Corollary 2.** Suppose that there exists an integer $m>1$ such that $(m,n-1)=1$ and $mN=0$. Suppose that $R$ satisfies (i)$_n$ and (ii)$_n$. Then, $R$ is commutative if and only if $R$ satisfies (iii)$_n$.

**Proof.** In view of Theorem 1, it suffices to show that if $R$ is commutative then (iii)$_n$ is satisfied. Suppose that both $b$ and $b+a$ are in $E_n$ with some $a \in N$. Then $b+nab^{n-1}=(b+a)^n=b+a$ (Lemma 1 (1)), and so $nab^{n-1}=a$, whence it follows that $nab=nab^n=ab$. Hence, $na=n^2ab^{n-1}=nab^{n-1}=a$, namely $(n-1)a=0$. Since $ma=0$ and $(m,n-1)=1$, we get $a=0$, proving (iii)$_n$. 

http://escholarship.lib.okayama-u.ac.jp/mjou/vol25/iss2/12
ON RINGS SATISFYING THE IDENTITY \((X - X^n)^2 = 0\)  183

Next, motivated by [3, Theorem 1], we prove the following

**Theorem 2.** Let \( p \) be a prime. If \( R \) satisfies (i), (ii)\(_p\) and \( pR = 0 \), then the following are equivalent:

1) \( R \) is commutative.
2) \( R \) satisfies (iii)\(_p\).
3) \( E_p \) is a subring of \( R \).
4) \( E_p \) is an additive subgroup of \( R \).
5) \( E_p \) is central.

**Proof.** Obviously, \( x^p \in E_p \) for any \( x \in R \), and \( N \) is a commutative nil ideal of bounded index at most \( p \) by [2, Lemma 2 (2)]. Then, it is easy to see that \( 1) \Rightarrow 3) \Rightarrow 4) \Rightarrow 2) \) and \( 1) \iff 5) \).

2) \( \Rightarrow 1) \). Let \( x \in R \), and \( a \in N \). Then we have \((x + a)^p = x^p + a' + a''\), where \( x^p \in E_p \), \( a' = \sum \sum a^{p-i-1}ax^i \in N \) and \( a'' \in N^2 \subseteq C \). Since \((x + a)^p\) is also in \( E_p \), (iii)\(_p\) shows that \( a' + a'' = 0 \). Hence, \([x, a'] = [x, a''] = 0\), and therefore \([x, a] = [x^p, a] + [x - x^p, a] = 0\), which shows that \( N \subseteq C \). Now, \( R \) is commutative by [1, Theorem 19].

**Examples.**

1) The commutative ring \( R = \mathbb{Z}/4\mathbb{Z} \) satisfies (ii)\(_3\), but does not (iii)\(_3\); the commutative ring \( \mathbb{Z}/8\mathbb{Z} \) satisfies (ii)\(_3\), but does neither (ii)\(_3\) nor (iii)\(_3\).

2) Let \( p \) be a prime. Then \( R = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in GF(p) \) is a non-commutative ring satisfying (ii)\(_p\) and \( pR = 0 \).

3) Let \( R = \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \mid a, b, c \in GF(3) \). Then \( R \) is a commutative ring satisfying (ii)\(_3\) and \( 3R = 0 \), but not (ii)\(_3\).

4) Let \( R = \begin{pmatrix} a & b & c & d \\ 0 & a & 0 & c \\ 0 & 0 & a & b \\ 0 & 0 & 0 & a \end{pmatrix} \mid a, b, c, d \in GF(2) \). Then \( R \) is a commutative ring satisfying (ii)\(_2\) = (ii)\(_2\) and \( 2R = 0 \), but not (ii)\(_2\)*.

These examples give the following table, where (c) signifies the property that \( R \) is commutative.

Produced by The Berkeley Electronic Press, 1983 3
In conclusion, we would like to express our indebtedness and gratitude to the referee for his helpful suggestions and valuable comments.

REFERENCES


O凯亚马大学, O凯亚马, 日本
大学加利福尼亚, 圣芭芭拉, U.S.A.

(Received June 30, 1983)