Math. J. Okayama Univ. 30 (1988), 33−40

ON RINGS IN WHICH EVERY ELEMENT IS UNIQUELY EXPRESSIBLE AS A SUM OF A NILPOTENT ELEMENT AND A CERTAIN POTENT ELEMENT

YASUYUKI HIRANO, HISAO TOMINAGA and ADIL YAQUB

Throughout, R will represent a ring. Let P, N and N^* denote respectively the sets of potent elements, nilpotent elements, and elements which square to zero, of R. Given a positive integer n, we put $E_n = \{x \in R \mid x^n = x\}$; in particular, $E = E_2$.

For any subsets A, B of R, we define R to be A-B (resp. $[A$-$B]$) *representable* if each $x \in R$ can be written as $x = a+b$, where $a \in A$ and $b \in B$ (resp. $a \in A$, $b \in B$, and $[a, b] = ab-ba = 0$). In case each $x \in R$ can be written uniquely as $x = a+b$, where $a \in A$ and $b \in B$ (resp. $a \in A$, $b \in B$, and $[a, b] = 0$), we say that R is $(A$-$B)$ (resp. $\{A$-$B\}$) *representable.* Also, we define R to be A-B (resp. $[A$-$B]$) *orthogonal* if $ab = 0 = ba$ for any $a \in A$, $b \in B$ (resp. for any $a \in A$, $b \in B$ with $[a, b] = 0$).

In view of [8, Theorem 3 (1)], R is a periodic ring if and only if R is $[P$-$N]$ representable. Furthermore, by [2, Theorem 1 (3)] (see, also Theorem 1 below), R is $(P$-$N)$ representable if and only if $R = P \oplus N$; strictly speaking, both P and N are ideals of R and R is the direct sum of P and N. It is an open question whether the P-N representability implies the periodicity of R. Needless to say, if R is A-B orthogonal then R is $[A$-$B]$ orthogonal, and if R is E-N^* orthogonal then R is normal, that is, E is central.

The present paper treats $(P$-$N)$ representable rings, $\{P$-$N\}$ representable rings, $(E$-$N)$ representable rings and $\{E$-$N\}$ representable rings. We shall begin with some examples.

Examples. (1) Obviously, the $\{P$-$N\}$ representability implies the $[P$-$N]$ representability. But the converse need not be true. Let R be the commutative ring $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a, b \in \mathrm{GF}(3)\right\}$. Then $P = E_7$ and $R = P \cup N$. Hence R is $[P$-$N]$ representable, but not $\{P$-$N\}$ representable.

(2) Let R be the commutative ring $\mathbf{Z}/4\mathbf{Z}$. Then $P = E_3 \neq E$ and R is $(E$-$N)$ representable. But E is not an ideal, and R is not $(P$-$N)$ representable.

(3) Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, \ b \in \mathrm{GF}(2) \right\}$. Then $R = E \cup N$ is not $(E\text{-}N)$ representable

(4) Let $R = M_2(\mathrm{GF}(2))$. Then R is not $[E\text{-}N]$ representable, but $E\text{-}N$ representable.

Now, we shall state our main theorems.

Theorem 1. *The following are equivalent:*

1) *R is $(P\text{-}N)$ representable.*
2) *R is $[P\text{-}N]$ representable and $E\text{-}N^*$ orthogonal.*
3) *$R = P \oplus N$.*

Theorem 2. *The following are equivalent:*

1) *R is $\{P\text{-}N\}$ representable.*
2) *R is $[P\text{-}N]$ representable and $[E\text{-}N^*]$ orthogonal.*

Theorem 3. *The following are equivalent:*

1) *R is $\{E\text{-}N\}$ representable.*
2) *R is $[E\text{-}N]$ representable.*
3) *$x - x^2 \in N$ for every $x \in R$.*
4) *N is an ideal and R/N is a Boolean ring.*

Theorem 4. *The following are equivalent:*

1) *R is $(E\text{-}N)$ representable.*
2) *R is normal and $E\text{-}N$ representable.*
3) *R is normal, and $x - x^2 \in N$ for every $x \in R$.*
4) *R is normal, N is an ideal, and R/N is a Boolean ring.*

Theorem 5. *The following are equivalent:*

1) *R is $E\text{-}N^*$ orthogonal and $(E\text{-}N)$ representable.*
2) *R is $E\text{-}N^*$ orthogonal and $E\text{-}N$ representable.*
3) *R is $E\text{-}N^*$ orthogonal, and $x - x^2 \in N$ for every $x \in R$.*
4) *R is $E\text{-}N^*$ orthogonal, N is an ideal, and R/N is a Boolean ring.*
5) *$R = E \oplus N$; strictly speaking, both E and N are ideals of R and R is the direct sum of E and N.*

Proof of Theorem 1. This is essentially proved in [2, Theorem 1 (3)]. However, for the sake of completeness, we shall give the proof. Obviously

3) implies 1).

1) $\Rightarrow$ 2). In view of the uniqueness of the expression, we can easily see that R is normal. Observe that if $x = u + a$ with $u \in P$, $a \in N$ and $[u, a] = 0$, there exists $n > 1$ such that $x^n - x \in N$. Let e be an arbitrary (central) idempotent, and $a \in N^*$. Applying the above observation to $2e$, we get a positive integer k such that $ke = 0$. Hence $e + ea = (e + ea)^{k+1}$ is potent, and the uniqueness of its representation implies that $ea = 0$, and thus $EN^* = 0$. Furthermore, by induction, we can easily see that $PN = 0 = NP$. By making use of this fact and the P-N representability, we can prove that N is an ideal, and therefore for each $x \in R$ there exists $m > 1$ such that $x - x^m \in N$. Hence R is $[P$-$N]$ representable by [8, Theorem 3 (1)].

2) $\Rightarrow$ 3). Since $EN^* = 0 = N^*E$, we can easily see that R is normal, $EN = 0$ and N is an ideal (see 1) $\Rightarrow$ 2) above). Now, let I be the ideal of R generated by E, and x an arbitrary element in $I \cap N$. We write $x = e_1x_1 + \cdots + e_kx_k$ with some $e_i \in E$ and $x_i \in R$. As is well known, there exists a central idempotent e such that $ee_i = e_i$ $(i = 1, \cdots, k)$. Then $x = ex \in EN = 0$, and hence $I \cap N = 0$. Since $P \subseteq I$ and R is $[P$-$N]$ representable, this proves that $P = I$ and $R = P \oplus N$.

Corollary 1 ([7, Theorem 3]). *If R satisfies the identity $x^n y = xy^n$ $(n > 1)$, then $R = P \oplus N$.*

Proof. Obviously, R is E-N^* orthogonal. Since R satisfies the identity $x^{n+2} = x^{2n-1}$, R is $[P$-$N]$ representable by [8, Theorem 3 (1)]. Hence $R = P \oplus N$ by Theorem 1.

Proof of Theorem 2. 1) $\Rightarrow$ 2). Let $e \in E$, $a \in N^*$, and $[e, a] = 0$. Then there exists a positive integer k such that $ke = 0$. Hence $e + ea = (e + ea)^{k+1}$ is a potent element, and the uniqueness of the representation implies that $ea = 0$.

2) $\Rightarrow$ 1). By induction, we can easily see that if $e \in E$, $a \in N$ and $[e, a] = 0$ then $ea = 0$. Let x be an arbitrary element of R. Then there exists a positive integer k such that $x^{2k} = x^k$, by a theorem of Chacron [4]. As is easily seen, $x^{k+1} \in P$ and $x - x^{k+1} \in N$. Now, let $x = u + a$, where $u^{n+1} = u$ with some positive integer n, $a \in N$, and $[u, a] = 0$. Then $u^n \in E$ implies that $u^n a = 0$, and so $ua = 0$. Hence $x^{n+1} = u^{n+1} + a^{n+1} = u + a^{n+1}$, and therefore there exists an integer $m > k$ such that $x^{m+1} = u$. Since $[x, a] = 0$ and $x^k \in E$, we get $x^k a = 0$ and $x^m(x - x^{k+1}) = x^{m-k}x^k(x - x^{k+1}) = 0$.

Thus, $u = x^{m+1} = x^m(x^{k+1}+(x-x^{k+1})) = x^{k+m+1} = x^k(u+a) = x^{k+1}$.

Corollary 2. *If a ring R with 1 is $|P\text{-}N|$ representable, then R is a potent ring.*

Proof of Theorem 3. Obviously, 1) ⇒ 2) ⇒ 3), and 4) ⇒ 3).

3) ⇒ 1). More generally, we shall show that if x is an element of a ring R such that $(x-x^2)^r = 0$ then x can be written uniquely as $x = e+a$, where $e \in E$, $a \in N$, and $[e, a] = 0$. Actually, $e = \sum_{i=r+1}^{2r} x^i(1-x)^{2r-i}$ is an idempotent and $a = x-e$ is a nilpotent. Suppose $x = f+b$, where $f \in E$, $b \in N$, and $[f, b] = 0$. Then $[e, f] = 0 = [a, b]$. Hence $e-f = (e-f)^3$ and $e-f = b-a \in N$, and therefore we get $f = e$.

3) ⇒ 4). Since R is a strongly π-regular ring, the (Jacobson) radical J of R is nil; $J \subseteq N$. Now, we shall show that R/J is commutative. To see this, it suffices to show that if S is a primitive ring satisfying 3) then S is a division ring, and hence it is GF(2). Suppose, to the contrary, that S is not a division ring. Then, by the structure theorem of primitive rings, there exists an integer $k > 1$ and a division ring D such that $M_k(D)$ is a homomorphic image of a subring of S. Needless to say, $M_k(D)$ satisfies 3). But $(E_{11}+E_{12}+E_{21})^2-(E_{11}+E_{12}+E_{21}) = E_{11}+E_{22}$ is not nilpotent. This contradiction shows that S is a division ring. Thus we have seen that R/J is commutative. Consequently, the commutator ideal of R is contained in J, and so it is contained in N also. Hence N forms an ideal.

Proof of Theorem 4. In case R is normal, the $(E\text{-}N)$ representability and the $E\text{-}N$ representability are equivalent to the $|E\text{-}N|$ representability and the $[E\text{-}N]$ representability, respectively. Since the $(E\text{-}N)$ representability implies the normality of R, the assertion is clear by Theorem 3.

The next generalizes [1, Theorem 6].

Corollary 3. *Let R be a commutative ring. Then the following are equivalent:*

1) *R is $(E\text{-}N)$ representable.*
2) *R is $E\text{-}N$ representable.*
3) *R/N is a Boolean ring.*

As is easily seen (see, e.g., [9, Lemma 1]), every factor ring of a normal π-regular ring is normal. Hence, by Theorem 4 3), we see that if R

is (E-N) representable then so is every factor subring of R.

Corollary 4. *If R is (E-N) representable, then R is a subdirect sum of nil rings and local rings R_α with radical N_α nil and $R_\alpha/N_\alpha = \mathrm{GF}(2)$.*

Corollary 5. *Let R be an Artinian and Noetherian ring. Then R is (E-N) representable if and only if R is a finite direct sum of nil rings and local rings R_i with radical N_i nil and $R_i/N_i = \mathrm{GF}(2)$.*

Proof of Theorem 5. Obviously, by Theorem 4, 1)—4) are equivalent. Since 5) implies 1), it remains only to show that 1) implies 5).

1) ⇨ 5). It is easy to see that R is E-N orthogonal. Now, let u be an arbitrary potent element: $u^n = u$ with $n > 1$. We write $u = e+a$, where e is a central idempotent and a is a nilpotent. Since u^{n-1} is an idempotent, we get $u = uu^{n-1} = (e+a)u^{n-1} = eu^{n-1} \in E$. This proves that $P = E$, and therefore $R = E \oplus N$, by Theorem 1.

Remark 1. In connection with the (E-N) representability, we consider the following condition:

(*) If $e, f \in E$ and $e-f \in N$, then $e = f$.

If e, f are central idempotents and $e-f \in N$, then $e-f = (e-f)^3$, and so $e-f = 0$. This proves that if R is normal then R satisfies (*). Conversely, suppose (*). Let $e \in E$, and $x \in R$. Then $f = e-ex(1-e) \in E$ and $e-f = ex(1-e) \in N^*$. Hence we have $ex = exe$; similarly $xe = exe$. This proves that R is normal.

Appendix. Given an integer $n > 1$, we consider the following condition:

$(\#)_n$ For each $x \in R$, $x^n - x \in N$.

As was shown in Theorem 2, N forms an ideal whenever R satisfies $(\#)_2$. In what follows, we shall prove the next

Theorem A.1. *Let $n > 1$ be an integer. Then the following are equivalent:*

1) *N forms an ideal whenever R satisfies $(\#)_n$.*
2) $n \not\equiv 1 \pmod 3$ *and* $n \not\equiv 1 \pmod 8$.
3) *For each prime p,* $n \not\equiv 1 \pmod{p^2-1}$.
4) *For each prime p, $M_2(\mathrm{GF}(p))$ fails to satisfy $(\#)_n$.*

In preparation for proving Theorem A.1, we state two lemmas.

Lemma A.1. *Let R be a ring in which every non-nil right ideal contains a non-zero idempotent. Then the following are equivalent:*

1) *N forms an ideal.*
2) *R contains no systems of 2^2 matrix units.*
3) *R contains no subrings isomorphic to $M_2(\mathbf{Z}/m\mathbf{Z})$ for a non-negative integer $m \neq 1$.*

Proof. Note that the Jacobson radical J of R is the largest nil ideal of R. Obviously, 1) ⇒ 3) ⇒ 2).

2) ⇒ 1). Suppose, to the contrary, that N does not form an ideal, namely $N \not\subseteq J$. Since $\bar{R} = R/J$ is a semiprimitive ring in which every non-zero right ideal contains a non-zero idempotent, a theorem of Levitzki [5, Theorem X. 11. 1] shows that there exist non-zero $e, f \in E$ such that $\bar{e}\bar{R}\bar{e} \simeq M_2(\bar{f}\bar{R}\bar{f})$. Then, as is well-known (see, e.g., [5, Theorem III. 8. 1]), $eRe \simeq M_2(fRf)$. This contradicts 2).

Corollary A.1 ([6, Theorem 1]). *Let R be a regular ring. Then the following are equivalent:*

1) *R is a reduced ring, namely a strongly regular ring.*
2) *If e, f are in E and $ef = 0$ then $fe = 0$.*
3) *R contains no subrings isomorphic to $M_2(F)$ for a prime field F.*

Proof. It is easy to see that 1) ⇒ 2) ⇒ 3).

3) ⇒ 1). Suppose, to the contrary, that $N \neq 0$. Then N does not form an ideal. Hence, by Lemma A.1, there exist non-zero $e, f \in E$ such that $eRe \simeq M_2(fRf)$. Now, suppose that the regular ring fRf contains no subring isomorphic to a finite prime field. We claim that fRf is torsion free. Actually, if fRf contains a non-zero element of finite order, then fRf contains an idempotent of prime order, which is impossible. Thus, for each non-zero $n \in \mathbf{Z}$, nf is invertible in fRf, and therefore fRf contains a subfield isomorphic to $\mathbf{Q}$.

Lemma A.2. *Let p be a prime, and $\Phi = \mathrm{GF}(p)$. Then $M_2(\Phi)$ satisfies $(\#)_n$ if and only if $n \equiv 1 \pmod{p^2-1}$.*

Proof. Let Ω be the algebraic closure of Φ, and $K = \mathrm{GF}(p^2)$. Suppose $M_2(\Phi)$ satisfies $(\#)_n$, and choose a generator a of the multiplicative group of K. Noting that K may be regarded as a subring of $M_2(\Phi)$, we see that $a^n - a = 0$, by $(\sharp)_n$. Since a is of order p^2-1, we get $n \equiv 1 \pmod{p^2-1}$. Conversely, suppose that $n-1 = (p^2-1)k$ for an integer k. Given $A \in M_2(\Phi)$, we can find an invertible $B \in M_2(\Omega)$ such that $B^{-1}AB = \begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix}$, where α, β are characteristic roots of A, which belong to K. Then

$$(A^{p^2}-A)^2 = B\{(B^{-1}AB)^{p^2}-B^{-1}AB\}^2B^{-1} = 0,$$

and so

$$(A^n-A)^2 = (A^{p^2}-A)^2(A^{(p^2-1)(k-1)}+\cdots+A^{p^2-1}+1)^2 = 0.$$

We are now ready to complete the proof of Theorem A.1.

Proof of Theorem A.1. By Lemma A.2, 3) and 4) are equivalent. Next, 1) implies 4), obviously. Conversely, suppose 4). If R satisfies $(\sharp)_n$, then we can easily see that R contains no subrings isomorphic to $M_2(\boldsymbol{Z}/m\boldsymbol{Z})$ for a non-negative integer $m \neq 1$. Hence, by Lemma A.1, N forms an ideal. We have thus seen that 1) and 4) are equivalent. Finally, as is easily seen, if p is a prime different from 2, 3 then $p^2-1 = (p-1)(p+1)$ is a multiple of $3\cdot 8$. Hence 2) and 3) are equivalent, completing the proof.

Remark A.1. By Dirichlet's Theorem (see, e.g., [3, Theorem 5.3.2]), the set of primes n such that $n \equiv 5 \pmod{24}$ is infinite. Hence there exists an infinite number of primes n such that $n \not\equiv 1 \pmod 3$ and $n \not\equiv 1 \pmod 8$.

REFERENCES

[1] D. D. ANDERSON : Generalizations of Boolean rings, Boolean-like rings and von Neumann regular rings, Comment. Math. Univ. St. Paul. 35 (1986), 69-76.

[2] H. E. BELL and H. TOMINAGA : On periodic rings and related rings, Math. J. Okayama Univ. 28 (1986), 101-103.

[3] Z. I. BOREVICH and I. R. SHAFAREVICH : Number Theory, Academic Press, New York, 1966.

[4] M. CHACRON : On a theorem of Herstein, Canad. J. Math. 21 (1969), 1348-1353.

[5] N. JACOBSON : Structure of Rings, Amer. Math. Soc. Colloq. Publ. 37 (rev. ed.), Amer. Math. Soc., Providence, 1964.

[6] L. LI and B. M. SCHEIN : Strongly regular rings, Semigroup Forum 32 (1985), 145-161.

[7] J. LUH : On the structure of pre-J-rings, Hung-ching Chow Sixty-fifth Anniversary Volume (1967), 47-52.

[8] M. ÔHORI : On strongly π-regular rings and periodic rings, Math. J. Okayama Univ. 27 (1985), 49-52.

[9] H. TOMINAGA and A. YAQUB : Some commutativity conditions for left s-unital rings satisfying certain polynomial identities, Resultate Math. 6 (1983), 217-219.

OKAYAMA UNIVERSITY, OKAYAMA, 700 JAPAN
OKAYAMA UNIVERSITY, OKAYAMA, 700 JAPAN
UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CALIFORNIA 93106, U.S.A.

(*Received August 7, 1987*)