BULL. AUSTRAL. MATH. SOC. 16A44
VOL. 46 (1992) [353–359]

ON ORDERS OF DIRECTLY INDECOMPOSABLE FINITE RINGS

YASUYUKI HIRANO AND TAKAO SUMIYAMA

Let R be a directly indecomposable finite ring. Let p be a prime, let m be a positive integer and suppose the radical of R has p^m elements. Then we show that $p^{m+1} \leqslant |R| \leqslant p^{m^2+m+1}$. As a consequence, we have that, for a given finite nilpotent ring N, there are up to isomorphism only finitely many finite rings not having simple ring direct summands, with radical isomorphic to N. Let R^* denote the group of units of R. Then we prove that $(1-1/p)^{m+1} \leqslant |R^*|/|R| \leqslant 1-1/p^m$. As a corollary, we obtain that if R is a directly indecomposable non-simple finite $2'$-ring then $|R| < |R^*|\,|\mathrm{Rad}\,(R)|$.

Stewart [7] considered the following problem. Given a finite group G, what are the possible finite rings with group of units isomorphic to G? In this paper, we consider a similar problem; given a finite nilpotent ring N, what are possible finite rings with radical isomorphic to N? For (not necessarily finite) algebras, this problem was considered by Flanigan [2] and Hall [3].

All the rings considered in this paper are finite, and have an identity. Let R be a directly indecomposable finite ring. Then, as is well known, the order $|R|$ of R is a power of a prime p. Let $\mathrm{Rad}\,(R)$ denote the (Jacobson) radical of R and suppose that $|\mathrm{Rad}\,(R)| = p^m > 1$. Mainwaring and Pearson [4] proved that there are at most $m+1$ minimal ideals in $R/\mathrm{Rad}\,(R)$. Using their method, we try to estimate $|R|$.

For a prime p and positive integers n and t, $GR(p^n, t)$ denotes the Galois extension of Z/Zp^n of degree t (see McDonald [5, p.307]). Especially the field $GR(p, t)$ of p^t elements is denoted by $GF(p^t)$.

A graph means a finite undirected graph without loops. The edge which joins two vertices x and y is denoted by (x, y).

We begin with the following lemma.

LEMMA 1. *Let $G = (V, E)$ be a non-trivial connected graph, where V is the set of vertices of G and E the set of edges of G. Let u be a vertex in V. Then there exists an injective mapping $\varphi\colon V \setminus \{u\} \to E$ satisfying the conditions: (i) $\varphi(w) = (w, u)$ for some $w \in V \setminus \{u\}$, and (ii) for any $v \in V \setminus \{u\}$, one of the endpoints of $\varphi(v)$ is v.*

PROOF: We proceed by induction on $|V|$. In case $|V| = 2$, our assertion is trivial. Assume $|V| > 2$ and let $G - u$ denote the subgraph of G obtained by deleting the

Received 1 November 1991

vertex u and all edges incident with u. Let $G_1 = (V_1, E_1), \dots, G_r = (V_r, E_r)$ be the connected components of $G - u$. Then, for each i, there exists $u_i \in V_i$ such that $(u, u_i) \in E$. If G_j is non-trivial, namely $|V_j| > 2$, then by induction hypothesis there exists an injective mapping $\varphi_j \colon V_j \setminus \{u_j\} \to E_j$ satisfying the conditions (i) and (ii). We now define a mapping $\varphi \colon V \setminus \{u\} \to E$ by $\varphi(u_j) = (u, u_i)$ for each i and $\varphi(v) = \varphi_j(v)$ if $v \in V_j \setminus \{u_j\}$. It is easy to see that φ satisfies (i) and (ii). $\square$

It is easy to check the set

$$\{(a_{ij}) \in M_{m+1}(GF(p)) \mid a_{21} = a_{31} = \dots = a_{m+1,1} = 0\}$$

forms a subring of $M_{m+1}(GF(p))$. We denote this subring by $A_{m+1}(p)$.

We shall estimate the order of a non-simple directly indecomposable finite ring in terms of the order of its radical.

THEOREM 1. *Let R be a directly indecomposable finite ring and suppose* $|\mathrm{Rad}(R)| = p^m$ *where p is a prime and m is a positive integer. Then*

$$p^{m+1} \leqslant |R| \leqslant p^{m^2+m+1}.$$

The first equality holds if and only if $R/\mathrm{Rad}(R) = GF(p)$, and the second equality holds if and only if R is either isomorphic or anti-isomorphic to $A_{m+1}(p)$.

PROOF: Since R has 1, we have $p \leqslant |R/\mathrm{Rad}(R)|$, so that $p^{m+1} \leqslant |R|$. The equality holds if and only if $R/\mathrm{Rad}(R) = GF(p)$.

To prove the latter inequality, suppose that $R/\mathrm{Rad}(R) = M_{n_1}(K_1) \oplus \dots \oplus M_{n_s}(K_s)$, where $K_i = GF(p^{k_i})$, $i = 1, \dots, s$. Let e_i denote the identity of $M_{n_i}(K_i)$. By McDonald [5, Theorem 7.12], $e_1, \dots, e_s$ can be lifted to orthogonal idempotents $f_1, \dots, f_s$ in R with $f_1 + \dots + f_s = 1$. In case $s = 1$, $\mathrm{Rad}(R)/\mathrm{Rad}(R)^2$ is a nonzero right $M_{n_1}(K_1)$-module, and hence is a direct sum of simple right $M_{n_1}(K_1)$-modules. It is well known that any simple right $M_{n_1}(K_1)$-module is isomorphic to the right ideal I consisting of all matrices with only the first row different from zero. Since $|I| = p^{n_1 k_1}$, we see

$$p^{n_1 k_1} \leqslant \left|\mathrm{Rad}(R)/\mathrm{Rad}(R)^2\right| \leqslant |\mathrm{Rad}(R)| = p^m,$$

whence $n_1 k_1 \leqslant m$. Therefore

$$|R| = p^{k_1 n_1^2 + m} \leqslant p^{m^2+m+1}.$$

Now suppose $s > 1$. We shall define a graph $G = (V, E)$ as follows: $V = \{1, 2, \dots, s\}$ and two distinct vertices i and j are joined by an edge (i, j) if either $f_i R f_j \neq 0$ or $f_j R f_i \neq 0$. According to the proof of Mainwaring and Pearson [4, Theorem], this graph G is connected. Since $\oplus_{i\neq j} f_iRf_j$ is contained in $\mathrm{Rad}(R)$, we see that $\prod_{i\neq j} |f_iRf_j| \leqslant p^m$. We shall estimate $|f_iRf_j|$. For the sake of simplification, we let $J = \mathrm{Rad}(R)$ and $F = GF(p)$. Now assume $f_iRf_j \neq 0$. Then f_iRf_j is a nonzero (f_iRf_i, f_jRf_j)-bimodule. Let M denote the factor module of f_iRf_j by $f_iJf_iRf_j + f_iRf_jJf_j$. By virtue of Nakayama's lemma [5, Theorem 5.2], M is a nonzero $(f_iRf_i/f_iJf_i, f_jRf_j/f_jJf_j)$-bimodule. Since f_hRf_h/f_hJf_h is isomorphic to $M_{n_h}(K_h)$, $1 \leqslant h \leqslant s$, M can be viewed as a nonzero $\left(M_{n_i}(K_i), M_{n_j}(K_j)\right)$-bimodule. Since the opposite ring of $M_{n_j}(K_j)$ is isomorphic to $M_{n_j}(K_j)$ itself, M can be regarded as a nonzero left $M_{n_i}(K_i) \otimes_F M_{n_j}(K_j)$-module. By the way, we can easily see that $K_i \otimes_F K_j = GF(p^{k_i}) \otimes_F GF(p^{k_j}) \simeq GF(p^\ell)^{(d)}$, the direct sum of d copies of $GF(p^\ell)$, where $d = \gcd\{k_i, k_j\}$ and $\ell = \mathrm{lcm}\{k_i, k_j\}$. Therefore $M_{n_i}(K_i) \otimes_F M_{n_j}(K_j) \simeq M_{n_in_j}(GF(p^\ell))^{(d)}$, whence we have $|f_iRf_j| \geqslant |M| \geqslant p^{n_in_j}$. Consequently we obtain

$$(1) \qquad \sum_{(i,j)\in E} n_in_j(\mathrm{lcm}\{k_i, k_j\}) \leqslant m.$$

Define a mapping $\psi\colon E \to Z$ by $\psi(i, j) = n_in_j(\mathrm{lcm}\{k_i, k_j\})$ for any $(i, j) \in E$. Then (1) can be rewritten as follows.

$$(2) \qquad \sum_{x\in E} \psi(x) \leqslant m.$$

By Lemma 1 there exists an injective mapping $\varphi\colon V' = \{1, 2, \dots, s-1\} \to E$ satisfying that, for each $i \in V'$, $\varphi(i) = (i, j)$ for some $j \in V$ and there exists $h \in V'$ with $\varphi(h) = (h, s)$. Since $(n_h^2 - 1)(n_s^2 - 1) \geqslant 0$, we have

$$\begin{aligned}(\psi(\varphi(h)))^2 = n_h^2n_s^2(\mathrm{lcm}\{k_h, k_s\})^2 &\geqslant (n_h^2k_h)(n_s^2k_s) \\ &\geqslant n_h^2k_h + n_s^2k_s - 1.\end{aligned}$$

On the other hand, by the definitions of φ and ψ, $(\psi(\varphi(i)))^2 \geqslant n_i^2k_i$, $1 \leqslant i \leqslant s-1$. By the inequality (2), we have $m \geqslant \sum_{i=1}^{s-1} \psi(\varphi(i))$. Hence we obtain

$$\begin{aligned} m^2 &\geqslant \sum_{j=1}^{h-1} (\psi(\varphi(i)))^2 + (\psi(\varphi(h)))^2 + \sum_{j=h+1}^{s-1} (\psi(\varphi(j)))^2 \\ &\geqslant \sum_{i=1}^{h-1} n_i^2k_i + \left(n_h^2k_h + n_s^2k_s - 1\right) + \sum_{j=h+1}^{s-1} n_j^2k_j \\ &= \sum_{i=1}^{s} n_i^2k_i - 1. \end{aligned}$$

Therefore we have

$$|R| = p^{n_1^2 k_1 + \dots + n_s^2 k_s + m} \leqslant p^{m^2+m+1}.$$

By the above argument, the equality holds if and only if either $s = 2$, $k_1 = k_2 = 1$, $n_1 = 1$, $n_2 = m$ or $s = 2$, $k_1 = k_2 = 1$, $n_1 = m$, $n_2 = 1$. Without loss of generality, we may assume that the former occurs. In this case, we have either $|f_1 R f_2| = p^m$ or $|f_2 R f_1| = p^m$. If $|f_1 R f_2| = p^m$, then $R = f_1 R f_1 \oplus f_1 R f_2 \oplus f_2 R f_2$, $f_1 R f_1 = GF(p)$ and $f_2 R f_2 = M_m(GF(p))$. Hence we have

$$R = \begin{pmatrix} f_1 R f_1 & f_1 R f_2 \\ 0 & f_2 R f_2 \end{pmatrix} \simeq A_{m+1}(p).$$

Similarly, if $|f_2 R f_1| = p^m$, then R is anti-isomorphic to $A_{m+1}(p)$. This completes the proof. ∎

COROLLARY 1. *If R is a finite ring not having simple ring direct summands, then $|R| \leqslant n^{n+1}$, where $n = |\mathrm{Rad}(R)|$.*

PROOF: First we assume that R is directly indecomposable. Then $|\mathrm{Rad}(R)| = p^m$ for some prime p and some positive integer m. Then we have $|R| \leqslant p^{m^2+m+1}$ by Theorem 1. Since $p \geqslant 2$, we can easily see that $m^2 + m + 1 \leqslant m(p^m + 1)$, whence we have $p^{m^2+m+1} \leqslant n^{n+1}$.

Returning to the general case, let $R = R_1 \oplus R_2 \oplus \dots \oplus R_s$ be the direct decomposition of R into directly indecomposable components and let $n_i = |\mathrm{Rad}(R_i)|$. By hypothesis, each n_i is greater than 1, and $n = n_1 n_2 \dots n_s$. By the result proved above, we obtain $|R_i| \leqslant n_i^{n_i+1}$, $1 \leqslant i \leqslant s$. Hence we obtain

$$|R| = |R_1| \dots |R_s| \leqslant n_1^{n_1+1} \dots n_s^{n_s+1} \leqslant n^{n+1}.$$

∎

As an immediate consequence of Corollary 1, we have

PROPOSITION 1. *For a given nilpotent ring N there are up to isomorphism only finitely many finite rings not having simple ring direct summands, with radical isomorphic to N.*

Let R^* denote the group of units of a ring R. Farahat [1] considered the proportion $\delta(R) = |R^*| / |R|$ for a finite ring R. We shall study $\delta(R)$ of a directly indecomposable non-simple finite ring R. To state the result, we need to introduce a class of rings. Let σ be an automorphism of $GF(p^m)$. We denote the subring

$$\left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \,\middle|\, a, b \in GF(p^m) \right\}$$

of $M_2(GF(p^m))$ by $B_\sigma(p^m)$.

THEOREM 2. *Let R be a directly indecomposable finite ring and suppose $|\mathrm{Rad}(R)| = p^m$ where p is a prime and m is a positive integer. Then*

$$(1-1/p)^{m+1} \leqslant \delta(R) \leqslant 1-1/p^m.$$

The first equality holds if and only if R is isomorphic to either $GR(p^2,m)$ or $B_\sigma(p^m)$. The second equality holds if and only if R is an algebra over $GF(p)$ such that $R/\mathrm{Rad}(R) \simeq GF(p)^{(m+1)}$.

PROOF: As in the proof of Theorem 1, let $R/\mathrm{Rad}(R) = M_{n_1}(K_1)\oplus\ldots\oplus M_{n_s}(K_s)$, where $K_i = GF(p^{k_i})$, $1 \leqslant i \leqslant s$. By [1, (3.2)], we have

$$\delta(R) = \sum_{i=1}^{s} \delta(M_{n_i}(K_i)) \leqslant \delta(M_{n_1}(K_1)).$$

Also, by Farahat [1, (3.6)], we have

$$\delta(M_{n_1}(K_1)) = (1-1/p^{k_1})(1-1/p^{2k_1})\ \ldots\ (1-1/p^{n_1k_1}).$$

This is not greater than $1-1/p^m$, because $k_1 \leqslant m$ as shown in the proof of Theorem 1. Hence we obtain $\delta(R) \leqslant 1-1/p^m$. The equality holds if and only if $s = n_1 = 1$ and $k_1 = m$, that is, $R/\mathrm{Rad}(R) = GF(p^m)$. We determine such a ring R. To do this, assume that R is of characteristic p^t. Then by Raghavendran [6, Theorem 8 (i)], R contains a subring S which is isomorphic to $GR(p^t,m)$. Since

$$p^{tm} = |S| \leqslant |R| = |R/\mathrm{Rad}(R)|\,|\mathrm{Rad}(R)| = p^{2m},$$

either $t=1$ or $t=2$. If $t=2$, then $R \simeq GR(p^2,m)$. Now suppose $t=1$. Since $\mathrm{Rad}(R)/\mathrm{Rad}(R)^2$ is a nonzero vector space over $R/\mathrm{Rad}(R) = GF(p^m)$, $\left|\mathrm{Rad}(R)/\mathrm{Rad}(R)^2\right| \geqslant p^m$. Since $|\mathrm{Rad}(R)| = p^m$ by hypothesis, this implies $\mathrm{Rad}(R)^2 = 0$. Then $R \simeq B_\sigma(p^m)$ for some σ by Raghavendran [6, Theorem 3].

Next we deal with the first inequality. We easily see

$$\begin{aligned}
\delta(R) &= \sum_{i=1}^{s} \delta(M_{n_i}(K_i)) \\
&= \sum_{i=1}^{s} \{(1-1/p^{k_i})(1-1/p^{2k_i})\ \ldots\ (1-1/p^{n_ik_i})\} \\
&\geqslant (1-1/p)^{n_1+n_2+\ldots+n_s}.
\end{aligned} \tag{3}$$

From (1) in the proof of Theorem 1, we get

$$m \geqslant \sum_{(i,j)\in E} n_in_j.$$

https://doi.org/10.1017/S0004972700011990 Published online by Cambridge University Press

Define a mapping $\chi\colon E \to Z$ by $\chi(i,j) = n_i n_j$. We again employ the mapping $\varphi\colon V' = \{1, 2, \ldots, s-1\} \to E$ in the proof of Theorem 1. Then there exists $h \in V'$ such that $\varphi(h) = (h, s)$. Then $\chi(\varphi(h)) = n_h n_s \geqslant n_h + n_s - 1$. Since $\chi(\varphi(i)) \geqslant n_i$, $1 \leqslant i \leqslant s-1$, we see

$$\begin{aligned} m &\geqslant \sum_{x\in E} \chi(x) \\ &\geqslant \sum_{i=1}^{s-1} \chi(\varphi(i)) \\ &= \sum_{i=1}^{h-1} \chi(\varphi(i)) + \chi(\varphi(h)) + \sum_{i=h+1}^{s-1} \chi(\varphi(i)) \\ &\geqslant \sum_{i=1}^{h-1} n_i + (n_h + n_s - 1) + \sum_{i=h+1}^{s-1} n_i \\ &= \sum_{i=1}^{s} n_i - 1. \end{aligned}$$

Combining this inequality with (3), we get $\delta(R) \geqslant (1-1/p)^{m+1}$. The equality holds if and only if $s = m+1$ and $n_i = k_i = 1$, $1 \leqslant i \leqslant s$, so that $R/\mathrm{Rad}(R) \simeq GF(p)^{(m+1)}$. By the definition of E, for any $(i,j) \in E$, either $f_iRf_j \neq 0$ or $f_jRf_i \neq 0$. Since $|E| \geqslant |V| - 1 = m$ and since

$$\prod_{(i,j)\in E} \{|f_iRf_j|\,|f_jRf_i|\} \leqslant |\mathrm{Rad}(R)| = p^m,$$

we conclude that $|E| = m$ and $|f_iRf_j|\,|f_jRf_i| = p$ for each $(i,j) \in E$. Since $R = \bigoplus_{i,j=1}^{m+1} f_iRf_j$ as additive group, this implies $\mathrm{char}(R) = p$. Therefore R is a $(2m+1)$-dimensional algebra over $GF(p)$. This completes the proof. □

We shall give an example of a ring satisfying the second equality in Theorem 2.

EXAMPLE. Let e_{ij} be the standard matrix units in $M_{m+1}(GF(p))$ and consider the subalgebra

$$R = \sum_{i=1}^{m+1} GF(p)e_{ii} + \sum_{j=2}^{m+1} GF(p)e_{1j}.$$

Then R is a directly indecomposable ring such that $|\mathrm{Rad}(R)| = p^m$ and $\delta(R) = 1 - 1/p^m$.

Note that $1+\mathrm{Rad}(R)$ is a (normal) subgroup of the group R^*, so that $|\mathrm{Rad}(R)| \leqslant |R^*|$. Thus the following improves Stewart [7, Corollary 2.5] in case R is a directly indecomposable finite $2'$-ring with nonzero radical.

COROLLARY 2. *If R is a directly indecomposable non-simple finite $2'$-ring, then* $|R| < |R^*|\,|\mathrm{Rad}\,(R)|$.

PROOF: By hypotheses, $|\mathrm{Rad}\,(R)| = p^m$ for some prime $p > 2$ and some positive integer m. By Theorem 2 we have

$$|R| \leqslant \left(\frac{p}{p-1}\right)^{m+1} |R^*|.$$

Now, since $p > 2$, we have

$$\left(\frac{p}{p-1}\right)^{m+1} < p^m = |\mathrm{Rad}\,(R)|.$$

$\square$

REFERENCES

[1] H.K. Farahat, 'The multiplicative groups of a ring', *Math. Z.* **87** (1965), 378–384.

[2] F.J. Flanigan, 'Radical behavior and the Wedderburn family', *Bull. Amer. Math. Soc.* **79** (1973), 66–70.

[3] M. Hall, 'The position of the radical in an algebra', *Trans. Amer. Math. Soc.* **48** (1940), 391–404.

[4] D. Mainwaring and K.R. Pearson, 'Decomposability of finite rings', *J. Austral. Math. Soc. Ser. A* **28** (1979), 136–138.

[5] B.R. McDonald, *Finite rings with identity* (Marcel Dekker, New York, 1974).

[6] R. Raghavendran, 'Finite associative rings', *Compositio Math.* **21** (1969), 195–229.

[7] I. Stewart, 'Finite rings with a specified group of units', *Math. Z.* **126** (1972), 51–58.

Department of Mathematics
Okayama University
Okayama 700
Japan

Department of Mathematics
Aichi Institute of Technology
Yakusa-chô, Toyota, 470-03
Japan