Can. J. Math., Vol. XXVIII, No. 1, 1976, pp. 94–103

# FINITE RINGS IN WHICH 1 IS A SUM OF TWO NON-*p-th* POWER UNITS

DAVID JACOBSON

**Introduction.** Let $R$ be a finite ring with 1 and let $R^*$ denote the group of units of $R$. Let $p$ be a prime number. In this paper we consider the question of whether there exist $a$, $b$ in $R^*$ such that $a$ and $b$ are non-$p$-th powers whose sum is 1. If such units $a$, $b$ exist in $R$, we say that $R$ is an $N(p)$-ring. Of course if $p$ does not divide $|R^*|$, the order of $R^*$, then every element in $R^*$ is a $p$th power.

Let $J$ denote the Jacobson radical of $R$. Hence $R/J$ is a direct product of full matrix rings over finite fields. If the two-element field occurs as a factor in $R/J$, then clearly 1 cannot be written as a sum of two units in $R$. On the other hand, if the two-element field does not occur in $R/J$, then it follows from [**3**, Theorem 11] that every element of $R$ is a sum of two units. So henceforth we assume that $R$ is a ring of this type.

We say that $R$ is an $N$-ring if $R$ is an $N(p)$-ring for all primes $p$ dividing $|R^*|$. For example, it is shown that a ring of one of the following kinds is an $N$-ring, namely a commutative ring, or a ring of odd order, or the ring $F_n$ of all $n \times n$ matrices over a finite field $F$ where $|F| > 2$. However if $|F| = 2$ and $p$ divides $|F_n^*|$, then $F_n$ is an $N(p)$-ring except if the order of $2 (\mathrm{mod}\, p)$ is $n - 1$ or $p = 2$ and $n = 2, 3, 5$ (see Theorem 2).

In Section 1 we consider finite commutative rings and in Section 2 we deal with finite semisimple rings. Section 3 is devoted to rings of odd order and finally in Section 4 we deduce additional results.

I wish to express my thanks to Professor G. Krause for his helpful comments.

**1. Commutative rings.** Let $R$ be a finite commutative ring and let $J$ be its Jacobson radical. We prove the following theorem.

THEOREM 1. *Let $R$ be a finite commutative ring such that the two-element field does not occur as a factor in $R/J$. Then $R$ is an $N$-ring.*

*Proof.* Let $p$ be any prime dividing $|R^*|$. We prove that $R$ is a $N(p)$-ring. Since $R$ is a direct product of local rings, we may assume that $R$ is a local ring with maximal ideal $J$. Let $F$ denote the finite field $R/J$. There exists an epimorphism $R^* \to F^*$ with kernel $1 + J$. As $|J|$ and $|F^*|$ are relatively prime, $R^*$ is isomorphic to the direct product of the groups $1 + J$ and $F^*$. Now let $S$ (resp. $N$) denote the set of $p$th (resp. non-$p$-th) powers in $R^*$ which are not in

Received January 8, 1975.
This research was supported in part by NRC grant A8749.

$1 + J$. Let $g : N \to R$ be the mapping defined by $g(a) = 1 - a$ for $a$ in $N$. Since $J$ is the set of all non-units in $R$, $g(N) \subseteq S \cup N$ and as $|N| = |g(N)|$, it suffices to prove that $|N| > |S|$. We distinguish the two cases $p||F^*|$ and $p||J|$.

First suppose that $p||F^*|$. Let $S_1$ be the subgroup of $p$-th powers in $F^*$. As every element in $1 + J$ is a $p$-th power,

$$|S| = |J|(|S_1| - 1) \text{ and } |N| = |J|(|F^*| - |S_1|).$$

Thus it suffices to prove that $|F^*| + 1 > 2|S_1|$. Let $f$ be the $p$th power map in $F^*$. Then $|F^*| = |\text{Ker} f||S_1|$ where $|\text{Ker} f| = p$ since $F^*$ is cyclic. Hence $|F^*| + 1 > 2|S_1|$, proving that $|N| > |S|$.

Assume now that $p||J|$. Let $S_0$ be the subgroup of $p$th powers in $1 + J$. As every element in $F^*$ is a $p$th power,

$$|S| = |S_0|(|F^*| - 1) \text{ and } |N| = (|J| - |S_0|)(|F^*| - 1).$$

Since $|F^*| - 1 > 0$, it suffices to show that $|J| > 2|S_0|$. Let $f_0$ be the $p$th power map in $1 + J$. Then $|J| = |\text{Ker} f_0||S_0|$ where $|\text{Ker} f_0| \geqq p$. Thus if $p > 2$, then $|N| > |S|$. So let $p = 2$. Suppose that $|\text{Ker} f_0| = 2$, that is, $1 + J$ has a unique element of order 2. Since $1 + J$ is an abelian 2-group, $1 + J$ is cyclic and hence $R^*$ is cyclic. Referring to the classification in [**2**], we see that $R$ is isomorphic to one of the following rings: $Z/(4)$, $F_0[x]/(x^m)$ where $F_0 = Z/(2)$ and $m = 2$ or $3$, or $Z[x]/(4, 2x, x^2 - 2)$. However each of these rings has a residue field of order 2, contrary to our hypothesis. Hence $|\text{Ker} f_0| > 2$ and again $|N| > |S|$, completing the proof.

**2. Semisimple rings.** Let $n$ be a positive integer and $F$ a finite field. As usual, we let $F_n$ denote the ring of all $n \times n$ matrices with entries in $F$.

THEOREM 2. *Let $F$ be a finite field.*
(1) *If $|F| > 2$, then $F_n$ is an $N$-ring.*
(2) *If $|F| = 2$ and $p$ divides $|F_n^*|$, then $F_n$ is an $N(p)$-ring except if*
(a) *$p|2^{n-1} - 1$ and $n - 1$ is the least positive integer with this property or*
(b) *$p = 2$ and $n = 2, 3, 5$.*

The proof of the theorem is preceded by the following lemma.

LEMMA 1. *Let $F$ be a finite field of characteristic $p$. Let $A$ be a matrix in $F_n$ whose minimum polynomial is $f(x)$. If $f(x)$ and $f'(x)$ are relatively prime, then $A$ is a $p$th power. Conversely if $A$ is a $p$th power and $f(x)$ has degree $n$, then $f(x)$ and $f'(x)$ are relatively prime.*

*Proof.* Let $F[A]$ denote the $F$-subalgebra generated by $A$. We prove that $f(x)$ and its derivative $f'(x)$ are relatively prime if and only if $A$ is a $p$th power in $F[A]$.

Let $f(x)$ and $f'(x)$ be relatively prime. It follows that

$$f(x) = f_1(x) \ldots f_m(x)$$

https://doi.org/10.4153/CJM-1976-011-6 Published online by Cambridge University Press

where $f_1, \ldots, f_m$ are distinct monic irreducibles in $F[x]$. Hence $F[A]$ is isomorphic to the direct product of the finite fields

$$F[x]/(f_1), \ldots, F[x]/(f_m),$$

each of characteristic $p$ and thus $(F[A])^p = F[A]$.

Conversely let $A = B^p$ for $B$ in $F[A]$. Since $F[A]$ is isomorphic to $F[x]/(f(x))$ where $A \to x + (f(x))$, there exist $g(x)$ and $h(x)$ in $F[x]$ such that

$$x - [g(x)]^p = f(x)h(x).$$

Differentiating each side yields that $1 = f(x)h'(x) + f'(x)h(x)$, proving that $f(x)$ and $f'(x)$ are relatively prime.

Finally suppose that $A = B^p$ where $B$ is in $F_n$ and $f(x)$ has degree $n$. To prove that $f(x)$ and $f'(x)$ are relatively prime, it suffices to show that $B \in F[A]$. Now $F[A] \subseteq F[B]$ and thus $|F[A]| \leqq |F[B]|$, that is $|F|^n \leqq |F|^{n_1}$ where $n_1$ is the degree of the minimum polynomial of $B$. However $n_1 \leqq n$ and hence $F[A] = F[B]$, completing the proof of the lemma.

Note that if $A$ is a unit in $F_n$ such that $p$ divides $|A|$ and $f(x)$ is of degree $n$, then $A$ is not a $p$th power in $F_n$.

We also remark that Lemma 1 does not always hold if $\deg f(x) < n$. For let $n = p^2$ and let $B$ be a matrix in $F_n$ whose minimum polynomial is $(x - \alpha)^n$ where $\alpha$ is in the prime subfield of $F$. Then $A = B^p$ has minimum polynomial $f(x) = (x - \alpha)^p$, whence $f'(x) = 0$.

We now return to the proof of the theorem. Let $|F| = q$. It is well known that

$$|F_n^*| = q^{(n-1)n/2}(q^n - 1) \ldots (q - 1).$$

Let $p$ be a prime dividing $|F_n^*|$.

We first assume that $p = \text{char. } F$, so that $n \geqq 2$. Let $q > 2$ and choose $\alpha$ in $F$, $\alpha \neq 0, 1$. Let $A = \alpha I_n + E$, where $E$ is the matrix with 1 in the $(i, i + 1)$ entry and zeros elsewhere. Set $B = I_n - A$. Then the minimum polynomials of $A$ and $B$ are respectively $(x - \alpha)^n$ and $(x - (1 - \alpha))^n$. Hence by Lemma 1, $A$ and $B$ are non-$p$-th power units in $F_n$ whose sum is $I_n$.

Now let $q = 2$, so that $p = 2$. We prove that $F_n$ is an $N(2)$-ring if and only if $n = 4$ or $n \geqq 6$.

Suppose that $n = 2m$ where $m \geqq 2$. Let $A$ in $F_n$ be the companion matrix of $f(x) = (x^2 + x + 1)^m$ and let $A + B = I_n$. Thus the minimum polynomial of $B$ is $f(x + 1) = f(x)$ and by Lemma 1, $A$ and $B$ are non-square units in $F_n$.

Now let $n = 2m + 3$ where $m \geqq 2$. Let $A$ in $F_n$ be the companion matrix of

$$f(x) = (x^2 + x + 1)^m(x^3 + x + 1)$$

and let $A + B = I_n$. Thus the minimum polynomial of $B$ is

$$f(x + 1) = (x^2 + x + 1)^m(x^3 + x^2 + 1)$$

and again by the lemma, $A$ and $B$ are non-square units in $F_n$.

This proves that $F_n$ is an $N(2)$-ring for $n = 4$ or $n \geqq 6$.

Assume now that $A$ is a non-square unit in $F_n$ where $n$ is 2, 3 or 5. Let $f(x)$ be the minimum polynomial of $A$. Since $f(x)$ and $f'(x)$ are not relatively prime and $x \nmid f(x)$, it is easy to verify that $x + 1$ is a divisor of $f(x)$. Hence if $A + B = I_n$, then $B$ is a non-unit in $F_n$ since $x$ divides $f(x + 1)$, the minimum polynomial of $B$.

Now suppose that $p$ divides $|F_n^*|$ and $p \neq$ char. $F$. Let $k$ be the least integer in $\{1, \ldots, n\}$ such that $p|(q^k - 1)$. Let $f_0(x)$ be a monic irreducible in $F[x]$ of degree $k$ and let $A_0$ in $F_k$ be the companion matrix of $f_0(x)$. Let $\langle A_0 \rangle_k$ denote the $F$-subalgebra of $F_k$ generated by $A_0$. Thus $\langle A_0 \rangle_k$ is a field of order $q^k$. Hence there exist non-$p$-th power units $A_1$, $A_2$ in $\langle A_0 \rangle_k$ such that $A_1 + A_2 = I_k$. Moreover the subfield $\langle A_1 \rangle_k$ is of order $q^{k_1}$. However if $k_1 < k$, then $p \nmid (q^{k_1} - 1)$, which contradicts that $A_1$ is not a $p$th power in $\langle A_1 \rangle_k$. Hence the minimum polynomial $f_1(x)$ of $A_1$ is of degree $k$ and irreducible in $F[x]$. It follows that $A_1$ is not a $p$th power in $F_k$. Similarly $A_2$ is not a $p$th power in $F_k$. Thus if $k = n$, then $F_n$ is an $N(p)$-ring.

So let $1 \leqq k < n$. Suppose that there exists a monic irreducible $g_1(x)$ in $F[x]$ of degree $n - k$ such that $f_1(x)$ and $g_1(x)$ are relatively prime and neither $x$ nor $x - 1$ divides $g_1(x)$. Then we claim that $F_n$ is a $N(p)$-ring. For let $B_1$ in $F_{n-k}$ be the companion matrix of $g_1(x)$. Let

$$A = \left[\begin{array}{c|c} A_1 & 0 \\ \hline 0 & B_1 \end{array}\right]$$

belong to $F_n$. Clearly there is a monomorphism of the ring $\langle A \rangle_n$ into the direct product of the fields $\langle A_1 \rangle_k$ and $\langle B_1 \rangle_{n-k}$ where $A \rightarrow (A_1, B_1)$. Thus $A$ is not a $p$-th power in $\langle A \rangle_n$. However the minimum polynomial of $A$ is $f_1(x)g_1(x)$ of degree $n$ and hence $A$ is not a $p$th power in $F_n$. Now let $A + B = I_n$. A similar argument shows that $B$ is not a $p$th power in $F_n$. Since $A$ and $B$ are units in $F_n$, the claim is established.

It is easy to see that there exists a $g_1(x)$ with the above properties except for the cases (i) $q = 3$, $n = 2$, $k = 1$, (ii) $q = 2$, $n = 4$, $k = 2$ and (iii) $q = 2$, $n - k = 1$.

We now consider these remaining cases.

(i) Let $q = 3$, $n = 2$, $k = 1$, whence $p = 2$. Let $f(x) = x^2 - x - 1$. As $f(1 - x) = f(x)$, it is clear that there exist $A$, $B$ in $F_2$ such that $A + B = I_2$ and $f(x)$ is their minimum polynomial. Since $f(x^2) = x^4 - x^2 - 1$ is irreducible in $F[x]$, it follows that $A$ and $B$ are non-square units in $F_2$.

(ii) Let $q = 2$, $n = 4$, $k = 2$, whence $p = 3$. Clearly we may choose $A$, $B$ in $F_4$ such that $A + B = I_4$ and $x^2 + x + 1$ is their minimum polynomial. However $x^6 + x^3 + 1$ is irreducible in $F[x]$ and thus $A$ and $B$ are non-cube units in $F_4$.

(iii) Finally let $q = 2$, $k = n - 1$. As $p|2^{n-1} - 1$, $n \geqq 3$. Let $A$ be any non-$p$-th power unit in $F_n$. We show that $I_n - A$ is a non-unit in $F_n$. Let $f(x)$ be

https://doi.org/10.4153/CJM-1976-011-6 Published online by Cambridge University Press

the minimum polynomial of $A$. Thus

$$f(x) = f_1^{l_1} \dots f_s^{l_s}$$

where $f_1, \dots, f_s$ are distinct monic irreducibles in $F[x]$. Let $\langle A \rangle$ denote the $F$-subalgebra generated by $A$. Hence $\langle A \rangle$ is isomorphic to the direct product $R_1 \times \dots \times R_s$ where each

$$R_i = F[x]/(f_i^{l_i}).$$

However $R_i$ is a local ring whose residue field is isomorphic to $F[x]/(f_i)$. Thus letting $d_i$ denote the degree of $f_i$, we have

$$|R_i^*| = 2^{d_i(l_i-1)}(2^{d_i} - 1)$$

and

$$|\langle A \rangle^*| = |R_1^*| \dots |R_s^*|.$$

Since $A$ is not a $p$th power, $p$ divides $|\langle A \rangle^*|$ and as $p$ is prime to 2, we may suppose that $p|(2^{d_1} - 1)$. Thus $d_1 = n$ or $d_1 = n - 1$. If $d_1 = n$, then $p$ divides $(2^n - 1) - (2^{n-1} - 1)$, that is $p|2^{n-1}$, a contradiction. So $d_1 = n - 1$. However

$$d_1l_1 + \dots + d_sl_s \leqq n$$

and since $n > 2$, it follows that $f(x) = f_1$ or $f(x) = f_1f_2$. Let $g(x)$ be the characteristic polynomial of $A$. It is well known that $f(x)$ and $g(x)$ have the same irreducible factors. Thus $f(x) = f_1$ is impossible since $f_1$ contains no linear factor. Hence $f(x) = f_1f_2$ where $f_2$ is of degree 1. As $A$ is a unit, $f_2 = x + 1$. Now let $A + B = I_n$. Thus the minimum polynomial of $B$ is $f(x + 1) = xf_1(x + 1)$, so that $B$ is not a unit. This completes the proof of Theorem 2.

For example, if $|F| = 2$, then $F_3$ is neither an $N(2)$- nor an $N(3)$-ring, but $F_7$ is an $N$-ring.

Note that if $|F| = 2$ and $p$ is a fixed odd prime, then $F_n$ is an $N(p)$-ring for all $n \geqq m + 2$ where $m$ is the order of $2 (\text{mod } p)$.

A finite ring $R$ is semisimple if its radical $J = (0)$. By the Wedderburn theorem, $R$ is semisimple if and only if it is a direct product of finite simple rings $R_1, \dots, R_m$, where each $R_i$ is isomorphic to a matrix ring over a finite field.

THEOREM 3. *Let $R$ be a direct product of finite simple rings, $R_1, \dots, R_m$ such that $|R_i| > 2$ for $i = 1, \dots, m$.*

(i) *$R$ is an $N(p)$-ring if and only if some $R_i$ is an $N(p)$-ring.*

(ii) *If the center of each $R_i$ has more than two elements, then $R$ is an $N$-ring.*

*Proof.* (i) Let $R$ be an $N(p)$-ring. It follows that there exist units $a_i, b_i$ in some $R_i$ such that $a_i$ is not a $p$th power in $R_i$ and $a_i + b_i = 1$. If the center $F_i$ of $R_i$ is not the two-element field, then $R_i$ is a $N(p)$-ring by (1) of Theorem 2. On the other hand, let $|F_i| = 2$. Since $b_i$ is a unit in $R_i$, the proof of Theorem 2 shows that neither (a) nor (b) applies to $p$. Hence $R_i$ is an $N(p)$-ring. The converse is clear.

(ii) The result follows immediately from (1) of Theorem 2 and part (i).

## 3. Rings of odd order.

In the sequel we shall often use the next result.

LEMMA 2. *Let $K$ be an ideal of the finite ring $R$ where $K \subseteq J$, the Jacobson radical of $R$.*

(i) *If $p$ is a prime divisor of $|R^*|$, then $p$ divides $|K|$ or $p$ divides $|(R/K)^*|$.*

(ii) *If $R/K$ is an $N(p)$-ring, then $R$ is an $N(p)$-ring.*

*Proof.* Since units lift (mod $J$), the natural map $R \rightarrow R/K$ induces an epimorphism $R^* \rightarrow (R/K)^*$ with kernel $1 + K$. Hence (i) and (ii) follow.

In the remainder of this section we assume that $R$ is a ring of odd order.

THEOREM 4. *Let $R$ be a ring of odd order. Then $R$ is an $N$-ring.*

*Proof.* Since a finite ring is a direct product of rings of prime power order, we may assume that $|R| = p_0^m$ where $p_0$ is an odd prime. Thus $R/J$ is a direct product of matrix rings over finite fields of characteristic $p_0$ and by Theorem 3, $R/J$ is an $N$-ring. If $p$ is a prime divisor of $|R^*|$ and $p \neq p_0$, then $p$ divides $|(R/J)^*|$ and hence $R$ is an $N(p)$-ring by Lemma 2. Thus it remains to prove that if $p_0$ divides $|R^*|$, then $R$ is an $N(p_0)$-ring. Of course if $p_0$ divides $|(R/J)^*|$, then $R$ is an $N(p_0)$-ring.

So we can assume that $p_0$ divides $|R^*|$ but $p_0$ does not divide $|(R/J)^*|$. It follows that $J \neq (0)$ and $R/J$ is a direct product of finite fields each of characteristic $p_0$.

We first consider the case that $R$ is a ring of characteristic $p_0$. Let $F_0$ denote the subfield of $R$ of order $p_0$ generated by 1. Since $R$ is a finite dimensional algebra over $F_0$, the Wedderburn Factor Theorem [**1**, p. 471] yields that $R = S + J$ where $S$ is a subring isomorphic to $R/J$ and $S \cap J = 0$. Thus $F_0 \subseteq S$ and we note that if $a \in S$ and $a^{p_0} = \alpha \in F$, then $a = \alpha$. Now as $J$ is nilpotent and non-zero, there exists $x$ in $J$ such that $x$ is not in the ideal $J^{p_0}$. Let $\alpha \in F_0$. We claim that $\alpha + x$ is not a $p_0$th power in $R$. For let

$$(a + y)^{p_0} = \alpha + x$$

where $a \in S$ and $y \in J$. Then $a^{p_0} + y_1 = \alpha + x$ where $y_1 \in J$. Thus $a^{p_0} = \alpha$ and as noted $a = \alpha$. However $\alpha$ is in the center of $R$ and char. $R = p_0$, so that

$$(\alpha + y)^{p_0} = \alpha^{p_0} + y^{p_0}.$$

Hence $y^{p_0} = x$, which contradicts that $x \notin J^{p_0}$ and establishes the claim. As $p_0 > 2$ there exist units $\alpha$, $\beta$ in $F_0$ such that $\alpha + \beta = 1$ and hence $\alpha + x$ and $\beta - x$ are non-$p_0$-th power units in $R$ whose sum is 1.

Now let $R$ not be of characteristic $p_0$. The ideal $p_0R$ is contained in $J$. Suppose that $p_0R$ is not equal to $J$. Let $R_1 = R/p_0R$. Then the Jacobson radical of $R_1$ is $J_1 = J/p_0R$ and $p_0$ divides $|R_1^*|$. Since $R_1/J_1$ is isomorphic to

$R/J$ and char. $R_1 = p_0$, the preceding case shows that $R_1$ is an $N(p_0)$-ring and hence by Lemma 2, $R$ is an $N(p_0)$-ring.

Thus we may suppose that $J = p_0R$. Assume that $J^2 = (0)$. We prove that $R$ is a commutative ring. As $R/J$ is a direct product of finite fields, there exists an integer $r > 1$ such that $a^r - a \in J$ for all $a$ in $R$. By [**4**, Theorem 3.2.3, p. 81], it suffices to prove that $J$ is contained in the center of $R$. Let $x \in J$ and let $a \in R$. Then $x = p_0b$ where $b \in R$ and hence $ax - xa = p_0(ab - ba)$. However $ab - ba \in J$ and $(0) = J^2 = p_0{}^2R$, so that $ax = xa$. Thus $R$ is commutative and by Theorem 1, $R$ is an $N(p_0)$-ring.

Finally let $J^2 \neq (0)$. Since $J$ is nilpotent, $J^2 \neq J$. Let $R_2 = R/J^2$. The radical of $R_2$ is $J_2 = J/J^2$ and $p_0$ divides $|R_2{}^*|$. Since $J_2 = p_0R_2$ and $J_2{}^2 = (0)$, the above argument shows that $R_2$ is commutative. Hence $R_2$ is an $N(p_0)$-ring and by Lemma 2, $R$ is an $N(p_0)$-ring. This completes the proof of the theorem.

THEOREM 5. *A ring of odd order is an $N(2)$-ring.*

*Proof.* Let $R$ be a ring of odd order. Then $R/J$ is of odd order and hence $R/J$ is an $N$-ring by Theorem 4. However 2 divides $|(R/J)^*|$ and thus Lemma 2 yields that $R$ is an $N(2)$-ring.

## 4. Additional results.

THEOREM 6. *Let $R$ be a finite dimensional algebra over a finite field $F$ of characteristic $p_0 > 2$. Then $R$ is an $N$-ring.*

*Proof.* Let $m = \dim_F R$. Then $|R| = |F|^m$ and since $p_0$ is an odd prime, $R$ is of odd order. Thus by Theorem 4, $R$ is an $N$-ring.

THEOREM 7. *Let $R$ be a finite ring with Jacobson radical $J$.*

(1) *If the two-element field does not occur as a factor in $R/J$, then for $n \geqq 2$, $R_n$ is an $N(2)$-ring.*

(2) *If the two element field does not occur as a factor in the center of $R/J$, then for $n \geqq 2$, $R_n$ is an $N$-ring.*

(3) *If $R/J$ is a direct product of finite fields each having more than two elements, then for $n \geqq 2$, $R_n$ is an $N$-ring.*

*Proof.* Since a ring of odd order is both an $N$-ring and an $N(2)$-ring, it suffices to prove the theorem for the case that $|R|$ is a power of 2.

(1) Suppose that the two-element field does not occur as a factor in $R/J$. As $|R| = 2^m$, it follows that each factor in $R/J$ is of the form $F_k$ where $F$ is a field of characteristic 2 and $k > 1$ if $|F| = 2$. Now let $n \geqq 2$. The radical of $R_n$ is $J_n$ and

$$R_n/J_n \cong (R/J)_n.$$

Hence each factor in $R_n/J_n$ is of the form $F_{kn}$ where $kn = 4$ or $kn \geqq 6$ if $|F| = 2$, while $kn \geqq 2$ if $|F| > 2$. Thus by Theorem 2, each $F_{kn}$ is an $N(2)$-ring and hence $R_n$ is an $N(2)$-ring.

(2) Suppose that each factor in $R/J$ is of the form $F_k$ where $F$ is a field of characteristic 2 and $|F| > 2$. Let $n \geqq 2$. Then by (1), $R_n$ is an $N(2)$-ring. However by Theorem 3, $R_n/J_n$ is an $N$-ring. Since $|R| = 2^m$, it follows that $R$ is an $N$-ring.

(3) This is an immediate consequence of (2).

THEOREM 8. *Let $R$ be a finite commutative ring such that the two-element field does not occur as a factor in $R/J$. Then for all $n$, $R_n$ is an $N$-ring.*

*Proof.* For $n \geqq 2$, $R_n$ is an $N$-ring by Theorem 7(2), while $R$ itself is an $N$-ring by Theorem 1.

THEOREM 9. *Let $R$ be the ring of lower (upper) triangular matrices over a finite field $F$ where $|F| > 2$. Then for all $n$, $R_n$ is an $N$-ring.*

*Proof.* $R$ is a subring of $F_k$ for some $k$. Let $J$ be the radical of $R$. Then $R/J$ is a direct product of $k$ copies of $F$ and hence by Theorem 7(3), $R_n$ is an $N$-ring for $n \geqq 2$. We now prove that $R$ itself is an $N$-ring. We may take $k \geqq 2$. Let $p = \text{char. } F$. Since $R/J$ is an $N$-ring and $|R|$ is a power of $p$, it remains to prove that $R$ is an $N(p)$-ring. However the proof of Theorem 2 showed that there exist $A$, $B$ in $R$ such that $A + B = 1$ and $A$, $B$ are non-$p$-th power units in $F_k$. Hence $A$, $B$ are also non-$p$-th power units in $R$, which completes the proof.

We note that if $R$ is an $N$-ring, then $R_n$ is not always an $N$-ring. For $R = F_7$ is an $N$-ring where $F$ is the two-element field, but $R_2 \cong F_{14}$ is not an $N$-ring since $2^{13} - 1$ is a prime.

Raghavendran [**6**, Theorem 3] has shown that a finite local ring of prime characteristic $p_0$ whose radical $J$ satisfies $J^2 = (0)$ is isomorphic to the ring $R$ of all $n \times n$ matrices of the form

$$\begin{bmatrix} a_1 & b_2 & b_3 & \ldots & b_n \\ 0 & a_1^{s_2} & 0 & \ldots & 0 \\ 0 & 0 & a_1^{s_3} & \ldots & 0 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ 0 & 0 & 0 & \ldots & a_1^{s_n} \end{bmatrix}$$

where $a_1, b_2, \ldots, b_n$ range over the field of order $p_0^r$ and for $i = 2, \ldots, n$, $s_i = p_0^{t_i}$ for fixed integers $t_i$ with $1 \leqq t_i \leqq r$. Conversely for every choice of the integers $t_i$, $R$ is local of characteristic $p_0$ and its radical $J$ satisfies $J^2 = (0)$.

If $p_0 > 2$, then $R$ is an $N(p_0)$-ring by Theorem 4. However for $p_0 = 2$, $R$ is not always an $N(2)$-ring. Namely we prove the following.

THEOREM 10. *Let $R$ be the above ring of matrices where $p_0 = 2$ and $n \geqq 2$. Then $R$ is not an $N(2)$-ring if and only if $GCD(t_i, r) = 1$ for all $i$.*

*Proof.* The radical $J$ of $R$ consists of those matrices for which $a_1 = 0$. Also $R = F \oplus J$ where $F$ is the field consisting of those matrices for which all $b_i = 0$.

We shall identify $a_1$ in the field of order $2^r$ with

$$\operatorname{diag}(a_1, a_1^{s_2}, \ldots, a_1^{s_n}) \text{ in } F.$$

Let $Y_i$ be the matrix with 1 in the $(1, i)$ position and zeros elsewhere. Then $Y_2, \ldots, Y_n$ is a left $F$-basis for $J$ and

$$Y_i a = a^{s_i} Y_i$$

for $a$ in $F$ and all $i$. Let $x$ be an element in $R$. Then there exist unique elements $a_1, a_2, \ldots, a_n$ in $F$ such that

$$x = a_1 + a_2 Y_2 + \ldots + a_n Y_n.$$

Since $J^2 = (0)$,

$$x^2 = a_1^2 + a_2(a_1 + a_1^{s_2}) Y_2 + \ldots + a_n(a_1 + a_1^{s_n}) Y_n.$$

Now as $|F| = 2^r$, note that if $GCD(t, r) = 1$ and $a \in F$, then $a + a^{2^t} = 0$ only for $a = 0, 1$. It follows that if $GCD(t_i, r) = 1$ for all $i$, then every non-square unit of $R$ belongs to $1 + J$ and thus $R$ is not an $N(2)$-ring.

Conversely suppose that for some $i$, $GCD(t_i, r) > 1$. Then there exists $a_1$ in $F$ such that

$$a_1 + a_1^{2^t} = 0 \text{ and } a_1 \neq 0, 1.$$

Hence $x_1 = a_1^2 + Y_i$ is a non-square unit in $R$. Since char. $R = 2$, $x_1 + 1$ is also a non-square unit, which proves that $R$ is an $N(2)$-ring.

Theorem 10 provides an example of a ring $R$ such that $R/J$ is an $N$-ring but $R$ is not an $N$-ring.

We now give an example of an $N$-ring $R$ such that $R/J$ is not an $N$-ring. Let $S = F_2$ where $F$ is the two-element field. Let $x$ be an indeterminate over $S$ and let $R = S[x]/(x^2)$. We may identify $S$ as a subring of $R$ and moreover each element of $R$ can be written uniquely as

$$a + by \text{ where } a, b \in S \text{ and } y = x + (x^2).$$

Clearly $J = Sy$ and $R/J \cong S$. By Theorem 2, $S$ is an $N(3)$-ring but not an $N(2)$-ring. Thus as $|R^*| = (2^5)3$, we have only to show that $R$ is an $N(2)$-ring. Define

$$T(a + by) = \operatorname{trace}(b).$$

Then $T((a + by)^2) = 0$ since $(a + by)^2 = a^2 + (ab + ba)y$ and char. $R = 2$. Let $a_1$, $a_2$ be units in $S$ such that $a_1 + a_2 = 1$. Choose $b_0$ in $S$ such that $\operatorname{trace}(b_0) = 1$. Hence $a_1 + b_0 y$ and $a_2 + b_0 y$ are non-square units in $R$ whose sum is 1, that is $R$ is an $N(2)$-ring. This proves that $R$ is an $N$-ring.

Finally we deduce the following result which is well known for fields [**5**, Theorem 12, p. 15].

THEOREM 11. *Let R be a commutative local ring of odd order. Then for any units $a$, $b$ in $R$, the equation $ax^2 + by^2 = 1$ is solvable in $R$.*

*Proof.* Let $a$, $b$ be units in $R$. If $a$ or $b$ is a square, the result is immediate. So let $a$, $b$ be non-squares. By Theorem 4, there exist non-square units $a_1$, $b_1$ such that $a_1 + b_1 = 1$. However the index $[R^* : S] = 2$ where $S$ is the subgroup of squares in $R^*$. Hence $a^{-1}a_1 = x^2$ and $b^{-1}b_1 = y^2$ for $x$, $y$ in $R^*$, completing the proof.

REFERENCES


1. Carl Faith, *Algebra: rings, modules and categories I* (Springer-Verlag, New York, 1973).
2. R. Gilmer, *Finite rings having a cyclic multiplicative group of units*, Amer. J. Math., *85* (1963), 447–452.
3. Melvin Henriksen, *Two classes of rings generated by their units*, (to appear).
4. I. N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs, Number 15, 1968.
5. Irving Kaplansky, *Linear algebra and geometry* (Allyn and Bacon, Inc., Boston, 1969).
6. R. Raghavendran, *Finite associative rings*, Compositio Math., *21* (1969), 195–229.


*University of Manitoba,*
*Winnipeg, Manitoba*