ON CERTAIN SEMIGROUPS ARISING FROM RADICALS OF MATRIX RINGS

by A. D. SANDS

(Received 1st March, 1984)

By a ring we shall mean an associative ring not necessarily containing an identity element. The fundamental definitions and properties of radicals may be found in Divinsky [2]. Similarly we refer to Howie [3] for the semigroup concepts.

If R is a ring $M_n(R)$ will denote the ring of $n \times n$ matrices with entries from R. For many important radicals α it has been shown that $\alpha(M_n(R)) = M_n(\alpha(R))$ for all rings R and all positive integers n. However this is not the case for all radicals α. Associated with each radical α we define a set of positive integers $S(\alpha)$ by

$$S(\alpha) = \{n \in N \mid \alpha(M_n(R)) = M_n(\alpha(R)) \text{ for all rings } R\}.$$

Here, and throughout, N denotes the multiplicative semigroup of positive integers. The aim of this note is to classify the sets $S(\alpha)$ which arise in this way. Clearly $1 \in S(\alpha)$ for all radicals α.

We use the following conventions and notations for matrix rings. We identify $M_m(M_n(R))$ with $M_{mn}(R)$ in the obvious way. If θ is a homomorphism from a ring R to a ring S we shall say that the homomorphism from $M_n(R)$ to $M_n(S)$ defined by $\theta([r_{ij}]) = [\theta(r_{ij})_{ij}]$ is induced by θ. We note that if A is an ideal of R then $M_n(A)$ is an ideal of $M_n(R)$ and, from the above, that $M_n(R/A) \cong M_n(R)/M_n(A)$. It is known that not every ideal of $M_n(R)$ need be of the form $M_n(A)$, A an ideal of R. It has been shown by Sands [4] that every prime ideal of $M_n(R)$ has the form $M_n(A)$ where A is a prime ideal of R and by Snider [5] that, for every radical α, $\alpha(M_n(R)) = M_n(A)$ for some ideal A of R.

Theorem 1. *Let T be a non-empty subset of N. Then there exists a radical α such that $S(\alpha) = T$ if and only if for all $m, n \in N$ whenever any two from m, n, mn belong to T so also does the remaining one.*

Proof. First assume that a radical α exists such that $S(\alpha) = T$. Let $m, n \in T$. Then $\alpha(M_{mn}(R)) = \alpha(M_m(M_n(R)) = M_m(\alpha(M_n(R))) = M_m(M_n(\alpha(R))) = M_{mn}(\alpha(R))$ for all rings R. Therefore $mn \in T$. Now let $m, n \in N$ and assume $m, mn \in T$. By the result of Snider [5], for any ring R there exists an ideal A of R such that $\alpha(M_n(R)) = M_n(A)$. Then, since $m \in T$, $\alpha(M_m(M_n(R))) = M_m(M_n(A))$. Since $mn \in T$, $\alpha(M_{mn}(R)) = M_{mn}(\alpha(R))$. It follows that $\alpha(R) = A$ and so that $n \in T$.

Conversely let T be a non-empty subset of N satisfying the given property. We need to construct a radical α such that $S(\alpha) = T$. Let F be a field. Let α be the upper radical generated by the class $\mathscr{C}$ of rings, where $\mathscr{C} = \{M_n(F) \mid n \in T\}$. Note that $F \in \mathscr{C}$, since

67

$n, n1 \in T$ implies $1 \in T$. Since $\mathscr{C}$ consists of simple rings with 1, α is a special radical and for each ring R we have $\alpha(R) = \cap A_i$, where the intersection is taken over all ideals A_i of R such that $R/A_i \in \mathscr{C}$ (see Divinsky [2, Ch. 7]). Let A_i be such an ideal and let $R/A_i \cong M_n(F)$, where $n \in T$. Let $m \in T$. Then $M_m(R)/M_m(A_i) \cong M_m(R/A_i) \cong M_{mn}(F) \in \mathscr{C}$. Conversely let B be an ideal of $M_m(R)$ such that $M_m(R)/B \in \mathscr{C}$. Since $M_m(R)/B$ is a simple ring B is a prime ideal of $M_m(R)$. It follows from Sands [4] that there is a prime ideal A in R such that $B = M_m(A)$. Then $M_m(R)/B = M_m(R)/M_m(A) \cong M_m(R/A)$ and, as this ring is in $\mathscr{C}$, it is isomorphic to $M_k(F)$ for some $k \in T$. Thus $M_m(R/A)$ is a simple ring satisfying the minimum condition on one-sided ideals. It follows easily that R/A is a simple ring also satisfying this minimum condition. By the Wedderburn–Artin Theorem there is an integer q and a division ring D such that $R/A \cong M_q(D)$. Then $M_m(R/A) \cong M_{mq}(D) \cong M_k(F)$. By the uniqueness part of the Wedderburn–Artin Theorem we have $D \cong F$ and $mq = k$. Since $k, m \in T$ it follows that $q \in T$. Therefore $R/A \in \mathscr{C}$. Hence $\alpha(M_m(R)) = \cap M_m(A_i) = M_m(\cap A_i) = M_m(\alpha(R))$, where the intersections are taken over all ideals A_i of R such that $R/A_i \in \mathscr{C}$. It follows that $m \in S(\alpha)$ and so $T \subseteq S(\alpha)$. Now let $m \notin T$. Since $M_m(F)$ is a simple ring which is not in $\mathscr{C}$, no image of $M_m(F)$ is in $\mathscr{C}$, and $\alpha(M_m(F)) = M_m(F)$. Since $F \in \mathscr{C}$, $\alpha(F) = 0$. It follows that $\alpha(M_m(F)) \neq M_m(\alpha(F))$. Therefore $m \notin S(\alpha)$. Thus $S(\alpha) = T$, as required.

We recall [3, p. 55] that a subset T of a semigroup S is left unitary in S if $a = bx$, $a, b \in T$, $x \in S$ imply $x \in T$. Right unitary is defined analogously and unitary is used to mean both left and right unitary. So we wish to describe the unitary subsemigroups of N. Before considering this problem we obtain some more general results. We consider especially the use of subsemigroups and of semigroups which can be embedded in a group.

Theorem 2. *Every subsemigroup of a semigroup S is unitary in S if and only if S is a torsion group.*

Proof. If S is a torsion group then every subsemigroup of S is a subgroup of S. It is clear that every subgroup of a group is unitary.

Conversely let every subsemigroup of S be unitary in S. Let $a \in S$. Let $T = \{a^n \in S \mid n \geq 2\}$. Since T is a subsemigroup and $a^2, a^3 \in T$ it follows that $a \in T$. Therefore there exists $n \geq 1$ with $a^{n+1} = a$. Let $a^n = e$. Then $e^2 = e$ and $ae = ea = a$. Now let $b \in S$. As above there exists $m \geq 1$ such that $b^{m+1} = b$ and $b^m = f$ satisfies $f^2 = f$, $bf = fb = b$. Let U be the subsemigroup of S generated by efe. Then $(efe)^2 = efefe$ and efe both in U implies $fe \in U$; $efe, fe \in U$ imply $e \in U$; $fe, e \in U$ imply $f \in U$. Therefore there exist $p, q \geq 1$ with $e = (efe)^p$, $f = (efe)^q$. Hence $e = e^q = (efe)^{pq} = f^p = f$. It follows that e is a neutral element for S and that S is a torsion group.

In the proof of Theorem 2 we have used the fact that U is both left and right unitary. If we restrict our attention to left unitary only we obtain a more general class of semigroups.

Theorem 3. *Every subsemigroup of a semigroup S is left unitary if and only if S is a direct product of a torsion group and a right zero semigroup.*

Proof. Let $S = G \times E$ where G is a torsion group and E is a right zero semigroup. We recall that multiplication is defined in E by $bd = d$ for all b, $d \in E$. Let T be a subsemigroup of S. Let $(a, b) \in T$, $(x, y) \in S$, $(c, d) \in T$ be such that $(a, b)(x, y) = (c, d)$. Then $ax = c$ and $by = d$. It follows that $x = a^{-1}c = a^k c$ for some positive integer k and that $y = d$. Then $(x, y) = (a^k c, d) = (a, b)^k(c, d) \in T$. Hence every subsemigroup of S is left unitary.

Conversely let S be a semigroup such that every subsemigroup of S is left unitary. Let E denote the set of idempotents of S. As in the proof of Theorem 2 it follows that given $a \in S$ there exists an integer $n \geq 1$ such that $a^{n+1} = a$ and $a^n = e$ is an idempotent with $ae = ea = a$. Thus the set E is not empty. For each $f \in E$ let

$$S_f = \{x \in S \mid fx = xf = x\}.$$

Let $b \in S$ be such that $bf = b$. Since the subsemigroup generated by b is left unitary there is a positive integer m such that $b^m = f$ and $fb = b^{m+1} = bf = b$. It follows that $b \in S_f$. In particular we have $Sf \subseteq S_f$. If b is idempotent then $b^m = f$ implies $b = f$; thus f is the only idempotent of S_f and some positive power of each element of S_f is equal to f. It follows that S_f is a torsion group. If f, $g \in E$ and $a \in S_f \cap S_g$ then some positive power of a is equal to g and so $g \in S_f$. It follows that $f = g$ and so for distinct f, $g \in E$ we have $S_f \cap S_g = \varnothing$.

Let f, $g \in E$ then $(gf)f = gf$ and so $gf \in S_f$. Hence $fgf = gf$ and so $(gf)^2 = g^2 f = gf$. Thus gf is an idempotent in S_f. Hence $gf = f$ and E is a right zero semigroup.

Choose $e \in E$. Considering the mapping μ from $S_e \times E$ to S given by $\mu(a, f) = af$ for each $a \in S_e$ and $f \in E$. Let $(b, g) \in S_e \times E$. Then $\mu((a, f)(b, g)) = abfg = abg = aebg = afebg = afbg = \mu(a, f)\mu(b, g)$. Thus μ is a homomorphism. Let $s \in S$. Then $s \in S_f$ for some $f \in E$ and $se \in Se \subseteq S_e$. Then $\mu(se, f) = sef = sf = s$. Thus μ is surjective. Finally $\mu(a, f) = \mu(b, g)$ implies $af = bg \in S_f \cap S_g$ which implies $f = g$ and also $afe = bge = ae = be = a = b$. Thus μ is injective. It follows that S is isomorphic to the direct product of a torsion group and a right zero semigroup.

The direct product of a group and a right zero semigroup is known as a right group. Further properties of right groups may be found in Clifford and Preston [1, Section 1.11]. Since a finite direct product of torsion groups is a torsion group and a direct product of right zero semigroups is a right zero semigroup it follows that a finite direct product of semigroups such that every subsemigroup is left unitary again has this property.

In the special case where G is the identity group S is a right zero semigroup. In this case every non-empty subset of S is a semigroup and so every subset of S is left unitary. The converse also holds. For if a, b are in S and $a \neq b$ then, if $\{a, ab\}$ is left unitary, we must have $ab = b$. If $a \neq a^2$ then $a^3 = aa^2 = a^2$ and also $a^3 = a^2 a = a$. Hence $a = a^2$. Thus S is a right zero semigroup.

There are dual results for semigroups in which every subsemigroup or every subset is right unitary. In particular every subset of a semigroup is unitary if and only if the semigroup S is both a left and a right zero semigroup, i.e. S has one element only.

Theorem 4. *Let a semigroup S be contained in a group G. If H is a subgroup of G such that $H \cap S \neq \varnothing$ then $H \cap S$ is unitary in S. If G is an abelian group then any unitary subsemigroup of S has the form $H \cap S$ for some subgroup H of G.*

Proof.   Let S be contained in G and let $T = H \cap S \neq \varnothing$, where H is a subgroup of G. Let $ax = b$ where $a, b \in T$ and $x \in S$. Then $x = a^{-1}b$ and $x \in H$ since $a, b \in H$. Thus $x \in H \cap S = T$. Similarly $ya = b$ implies $y \in T$, where $a, b \in T$, $y \in S$. Thus T is unitary.

Now let the group G be abelian and let T be any unitary subsemigroup of S. Let H be the subgroup of G generated by T. Then $T \subseteq H \cap S$. Let $h \in H \cap S$. Since G is abelian there exist elements $a, b \in T$ with $h = ab^{-1}$. Then $a = hb$. It follows that $h \in T$. Therefore $T = H \cap S$.

It is clear that the second part of Theorem 4 also holds trivially in the class of torsion groups. We do not know for which other classes of groups it holds. That it does not hold in the class of all groups is shown by the following example.

Let F_2 be the free group on two generators, say a and b. Let S be the subsemigroup of F_2 generated by a, ab, ab^2; let T be the subsemigroup of S generated by a, ab. Clearly $T \neq S$ since $ab^2 \notin T$. Let $ux = v$ where $u, v \in T$, $x \in S$. Since products of a, ab, ab^2 are already in reduced form it is clear that b^2 cannot occur in x since it does not occur in v. Therefore $x \in T$. Similarly $yu = v$ implies $y \in T$, Hence T is unitary in S. The subgroup of F_2 generated by T is F_2 itself. Thus there is no subgroup H of F_2 with $H \cap S = T$.

We recall a well-known property of the additive group $\mathbb{Q}/\mathbb{Z}$ of rationals modulo 1. If g is a non-identity element of any abelian group G then, since $\mathbb{Q}/\mathbb{Z}$ contains elements of all finite orders, there is a non-zero homomorphism from the cyclic subgroup generated by g to $\mathbb{Q}/\mathbb{Z}$. Since $\mathbb{Q}/\mathbb{Z}$ is divisible this homomorphism will extend to a homomorphism θ from G to $\mathbb{Q}/\mathbb{Z}$ such that $\theta(g) \neq 0$. For any abelian group G we denote the homomorphism group $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ by G^*.

Theorem 5.   *Let S be a subsemigroup of an abelian group G with $1 \in S$. Then T is a unitary subsemigroup of S if and only if there exists a subset A^* of G^* such that*

$$T = \{x \in S \,|\, \theta(x) = 0 \quad \text{for all} \quad \theta \in A^*\}.$$

Proof.   Let A^* be a subset of G^* and let T be defined as above. Clearly $1 \in T$; thus T is non-empty. If $a, b \in T$ then $\theta(ab) = \theta(a) + \theta(b) = 0$, for all $\theta \in A^*$. It follows that $ab \in T$ and so T is a subsemigroup of S. Now let $ax = b$, where $a, b \in T$ and $x \in S$. Let $\theta \in A^*$. Then $\theta(ax) = \theta(a) + \theta(x) = 0 + \theta(x) = \theta(b) = 0$. Therefore $\theta(x) = 0$. Thus $x \in T$ and T is unitary in S.

Conversely let T be a unitary subsemigroup of S. Let $A^* = \{\theta \in G^* \,|\, \theta(t) = 0$ for all $t \in T\}$. Let $K = \{g \in G \,|\, \theta(g) = 0$ for all $\theta \in A^*\}$. Let H be the subgroup of G generated by T. Since each $h \in H$ may be expressed as $h = ab^{-1}$ with $a, b \in T$ it follows that $H \subseteq K$. Let $g \in K$. If $g \notin H$ then gH is a non-identity element of G/H. Thus there is a homomorphism from G/H to $\mathbb{Q}/\mathbb{Z}$ mapping gH to some non-zero image. This gives rise to a homomorphism θ from G to $\mathbb{Q}/\mathbb{Z}$ such that $H \subseteq \ker \theta$ and $\theta(g) \neq 0$. Then $\theta(t) = 0$ for all $t \in T$ and so $\theta \in A^*$, which contradicts $g \in K$. It follows that $H = K$. By Theorem 4, $T = H \cap S$. Thus

$$T = K \cap S = \{x \in S \,|\, \theta(x) = 0 \quad \text{for all} \quad \theta \in A^*\}.$$

We now return to the case of the multiplicative semigroup N of positive integers. The group generated by N is the multiplicative group $\mathbb{Q}_+$ of all positive rationals. $\mathbb{Q}_+$ is a

free abelian group with free generating set p_j, $j \in N$, where p_j is the jth prime. Thus any $\theta \in \mathbb{Q}_+^*$ determines a sequence $\{r_j\}$ of rationals mod 1 where $\theta(p_j) = r_j$ and conversely any such sequence determines an element of $\mathbb{Q}_+^*$ in this way. Hence $\mathbb{Q}_+^*$ is the unrestricted direct product of countably many copies of $\mathbb{Q}/\mathbb{Z}$.

From Theorem 4 it follows that T is a unitary subsemigroup of N if and only if $T = H \cap N$ for some subgroup H of $\mathbb{Q}_+$. We should note that different subgroups H may give rise to the same subsemigroup T. For example if $m > 1$ and $n > 1$ are relatively prime integers and $H(m/n)$ is the cyclic subgroup generated by m/n then $H(m/n) \cap N = \{1\}$.

From Theorem 5 it follows that T is a unitary subsemigroup of N if and only if there exists a family $\{r_{ij}\}$, $i \in I, j \in N$, of sequences of rationals such that

$$T = \{n \in N \mid n = \pi p_j^{e_j} \quad \text{and} \quad \sum_j r_{ij} e_j \in \mathbb{Z} \quad \text{for each} \quad i \in I\}.$$

We may assume $0 \le r_{ij} < 1$. There is a largest such family of rationals for any such T, namely the family of all such sequences. It may not be possible to choose a smallest family. For example let T be the semigroup of all odd integers in N. Clearly T is unitary in N. Taking $p_1 = 2$ any family of sequences of rationals $(1/m, 0, 0, \ldots)$ determines T where m ranges over any unbounded set of non-zero integers. The complete family has typical member $(q, 0, 0, \ldots)$ where q ranges over all rationals but no minimal family exists.

Unitary subsemigroups of N are obtained in this manner from homomorphisms of $\mathbb{Q}_+$ into any abelian group G. For example the semigroup T of odd integers may be obtained more easily by considering homomorphisms from $\mathbb{Q}_+$ into $\mathbb{Z}$, the additive group of all integers. In the previous notation it then arises from the single sequence $(1, 0, 0, \ldots)$. However $\mathbb{Q}/\mathbb{Z}$ is the smallest abelian group which will give rise to every unitary subsemigroup of N. To see this we recall that $\mathbb{Q}/\mathbb{Z}$ is the direct sum, taken over all primes q, of the quasi-cyclic groups $\mathbb{Z}(q^\infty)$. $\mathbb{Z}(q^\infty)$ is generated by the rationals, mod 1, $a_n = 1/q^n$, $n = 1, 2, \ldots$, which satisfy $qa_1 = 0, \ldots, qa_{n+1} = a_n, \ldots$. Since $\mathbb{Q}_+$ is a free abelian group with countably many generators every countably generated abelian group is an image. Thus the groups $\mathbb{Z}(q^\infty)$ are homomorphic images of $\mathbb{Q}_+$. In order to see that these groups are needed to obtain unitary subsemigroups, we need to find such a homomorphism for which the kernel is generated by integers. To do this let $A_q = \{p_1^q, p_1 p_2^q, p_2 p_3^q, \ldots, p_r p_{r+1}^q, \ldots\}$. Let H be the subgroup of $\mathbb{Q}_+$ generated by A_q and let $S = H \cap N$. One should note that S contains but is not equal to the subsemigroup of N generated by A_q, since, for example, $p_2^{q^2} = (p_1^q)^{-1}(p_1 p_2^q)^q$ belongs to S but clearly not to this subsemigroup. It is easy to see that the primes $p_1, p_2, p_3, \ldots$ do not belong to H and so $\mathbb{Q}_+/H$ is generated by the elements $g_r = p_r^{(-1)^{r+1}} H, r = 1, 2, \ldots$, which are not equal to 1. These satisfy $g_1^q = 1$, $g_2^q = g_1, \ldots, g_{r+1}^q = g_r, \ldots$. Thus $\mathbb{Q}_+/H$ is the group $\mathbb{Z}(q^\infty)$ in multiplicative form. Now any non-zero image of $\mathbb{Z}(q^\infty)$ is isomorphic to $\mathbb{Z}(q^\infty)$. Suppose that G is an abelian group which contains no subgroup isomorphic to $\mathbb{Z}(q^\infty)$. Let A be a family of homomorphisms from $\mathbb{Q}_+$ to G which send each $n \in S$ to 0. Then, if $\theta \in A$, since $A_q \subseteq \ker \theta$ we have $H \subseteq \ker \theta$. Therefore the image of θ is an image of $\mathbb{Q}_+/H \cong \mathbb{Z}(q^\infty)$. Since G contains no subgroup isomorphic to $\mathbb{Z}(q^\infty)$ it follows that the image of θ is 0. Therefore the subsemigroup determined by A is N and S cannot arise in this way. Thus

any group G giving rise to all unitary subsemigroups of N must contain all quasi-cyclic groups. $\mathbb{Q}/\mathbb{Z}$ is the smallest such group.

REFERENCES

1. A. H. CLIFFORD and G. B. PRESTON, *The Algebraic Theory of Semigroups,* vol 1 (Mathematical Surveys, 7, American Mathematical Society, 1961).

2. N. J. DIVINSKY, *Rings and Radicals* (Allen and Unwin, 1965).

3. J. M. HOWIE, *An Introduction to Semigroup Theory* (Academic Press, 1976).

4. A. D. SANDS, Prime Ideals in Matrix Rings, *Proc. Glasgow Math. Assoc.* **2** (1956), 193–195.

5. R. L. SNIDER, Lattices of Radicals, *Pacific J. Math.* **40** (1972), 207–220.

DEPARTMENT OF MATHEMATICAL SCIENCES
THE UNIVERSITY
DUNDEE DD1 4HN
SCOTLAND