Internat. J. Math. & Math. Sci.
VOL. 17 NO. 4 (1994) 807-812

J-RINGS OF CHARACTERISTIC TWO THAT ARE BOOLEAN

D. J. HANSEN and JIANG LUH

Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27695-8205, U.S.A.

YOUPEI YE

East China Institute of Technology
Nanjing, China

(Received July 27, 1993)

ABSTRACT. This paper is concerned with determining all integers n, with $n \geq 2$, such that if R is a ring having the property that $x^n = x$ and $2x = 0$ for each $x \in R$, then R is boolean. The solution to the above problem extends previous results obtained by Shiue and Chao in [5] and that of MacHale in [4].

KEY WORDS AND PHRASES. J-ring, boolean ring.
1992 AMS SUBJECT CLASSIFICATION CODES. 16A38.

1. INTRODUCTION.

A ring R is called a J-ring if there exists an integer $n \geq 2$ such that $x^n = x$ for each $x \in R$. It is well known that a J-ring is commutative, see [3].

Shiue and Chao showed in [5] that if R is a J-ring, where $n = 2^{q(m+1)} + 2^m$, with $1 \leq q$ and $1 \leq m$, then it is the case that R is of characteristic two and, in addition, $x^2 = x$ for each $x \in R$, that is, R is boolean. Recently, MacHale proved that if R is a ring of characteristic two and n is a nonnegative integer such that $x^{2^n+1} = x$, for each $x \in R$, then R is also boolean. In this paper, we will extend both of the above results by determining all integers n, with $n \geq 2$, such that if R is a ring having the property that $x^n = x$ and $2x = 0$, for each $x \in R$, then $x^2 = x$ for each $x \in R$. It should be noted that, in a related paper, Batbedat [2] used sheaf theory to obtain some structure theorems for a ring R satisfying $a^{n+1} = a$ for each $a \in R$. His results were used to determine all values of $n \leq 50$ for which R is boolean.

2. A PRELIMINARY RESULT.

THEOREM 1. Let n denote an integer ≥ 2. Then $2^t - 1 \nmid n - 1$ for each integer $t \geq 2$ if and only if for each ring R such that $x^n = x$ and $2x = 0$ for each $x \in R$ implies that R is boolean.

PROOF. Suppose $2^t - 1 | n - 1$ for some integer $t \geq 2$. Let R denote the Galois field GF (2^t). If $x \in R$, with $x \neq 0$, then $x^{2^t-1} = 1$ and thus $x^{n-1} = 1$ since $2^t - 1 | n - 1$. Hence $x^n = x$. Since $0^n = 0$, we thus have that $x^n = x$ for each $x \in R$. It is well known that GF(2^t) is of characteristic 2. Consequently, $R = GF(2^t)$ is a ring such that $x^n = x$ and $2x = 0$ for each $x \in R$, however R is not boolean.

Next assume that $2^t - 1 \nmid n-1$ for each $t \geq 2$. Suppose to the contrary that there exists a nonboolean ring R such that $x^n = x$ and $2x = 0$ for each $x \in R$. Then there exists an $a \in R$ such that $a^2 \neq a$. Consider $< a >$, the subring of R generated by a. First, note that $< a >$ is finite and commutative. Also, $< a >$ is semi-simple since, for each $x \in < a >$, x^{n-1} is idempotent and the Jacobson radical of $< a >$ does not contain non-zero idempotent elements. Hence, by the Wedderburn-Artin theorem, $< a >$ is a direct sum of finitely many Galois fields of characteristic 2, say, $< a >= \sum_{i=1}^{m} \oplus GF(2^{t_i})$. Clearly, $2^{t_i} - 1 | n-1$ for $i = 1, 2, \cdots, m$ and thus $t_i = 1$ for $i = 1, 2, \cdots, m$ since $2^t - 1 \nmid n-1$ for each $t \geq 2$. Hence $a^2 = a$ and this is a contradiction. Therefore if R is a ring of characteristic two such that $x^n = x$ for each $x \in R$, then R is boolean.

3. A SPECIAL CLASS OF MATRICES.

Let k denote an integer ≥ 2. For each such k, define the matrix M_k to be the matrix with k columns whose rows are of the form $[k - t_1, k - t_2, \cdots, k - t_k]$, where each $t_1, t_2, \cdots, t_k$ is a non-negative integer such that $t_1 \geq t_2 \geq \cdots \geq t_k$ and $2^{t_1} + 2^{t_2} + \cdots + 2^{t_k} = 2^k$. Furthermore, if $r = [k - t_1, k - t_2, \cdots, k - t_k]$ and $r' = [k - t'_1, k - t'_2, \cdots, k - t'_k]$ are two rows in M_k, then r is a above r' if and only if either $k - t_1 < k - t'_1$ or $k - t_i = k - t'_i$ for $i = 1, 2, \cdots, m$ and $k - t_{m+1} < k - t'_{m+1}$.

The following lemma and theorem will give an inductive method for constructing the above type of matrices.

LEMMA 2. Let k denote an integer ≥ 2. Let each of t and $t_1, t_2, \cdots, t_k$ denote a nonnegative integer such that $2^{t_1} + 2^{t_2} + \cdots + 2^{t_k} = 2^t$, where $t_1 \geq t_2 \geq \cdots \geq t_k$. Then $t_{k-1} = t_k$.

PROOF. Clearly $t > t_i$ for $i = 1, 2, \cdots, k$. From $2^{t_1} + 2^{t_2} + \cdots + 2^{t_k} = 2^t$, we obtain $2^{t_1 - t_k} + 2^{t_2 - t_k} + \cdots + 2^{t_{k-1} - t_k} + 1 = 2^{t - t_k}$. Since 2^{t-t_k} is even, then at least one of $t_i - t_k, 1 \leq i \leq k-1$, is zero, say, $t_j - t_k$. Then $t_j = t_k$ which implies that $t_{k-1} = t_k$ since $t_j \geq t_{k-1} \geq t_k$.

LEMMA 3. Let k denote an integer ≥ 2. If l is an integer, with $2 \leq l \leq k$, and if each of $t_1, t_2, \cdots, t_l$ is a nonnegative integer such that $2^{t_1} + 2^{t_2} + \cdots + 2^{t_l} = 2^k$, then $t_i > 0$ for all $i, 1 \leq i \leq l$.

PROOF. The proof is by induction on k. Let S denote the set such that $k \in S$ if and only if $k \geq 2$ and $2^{t_1} + 2^{t_2} + \cdots + 2^{t_l} = 2^k$ implies that $t_i > 0$ for $1 \leq i \leq l$, where $2 \leq l \leq k$. For $k = 2$, the only equation, since $l = 2$, is $2^{t_1} + 2^{t_2} = 2^2$ and this implies that $t_1 = t_2 = 1$. Thus $2 \in S$. Let $k \in S$. Next, let $2 \leq l' \leq k+1$ and suppose $t'_1 \geq t'_2 \geq \cdots \geq t'_{l'} \geq 0$ such that $2^{t'_1} + 2^{t'_2} + \cdots + 2^{t'_{l'}} = 2^{k+1}$. Now, suppose there exits a t'_i which is zero. Then either all of the t'_i's are zero, and thus l' would be even in that case or there exists a j such that $t'_j > 0$ with $t'_{j+1} = 0$ and this would imply that there exists again an even number of t'_i's equal to zero. Hence, in either ease, we can group the 2^o's in pairs and obtain either $(2^o + 2^o) + (2^o + 2^o) + \cdots + (2^o + 2^o) = 2^{k+1}$ or $2^{t'_1} + 2^{t'_2} + \cdots + 2^{t'_j} + (2^o + 2^o) + \cdots + (2^o + 2^o) = 2^{k+1}$. Since $2^o + 2^o = 2$, we have either $2^1 + 2^1 + \cdots + 2^1 = 2^{k+1}$ or $2^{t'_1} + 2^{t'_2} + \cdots + 2^{t'_j} + 2^1 + \cdots + 2^1 = 2^{k+1}$ and this gives, on dividing both sides by 2, either $2^o + 2^o + \cdots + 2^o = 2^k$ or $2^{t'_1 - 1} + 2^{t'_2 - 1} + \cdots + 2^{t'_j - 1} + 2^o + \cdots + 2^o = 2^k$. Note that the number of terms on the left in either equation is now $\leq k$. Hence we have arrived at a contradiction since $k \in S$ implies that all of the exponents in either equation must be positive. Therefore $k + 1 \in S$ and this completes the induction argument.

COROLLARY 4. $M_2 = [1, 1]$.

PROOF. For $k = 2$, we consider $2^{t_1} + 2^{t_2} = 2^2$. From Lemma 2, we have that $t_1 = t_2$. Thus $2^{t_1 + 1} = 2^2$ which implies that $t_1 = 1$. Since $t_2 = t_1$, we have that $t_2 = 1$. Hence $M_2 = [k - t_1, k - t_2] = [2 - 1, 2 - 1] = [1, 1]$.

THEOREM 5. Suppose $M_k = [s_{ij}^{(k)}]$. Then the rows of M_{k+1} are precisely the rows obtained from the rows of M_k by replacing one entry $s_{ij}^{(k)}$ by the 1×2 matrix $[s_{ij}^{(k)} + 1, s_{ij}^{(k)} + 1]$, and following this by a suitable rearrangement of the entries.

PROOF. First, we will show that a row obtained from the i^{th} row of M_k by replacing the entry $s_{ij}^{(k)}$ by $[s_{ij}^{(k)}+1, s_{ij}^{(k)}+1]$ is, follwed by a suitable rearrangement of the entries, a row in the matrix M_{k+1}, that is, $[s_{i1}^{(k)}, \cdots, s_{i,j-1}^{(k)}, s_{ij}^{(k)}+1, s_{ij}^{(k)}+1, s_{i,j+1}^{(k)}, \cdots, s_{ik}^{(k)}]$ follwed by rearranging the numbers in ascending order will be a row in M_{k+1}. To see that this is the case, consider, from the definition of M_{k+1}, the sum $\sum_{q=1}^{j-1} 2^{k+1-s_{iq}^{(k)}} + 2^{k+1-(s_{ij}^{(k)}+1)} + 2^{k+1-(s_{ij}^{(k)}+1)} + \sum_{q=j+1}^{k} 2^{k+1-s_{iq}^{(k)}} = \sum_{q=1}^{j-1} 2^{k+1-s_{iq}^{(k)}}$ $+ 2^{k+1-s_{ij}^{(k)}} + \sum_{q=j+1}^{k} 2^{k+1-s_{iq}^{(k)}} = \sum_{q=1}^{k} 2^{k+1-s_{iq}^{(k)}} = 2\sum_{q=1}^{k} 2^{k-s_{iq}^{(k)}} = 2 \cdot 2^k = 2^{k+1}$. Hence, from the definition of M_{k+1}, we have confirmed what we stated above.

Next, we need to show that each row of M_{k+1} is obtained from a certain row of M_k by the above described replacement. Let $r_i = [s_{i1}^{(k+1)}, s_{i2}^{(k+1)}, \cdots, s_{i,k+1}^{(k+1)}]$ be the i^{th} row of M_{k+1}. Then, from the definition of M_{k+1} and Lemma 3, $\sum_{q=1}^{k+1} 2^{k+1-s_{iq}^{(k+1)}} = 2^{k+1}$ and $1 \leq s_{i1}^{(k+1)} \leq s_{i2}^{(k+1)} \leq \cdots \leq s_{ik}^{(k+1)} \leq s_{i,k+1}^{(k+1)} \leq k$. By Lemma 2, $k+1-s_{ik}^{(k+1)} = k+1-s_{i,k+1}^{(k+1)}$ or $s_{ik}^{(k+1)} = s_{i,k+1}^{(k+1)}$. Thus $2^{k+1} = \sum_{q=1}^{k+1} 2^{k+1-s_{iq}^{(k+1)}} = \sum_{q=1}^{k-1} 2^{k+1-s_{iq}^{(k+1)}} + 2^{k+2-s_{ik}^{(k+1)}}$. Since $k+1-s_{iq}^{(k+1)} \geq 1$ for $q = 1, 2, \cdots, k$, we thus have that $2^k = \sum_{q=1}^{k-1} 2^{k-s_{iq}^{(k+1)}} + 2^{k+1-s_{ik}^{(k+1)}} = \sum_{q=1}^{k-1} 2^{k-s_{iq}^{(k+1)}} + 2^{k-(s_{ik}^{(k+1)}-1)}$.

Hence, after a suitable rearrangement of the entries, $[s_{i1}^{(k+1)}, \cdots, s_{i,k-1}^{(k+1)}, s_{ik}^{(k+1)}-1]$ will be a row in M_k, that is, $[s_{i1}^{(k+1)}, \cdots, s_{i,k-1}^{(k+1)}, s_{ik}^{(k+1)}-1] = [s_{p\sigma(1)}^{(k)}, \cdots s_{p,\sigma(k-1)}^{(k)}, s_{p,\sigma(k)}^{(k)}]$ for some p and some permutation σ on the set $\{1, 2, \cdots, k\}$.

By noting that $s_{ik}^{(k+1)} = s_{p,\sigma(k)}^{(k)} + 1$ and $s_{ik}^{(k+1)} = s_{i,k+1}^{(k+1)}$, we can thus conclude that r_i is obtained from the $p^{th}-row$ of M_k by replacing the entry $s_{p,\sigma(k)}^{(k)}$ by the matrix $[s_{p,\sigma(k)}^{(k)}+1, s_{p,\sigma(k)}^{(k)}+1]$ and followed by a suitable rearrangement of the entries.

As a result of Corollary 4 and Theorem 5, we can easily exhibit the matrices M_k. For example, $M_2 = [1,1], M_3 = [1,2,2], M_4 = \begin{pmatrix} 1 & 2 & 3 & 3 \\ 2 & 2 & 2 & 2 \end{pmatrix}$, and $M_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 4 \\ 1 & 3 & 3 & 3 & 3 \\ 2 & 2 & 2 & 3 & 3 \end{pmatrix}$.

LEMMA 6. Let each of m, m' and t denote a positive integer. Then $2^m \equiv 2^{m'} \, mod(2^t - 1)$ if and only if $m \equiv m' \, mod\, t$.

PROOF. Assume $m \geq m'$. Suppose $m \equiv m' \, mod\, t$. Then, $m = m' + kt$ for some integer $k \geq 0$. Thus $2^m - 2^{m'} = 2^{m'+kt} - 2^{m'} = 2^{m'}(2^{kt} - 1)$. Now $2^t - 1 | 2^{kt} - 1$ and so $2^m \equiv 2^{m'} \, mod(2^t - 1)$. Conversely, suppose $2^m \equiv 2^{m'} \, mod(2^t - 1)$. Then $2^t - 1 | 2^m - 2^{m'} = 2^{m'}(2^{m-m'} - 1)$. Since gcd $(2^t - 1, 2^{m'}) = 1$, we thus have that $2^t - 1 | 2^{m-m'} - 1$. Hence $t | m - m'$ and therefore $m \equiv m' \, mod\, t$.

THEOREM 7. Let $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$, where $k \geq 2$, and each m_i is a nonnegative integer. Also, let t denote an integer ≥ 2. Then $2^t - 1 | n - 1$ if and only if

$$t | gcd(m_{\sigma(1)} + s_{i1}^{(k)}, m_{\sigma(2)} + s_{i2}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)})$$

for some i and some permutation σ on the set $\{1, 2, \cdots, k\}$, where $[s_{i1}^{(k)}, s_{i2}^{(k)}, \cdots, s_{ik}^{(k)}]$is the i^{th} row of M_k.

PROOF. Suppose there exists a row i in M_k and a permutation σ on the set $\{1, 2, \cdots, k\}$ such that gcd $(m_{\sigma(1)} + s_{i1}^{(k)}, m_{\sigma(2)} + s_{i2}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)}) = d$ is divisible by the integer $t, t \geq$

2. Let q denote a positive integer such that $qt \geq k$. Then $m_{\sigma(j)} \equiv qt - s_{ij}^{(k)} \, mod \, t$ for $j = 1, 2, \cdots, k$. Hence, by Lemma 6, we have that $n - 1 = 2^{m_{\sigma(1)}} + 2^{m_{\sigma(2)}} + \cdots + 2^{m_{\sigma(k)}} - 1 \equiv 2^{qt - s_{i1}^{(k)}} + 2^{qt - s_{i2}^{(k)}} + \cdots + 2^{qt - s_{ik}^{(k)}} - 1 \, mod(2^t - 1)$. Now, from the definition of the matrices M_k, we have that $2^{k - s_{i1}^{(k)}} + 2^{k - s_{i2}^{(k)}} + \cdots + 2^{k - s_{ik}^{(k)}} = 2^k$. Multiplying both sides by 2^{qt-k} gives $2^{qt - s_{i1}^{(k)}} + 2^{qt - s_{i2}^{(k)}} + \cdots + 2^{qt - s_{ik}^{(k)}} = 2^{qt}$. Hence $n - 1 \equiv 2^{qt} - 1 \, mod(2^t - 1)$. Since $2^t - 1 | 2^{qt} - 1$, we thus have that $2^t - 1 | n - 1$.

Next, assume $2^t - 1 | n - 1$, where t is an integer ≥ 2. Also, suppose $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$, where each m_i is a nonnegative integer. We want to show that $t | gcd(m_{\sigma(1)} + s_{i1}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)})$ for some permutation σ and some row i of M_k. We will proceed by induction on k.

Suppose $k = 2$ and $n = 2^{m_1} + 2^{m_2}$. Let $m_1 \equiv m_1' \, mod \, t$ and $m_2 \equiv m_2' \, mod \, t$, where $0 \leq m_1', m_2' \leq t - 1$. Then, by Lemma 6, $n \equiv 2^{m_1'} + 2^{m_2'} \, mod \, (2^t - 1)$. If $m_1' \neq m_2'$, then $2^{m_1'} + 2^{m_2'} - 1 \leq 2^{t-1} + 2^{t-2} - 1 < 2^{t-1} + 2^{t-1} - 1 = 2^t - 1$ and this is a contradiction since $2^t - 1 | 2^{m_1'} + 2^{m_2'} - 1$. Hence $m_1' = m_2'$ and $0 \equiv n - 1 \equiv 2^{m_1' + 1} - 1 \, mod \, (2^t - 1)$. Thus $2^t - 1 | 2^{m_1'+1} - 1$ which implies that $t | m_1' + 1$. Since $1 \leq m_1' + 1 \leq t$, we can conclude that $m_1' + 1 = t$. Thus $m_1' = m_2' = t - 1$ and consequently $m_1 + 1 \equiv m_2 + 1 \equiv 0 \, mod \, t$. Therefore $t | gcd(m_1 + 1, m_2 + 1) = gcd(m_1 + s_{11}^{(2)}, m_2 + s_{12}^{(2)})$ from the definition of M_2.

Now suppose $k > 2, n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$, and $2^t - 1 | n - 1$, where $t \geq 2$. Let $m_i \equiv m_i' \, mod \, t$ for $i = 1, 2, \cdots, k$, where $0 \leq m_i' \leq t - 1$. We claim that the numbers m_i' cannot be all distinct. For, suppose that they were all distinct. Then $2^{m_1'} + 2^{m_2'} + \cdots + 2^{m_k'} - 1 \leq 2^{t-1} + 2^{t-2} + \cdots + 2^{t-k} - 1 < 2^t - 1$. Now, by Lemma 6, $m_i \equiv m_i' \, mod \, t$ implies that $2^{m_i} \equiv 2^{m_i'} \, mod \, (2^t - 1)$ for $i = 1, 2, \cdots, k$. Thus $2^t - 1 | 2^{m_1'} + 2^{m_2'} + \cdots + 2^{m_k'} - 1$ and this contradicts the above statement that $2^{m_1'} + 2^{m_2'} + \cdots + 2^{m_k'} - 1 < 2^t - 1$. Hence there exists an ℓ such that $m_\ell' = m_{\ell+1}'$. For convenience, we will assume $\ell = k - 1$. Then $2^{m_1'} + 2^{m_2'} + \cdots + 2^{m_k'} - 1 = 2^{m_1'} + 2^{m_2'} + \cdots + 2^{m_{k-2}'} + 2^{m_{k-1}' + 1} - 1$. Now, by the induction hypothesis there is a pemutation σ on the set $\{1, 2, \cdots, k - 1\}$ and a row i in M_{k-1} such that $t | gcd(m_{\sigma(1)}' + s_{i1}^{(k-1)}, \cdots, m_{\sigma(j)}' + 1 + s_{ij}^{(k-1)}, \cdots, m_{\sigma(k-1)}' + s_{i,k-1}^{(k-1)})$ where $\sigma(j) = k - 1$. Since $m_{\sigma(1)} \equiv m_{\sigma(1)}' \, mod \, t, \cdots, m_{\sigma(k-1)} \equiv m_{\sigma(k-1)}' \, mod \, t$, we thus see that $t | gcd(m_{\sigma(1)} + s_{i1}^{(k-1)}, \cdots, m_{\sigma(j)} + 1 + s_{ij}^{(k-1)}, \cdots, m_{\sigma(k-1)} + s_{i,k-1}^{(k-1)})$ Now recalling that $m_{k-1}' = m_k'$ implies that $m_{k-1} + 1 + s_{ij}^{(k-1)} \equiv m_k + 1 + s_{ij}^{(k-1)} \, mod \, t$, we finally obtain that $t | gcd(m_{\sigma(1)} + s_{i1}^{(k-1)}, \cdots, m_{k-1} + 1 + s_{ij}^{(k-1)}, m_k + 1 + s_{ij}^{(k-1)}, \cdots, m_{\sigma(k-1)} + s_{i,k-1}^{(k-1)})$. This completes the proof since $\{m_{\sigma(1)}, \cdots, m_{k-1}, m_k, \cdots, m_{\sigma(k-1)}\}$ is a rearrangement of $\{m_1, m_2, \cdots, m_k\}$ and $[s_{i1}^{(k-1)}, \cdots, s_{i,j-1}^{(k-1)}, 1 + s_{ij}^{(k-1)}, 1 + s_{ij}^{(k-1)}, s_{i,j+1}^{(k-1)}, \cdots, s_{i,k-1}^{(k-1)}]$ is, on being rearranged in ascending order, a certain row of the matrix M_k which is obtained from the i^{th} row of M_{k-1} by replacing the j^{th} entry by the 1×2 matrix $[1 + s_{ij}^{(k-1)}, 1 + s_{ij}^{(k-1)}]$.

4. MAIN RESULT.

THEOREM 8. Let k denote an integer ≥ 2 and let $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$, where each m_i is a nonnegative integer. Also, let C denote the set such that $R \in C$ if and only if R is a ring of characteristic two and $x^n = x$ for each $x \in R$. Then the following two statements are equivalent.

1) Each member in C is boolean.
2) $gcd(m_{\sigma(1)} + s_{i1}^{(k)}, m_{\sigma(2)} + s_{i2}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)}) = 1$ for each permutation σ on the set $\{1, 2, \cdots, k\}$ and for each row $[s_{i1}^{(k)}, s_{i2}^{(k)}, \cdots, s_{ik}^{(k)}]$ in M_k.

PROOF. Suppose each member in C is boolean. Then, by Theorem 1, there does not exist an integer $t \geq 2$ such that $2^t - 1 | n - 1$. Hence, by Theorem 7, if $t \geq 2$, then $t \nmid gcd(m_{\sigma(1)} + s_{i1}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)})$ for each σ and each i. Thus $gcd(m_{\sigma(1)} + s_{i1}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)}) = 1$ for each i and σ.

Conversely, if $gcd(m_{\sigma(1)} + s_{i1}^{(k)}, \cdots, m_{\sigma(k)} + s_{ik}^{(k)}) = 1$ for each i and σ, then, by Theorem 7,

$2^t - 1 \nmid n - 1$ for each integer $t \geq 2$. Hence, by Theorem 1, R is boolean for each $R \in C$.

5. EXAMPLES ILLUSTRATING THEOREM 8.

LEMMA 9. Let R denote a ring and let $x \in R$ such that $x^n = x$ for some integer $n \geq 2$. If each of h and k is a positive integer such that $h \equiv k \mod (n-1)$, then $x^h = x^k$.

This result can be obtained easily by induction, see [1].

LEMMA 10. Let R denote a J-ring of characteristic two and suppose n is a positive integer ≥ 2. The following two statements are equivalent.

1) $x^n = x$ for each $x \in R$.

2) $x^{2n-1} = x$ for each $x \in R$.

PROOF. Suppose (1) holds. Then (2) is immediate by Lemma 9. Next, suppose $x^{2n-1} = x$ for each $x \in R$. Then $x^{2n} = x^2$ and thus $(x + x^n)^2 = x^2 + x^{2n} = 0$ since R is of characteristic two. Hence $x^n = x$ since a J-ring does not contain non-zero nilpotent elements.

THEOREM 11. Let R denote a ring of characteristic two. Suppose each of s and t is a positive integer with $s \neq t$ and $gcd(s,t) = 1$. If $x = x^{2^s} = x^{2^t}$ for each $x \in R$, then R is boolean.

PROOF. We may assume that $s > 1$. Then $x = x^{2^s} = xx^{2^s-1} = x^{2^t}x^{2^s-1} = x^{2^t+2^s-1} = x^{2(2^{t}-1+2^{s}-1)-1}$ for each $x \in R$. Hence, by Lemma 10, $x = x^{2^{t}-1+2^{s}-1}$ for each $x \in R$. Now $M_2 = [1,1]$ and $gcd(t-1+1, s-1+1) = gcd(t,s) = 1$. Consequently, by Theorem 8, we have that R is boolean.

The following examples illustrate the use of some of the preceding theorems.

EXAMPLE 1. Let R denote a ring of characteristic two such that $x^{595} = x$ for each $x \in R$. Since $595 = 2(298) - 1$ and $x^{595} = x$ for each $x \in R$ is equivalent, by Lemma 10, to $x^{298} = x$ for each $x \in R$, we can thus apply our results to $x^{298} = x$. Now $298 = 2^1 + 2^8 + 2^5 + 2^3$. Using the matrix M_4 and applying Theorem 8, we obtain $gcd(1 + s_{11}^{(4)}, 8 + s_{12}^{(4)}, 5 + s_{13}^{(4)}, 3 + s_{14}^{(4)}) = gcd(1+1, 8+2, 5+3, 3+3) = gcd(2,10,8,6) = 2 \neq 1$. Hence R is not necessarily boolean.

EXAMPLE 2. Let m denote a nonnegative integer. Let R denote a ring of characteristic two and suppose $x^n = x$ for each $x \in R$, where $n = 2^m + 2^{m+1} + 2^{m+2}$. Take $M_3 = [1,2,2]$. Now $gcd(m+1, m+1+2, m+2+2) = 1, gcd(m+2+1, m+1+2, m+2) = 1$,and $gcd(m+1+1, m+2+2, m+2) = gcd(m+2, m+4)$. Thus, by Theorem 8, R is boolean if $gcd(m+2, m+4) = 1$, that is, if m is odd, and not necessarily boolean if m is even.

REFERENCES

1. AYOUB, R. and AYOUB, C. On commutativity of rings, Amer. Math. Monthly, 71, (1964), 267-271.

2. BATBEDAT, A. Anneaux d'order n, Rev.Roumaine Math.Pures Appl., 16, (1971), 1305-1311.

3. JACOBSON , N. Structure of rings, Amer. Math. Soc. Colloq. Publ., New York, 37, (1956).

4. MACHALE, D. A remark on boolean rings, Mathematics Magazine, 63, (1990), 248-249.

5. SHIUE, J. S. and CHAO, W.M. On boolean rings, Yokohama Math. J., 24, (1976), 93-96.