ON THE PRODUCT OF ALL NONZERO ELEMENTS OF A FINITE RING

by PETER Z. HERMANN*

(Received 19 May, 1987)

The aim of the present note is to describe the possible products when taking all the nonzero elements of a finite ring in some sequence. Compared with the analogous situation for finite groups, where the set of products of all elements has been shown in **[2]** to be a whole coset of the derived group, for rings the set of the above mentioned products will be proved either to be as large as possible or to consist of one or two elements only.

NOTATION. Let $H=\{r_1, r_2, \ldots, r_k\}$ be a subset of cardinality k in a finite ring; we denote by $p(H)$ the set $\{r_{\pi(1)}r_{\pi(2)}\cdots r_{\pi(k)}:\pi\in\Sigma_k\}$, where Σ_k stands for the symmetric group on k letters. If $V=V(n,q)$ is an n-dimensional vector space over the q-element field and $1\leqslant t\leqslant n$, we write $\mathrm{Hom}(V;t)$ for the set of linear mappings of V (into itself) of rank t and $\mathrm{Hom}(V)$ for the set of all V to V linear mappings. We write A_t for the set of all t-dimensional subspaces of V.

Our main result can be formulated as follows.

THEOREM. *Let R be a finite ring.*

(1) *If R is a finite field or the* 2*-element zero ring then $p(R\backslash\{0\})$ consists of a single* (*certainly nonzero*) *element only.*

(2) (a) *If R is isomorphic to the ring of* 2 *by* 2 *upper triangular matrices over the* 2*-element field with zero trace then* $p(R\backslash\{0\})=\left\{\begin{bmatrix}0&1\\0&0\end{bmatrix}\right\}$.

(b) *If R is $\mathbb{Z}/4\mathbb{Z}$, the ring of the residue classes of the rational integers modulo* 4, *then* $p(R\backslash\{0\})=\{\bar{2}\}$.

(c) *If R is isomorphic to the whole ring of* 2 *by* 2 *upper triangular matrices over the* 2*-element field then* $p(R\backslash\{0\})=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix}\right\}$.

(d) *If R is*

$$\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}1&1\\0&0\end{bmatrix}\right\}\quad or\quad\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\1&0\end{bmatrix}\right\}$$

over the two-element field, then

$$p(R\backslash\{0\})=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix}\right\}\quad or\quad\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&0\end{bmatrix}\right\},$$

respectively.

(3) *If $V=V(n,q)$, $R=\mathrm{Hom}(V)$ and $n\geqslant 2$ then $p(R\backslash\{0\})=\mathrm{Hom}(V;1)\cup\{0\}$.*

(4) *$p(R\backslash\{0\})=\{0\}$ in all other cases.*

* Research supported by Hungarian National Foundation for Scientific Research grant no. 1813.

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press

The first (and main) step in the proof is to handle case (3). To do so we need some lemmas.

LEMMA 1. *Let $V=V(n,q)$, $n\geqslant 2$ and $1\leqslant r\leqslant n-1$ with $r\neq\frac{1}{2}n$; there exists a bijection m on $A_r\cup A_{n-r}$ such that*

(i) $U\in A_r\cup A_{n-r}\Rightarrow U\oplus U^m=V$,

(ii) $(U^m)^m=U\,(\forall U\in A_r\cup A_{n-r})$.

Proof. Consider the simple bipartite graph $\mathcal{G}$ with $V(\mathcal{G})=A_r\cup A_{n-r}$ and $E(\mathcal{G})=\{(U,W)\colon U\in A_r,\ W\in A_{n-r},\ U\oplus W=V\}$. As $\mathcal{G}$ is regular, it possesses a 1-factor giving m.

LEMMA 2. *Let $V=V(n,q)$, $f\in\operatorname{Hom}(V;r)$, $1\leqslant r\leqslant n-1$, $r\neq\frac{1}{2}n$, and let m denote any bijection which fulfils* (i) *and* (ii) *of Lemma* 1. *There exists a unique $f^-\in\operatorname{Hom}(V;r)$ such that*

$$\ker(f^-)=(\operatorname{Im}(f))^m,\qquad \operatorname{Im}(f^-)=(\ker(f))^m,$$

$$ff^-f=f.$$

Proof. Let $U=(\ker(f))^m$. As $U\cap\ker(f)=\{0\}$, the restriction g of f to U is one to one from U to $\operatorname{Im}(f)$, and $\operatorname{Im}(g)=\operatorname{Im}(f)$ since $U+\ker(f)=V$. The restriction of f^- to $\operatorname{Im}(f)$ can be nothing but the (unique) inverse of g, and, since $\operatorname{Im}(f)\oplus(\operatorname{Im}(f))^m=V$, such an f^- does exist.

COROLLARY 1. *In the notation of the above lemma, $(f^-)^-=f$.*

It is useful to fix a bijection m (in Lemma 1) for the case $r=1$. Therefore we prove the following result.

LEMMA 3. *Let $V=V(n,q)$, $n>2$. Denote by $\mathcal{G}$ the simple bipartite graph with $V(\mathcal{G})=A_1\cup A_{n-1}$ and $E(\mathcal{G})=\{(U,W)\colon U\in A_1, W\in A_{n-1}, U\cap W=\{0\}\}$; then $\mathcal{G}$ possesses a Hamilton cycle.*

Proof. A_1 and A_{n-1} are of size $(q^n-1)/(q-1)$; so $v=|V(G)|=2(q^n-1)/(q-1)$. Each vertex of $\mathcal{G}$ has degree $d=(q^n-q^{n-1})/(q-1)=q^{n-1}$. Thus $d>\frac{1}{4}v$ and, by Chvátal's result (see [**1**, Ex. 4.2.6, p. 61]), there exists a Hamilton cycle in $\mathcal{G}$.

DEFINITION 1. For all V of dimension at least three, we fix a Hamilton cycle $(U_1,U_2,\ldots,U_v)$ (guaranteed by the previous lemma), and by means of that define the bijection μ on $A_1\cup A_{n-1}$ in the following way:

$$U_i^\mu=\begin{cases}U_{i+1} & \text{if } i \text{ is odd,}\\ U_{i-1} & \text{if } i \text{ is even.}\end{cases}$$

COROLLARY 2. *The bijection μ satisfies the requirements* (i) *and* (ii) *of Lemma* 1 (*for* $r=1$).

PROPOSITION 1. $p(\operatorname{Hom}(V;1))\neq\{0\}$.

Proof. Firstly assume $n>2$. By Corollary 2 and Lemma 2 (using μ for m),

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press

we can express $\operatorname{Hom}(V;1)$ as the union of pairwise disjoint sets B, B^- and S with

$$B^- = \{f^- : f \in B\},$$
$$S = \{f \in \operatorname{Hom}(V;1) : f = f^-\}.$$

Let $C = \{ff^- : f \in B\}$; then $C \subseteq S$, and hence $p(\operatorname{Hom}(V;1)) \supseteq p(S)$. For the elements of S, we obviously have

$$\ker(g) = (\operatorname{Im}(g))$$

Hence

$$\ker(g) = \ker(h) \Leftrightarrow \operatorname{Im}(g) = \operatorname{Im}(h).$$

Thus if $g, h \in S$ and $\ker(g) = \ker(h)$ then $gh \in S$ and

$$\ker(gh) = \ker(g) = \ker(h), \qquad \operatorname{Im}(gh) = \operatorname{Im}(g) = \operatorname{Im}(h)$$

Therefore $p(\operatorname{Hom}(V;1)) \supseteq p(T)$, where T is some subset of S satisfying

$$\{\ker(f) : f \in T\} = A_{n-1},$$
$$\{\operatorname{Im}(f) : f \in T\} = A_1,$$
$$\ker(f) = \ker(g) \Leftrightarrow f = g \qquad (f, g \in T).$$

Now consider the graph $\mathscr{G}$ in Lemma 3. We can assume $U_1 \in A_{n-1}$, and hence $T = \{f_2, f_4, \ldots, f_v\}$ with $\ker(f_{2i}) = U_{2i-1}$, $\operatorname{Im}(f_{2i}) = U_{2i}$. Since $(U_{2i}, U_{2i+1}) \in E(\mathscr{G})$, $f_{2i+2}f_{2i} \neq 0$. That yields

$$0 \neq f_v f_{v-2} \ldots f_4 f_2 \in p(T) \subseteq p(\operatorname{Hom}(V;1)).$$

Turning to the case $n = 2 < q$, one defines the simple graph $\mathscr{H}$ by $V(\mathscr{H}) = \operatorname{Hom}(V;1)$, $E(\mathscr{H}) = \{(f, g) : f \neq g,\ fg \neq 0 \neq gf\}$. Let $f \in V(\mathscr{H})$; there are $(q^2 - q)/(q-1) = q$ choices for $\ker(g)$ to get $gf \neq 0$ and similarly q choices for $\operatorname{Im}(g)$ to fulfil $fg \neq 0$. Thus the degree of f in $\mathscr{H}$ is at least

$$d = q^2(q-1) - 1 > \frac{1}{2}\frac{q^2-1}{q-1}(q^2-1) = \tfrac{1}{2}|V(\mathscr{H})|.$$

So, by Dirac's theorem, there exists a Hamilton cycle in $\mathscr{H}$ (see [3]). Taking the product according to the sequence of any Hamilton path we get a nonzero element. As for the remaining case of $n = 2 = q$,

$$\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&1\\0&1\end{bmatrix}\begin{bmatrix}0&0\\1&1\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}0&0\\1&0\end{bmatrix}\begin{bmatrix}1&1\\1&1\end{bmatrix}\begin{bmatrix}0&0\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&0\end{bmatrix}\begin{bmatrix}1&1\\0&0\end{bmatrix}=\begin{bmatrix}1&1\\0&0\end{bmatrix}$$

directly shows that $p(\operatorname{Hom}(V;1)) \neq \{0\}$.

Lemma 4. *Let* $\operatorname{Hom}(V;1) = \{f_1, f_2, \ldots, f_v\}$ $(f_i \neq f_j$ *for* $i \neq j)$, *and let* $P = \{g_1, g_2, \ldots, g_v\} \subseteq \operatorname{Hom}(V;1)$ *with* $\ker(g_i) = \ker(f_i)$, $\operatorname{Im}(g_i) = \operatorname{Im}(f_i)$, $(\forall i \leq v)$. *If* $f_1 \ldots f_v \neq 0$ *then* $g_1 \ldots g_v \neq 0$.

Proof. Trivial.

Proposition 2. *Let* $V = V(n, q)$; *then* $p\Bigl(\bigcup_{1 \leq k \leq n-1} \operatorname{Hom}(V;k)\Bigr) \supseteq L$ *with* $\{\ker f : f \in L\} = A_{n-1}$.

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press

Proof. By Proposition 1, it can be assumed that $n>2$. Let $2\leqslant k\leqslant n-1$ and $k\neq\frac{1}{2}n$; as a consequence of Lemma 2, $\mathrm{Hom}(V;k)=B\cup B^{-}\cup C$ with

$$B\cap B^{-}=B\cap C=B^{-}\cap C=\varnothing,$$
$$B^{-}=\{f^{-}:f\in B\},$$
$$C=\{f\in\mathrm{Hom}(V;k):f^{-}=f\}.$$

Suppose $g\in C\cup\{ff^{-}:f\in B\}$; then there exists a nonzero vector $v\in V$ such that $g(v)=\pm v$; taking $h\in\mathrm{Hom}(V;1)$ to satisfy $v\in\mathrm{Im}(h)$, we have $\ker(gh)=\ker(h)$, $\mathrm{Im}(gh)=\mathrm{Im}(h)$. Therefore, by Lemma 4, h can be replaced by gh in Proposition 1. Having done that procedure for all members of $\mathrm{Hom}(V;k)$ (for all k), we get rid of $\mathrm{Hom}(V;k)$ (for $\frac{1}{2}n\neq k>1$) and have to deal only with $k=\frac{1}{2}n$.

Now suppose $n=2r>2$, and take $\mathrm{Hom}(V;r)=\bigcup_{0\leqslant i\leqslant r}H_i$, where

$$H_i=\{f\in\mathrm{Hom}(V;r)\colon \dim(\ker(f)\cap\mathrm{Im}(f))=r-i\}.$$

Assume $r>i>0$. Let V_1, V_2 be subspaces of V of dimension r and suppose that $\dim(V_1\cap V_2)=r-i$. Choose a basis $\{a_1,\ldots,a_i,\ c_1,\ldots,c_i,\ b_1,\ldots,b_{r-i}\}$ of V_1+V_2 so that $\{a_1,\ldots,a_i,\ b_1,\ldots,b_{r-i}\}\subset V_1$, $\{c_1,\ldots,c_i,\ b_1,\ldots,b_{r-i}\}\subset V_2$. Let $V=(V_1+V_2)\oplus W$, and denote by U_1 and U_2 the subspaces with bases $\{a_1+c_1,\ldots,a_i+c_i\}$ and $\{b_1+a_1+c_2,\ a_2+c_3,\ldots,a_i+c_1\}$ respectively. Now, if $W_j=U_j\oplus W$ $(j=1,2)$ then $W_1\cap W_2=W$ is of dimension $r-i$ and $V_j\cap W_t=\{0\}$ for any $j,t\in\{1,2\}$.

Let $D_i=\{\langle M,N\rangle\in A_r\times A_r\colon \dim(M\cap N)=r-i\}$. Then the elements of D_i can be divided into two subsets $D_i^{(1)}$ and $D_i^{(2)}$ so that

$$\langle M,N\rangle\in D_i^{(1)}\Leftrightarrow\langle N,M\rangle\in D_i^{(2)}.$$

We define the simple graph $\mathcal{G}_i$ with $V(\mathcal{G}_i)=D_i$,

$$E(\mathcal{G}_i)=\{(\langle K_1,K_2\rangle,\langle L_1,L_2\rangle)\in D_i^{(1)}\times D_i^{(2)}:K_j\cap L_s=\{0\}\}.$$

The previous construction of W_1, W_2 shows that $E(\mathcal{G}_i)$ is nonempty. As $\mathcal{G}_i$ is obviously regular bipartite, it has a 1-factor given by some bijection b. Let $f\in H_i$; then, by means of b, we can define f^{-} to be the unique mapping in H_i which satisfies

$$\ker(f^{-})=(\mathrm{Im}(f))^{b},\qquad \mathrm{Im}(f^{-})=(\ker(f))^{b},$$
$$v\in\mathrm{Im}(f)\Rightarrow ff^{-}(v)=v.$$

For $g\in H_r$, g^{-} can be defined uniquely by

$$\ker(g^{-})=\ker(g),\ \mathrm{Im}(g^{-})=\mathrm{Im}(g),$$
$$v\in\mathrm{Im}(f)\Rightarrow gg^{-}(v)=v.$$

From now on, one can proceed in the same way as at the earlier elimination of $\mathrm{Hom}(V;k)$ (for $k\neq\frac{1}{2}n$); this leads to some z with

$$0\neq z\in p\Big(\bigcup_{1\leqslant k\leqslant n-1}\mathrm{Hom}(V;k)\backslash H_0\Big).$$

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press

For H_0, we consider the simple graph $\mathscr{H}$ with

$$V(\mathscr{H})=H_0,\ E(\mathscr{H})=\{(f,g):\ker(f)\cap\ker(g)=\{0\}\}.$$

It should be mentioned that, for the members of H_0, kernels and images coincide so

$$(f,g)\in E(\mathscr{H})\Leftrightarrow\operatorname{rank}(fg)=\operatorname{rank}(gf)=r.$$

As $\mathscr{H}$ is regular, $V(\mathscr{H})$ is the disjoint union of the vertex sets of some cycles K_1, $K_2,\ldots,K_s$: those of length two are also allowed. Let K_1 look like $(f_1,f_2,\ldots,f_k)$ $(k\geqslant 2)$. It cannot happen that $\operatorname{Im}(z)\subseteq\ker(f_1)\cap\ker(f_2)$, since by $(f_1,f_2)\in E(\mathscr{H})$, $\{0\}=\operatorname{Im}(f_2)\cap\ker(f_1)=\ker(f_2)\cap\ker(f_1)$. Thus we can assume $\operatorname{Im}(z)\cap\ker(f_1)=\{0\}$ (since $\dim(\operatorname{Im}(z))=1$). Hence $z_2=f_kf_{k-1}\ldots f_2f_1z\neq 0$. The same argument works for z_2 and k_2, etc., yielding $0\neq h\in p(\bigcup_{1\leqslant k\leqslant n-1}\operatorname{Hom}(V;k))$. Let $L=\{g^{-1}hg:g\in\operatorname{Hom}(V;n)\}$. Then $L\subseteq p(\bigcup_{1\leqslant k\leqslant n-1}\operatorname{Hom}(V;k))$ and $\{\ker f:f\in L\}=\{g^{-1}(\ker h):g\in\operatorname{Hom}(V;n)\}=A_{n-1}$.

PROPOSITION 3. *$p(\operatorname{Hom}(V)\backslash\{0\})=\operatorname{Hom}(V;1)\bigcup\{0\}$ provided $\dim(V)=n\geqslant 2$.*

Proof. As $0\in p(\operatorname{Hom}(V)\backslash\{0\})\subseteq\operatorname{Hom}(V;1)\cup\{0\}$, all we have to prove is $\operatorname{Hom}(V;1)\subseteq p(\operatorname{Hom}(V)\backslash\{0\})$. Let $G=\operatorname{Hom}(V;n)$, and denote the derived group of G by G^1. It is known that $p(G)$ is a coset of G^1 (see [**2**]), and it is easy to see that this coset is actually G^1, except when the Sylow 2-subgroups of G are (nontrivial) cyclic. For our G, that happens only if $n=2=q$; then, using the matrix form of the elements of G, $p(G)=\left\{\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}0&1\\1&0\end{bmatrix}\right\}$. Otherwise $p(G)=G^1$ holds, and G^1 consists of the elements of G whose determinant is 1. In both cases, $p(G)$ permutes the nonzero vectors of V transitively.

We can use Proposition 2 to deduce: for any subspace U of V of dimension $n-1$, there exists a mapping $f_U\in p(\operatorname{Hom}(V)\backslash(G\cup\{0\}))$ such that $\ker(f_U)=U$. Let $u\in V\backslash U$ and $w\in V\backslash\{0\}$. Then $g(f_U(u))=w$ for a suitable $g\in p(G)$. Hence $gf_U\in p(\operatorname{Hom}(V)\backslash\{0\})$; i.e. $p(\operatorname{Hom}(V)\backslash\{0\})$ contains any prescribed element of $\operatorname{Hom}(V;1)$.

Proof of the theorem. Assume that 0 is the only nilpotent ideal of R. Then, by the Wedderburn–Artin theorems, R is the direct sum of ideals $I_1,\ldots,I_k$, where each I_i is isomorphic to $\operatorname{Hom}(V_i)$ for suitable finite vector spaces V_i. If $k=1$, we get (3) from Proposition 3. Suppose that $k\geqslant 2$; let $a_1\in I_1\backslash\{0\}$, $a_2\in I_2\backslash\{0\}$. Then all elements of $p(R\backslash\{0\})$ are of the form $c=xa_iya_jz$ (some of x,y,z may be empty). That form immediately implies $c\in I_1\cap I_2=0$. Exclude the trivial case of the 2-element zeroring and suppose that R possesses nonzero nilpotent ideals. There must exist a nonzero ideal I with $I^2=0$ as well. If I has at least three elements then, with a_1, $a_2\in I\backslash\{0\}$ and $a_1\neq a_2$, we have every element of $p(R\backslash\{0\})$ of the form xa_iya_jz, obviously belonging to $II=0$. Thus $I=\{0,\rho\}$ can be assumed. Let $L=\{x\in R:xI=0\}$, $K=\{y\in R:Iy=0\}$; K and L are ideals in R, and the factor rings R/K, R/L are subrings in the endomorphism ring of the additive group of I; that implies $|R/K|$, $|R/L|\leqslant 2$. Suppose that $a\in(K\cap L)\backslash I$. Then

$$p(R\backslash\{0\})\subseteq\{xay\rho z,x\rho yaz:x,y,z\in R\cup\{1\}\}\subseteq(K\cap L)I\cup I(K\cap L)=0.$$

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press

So we can assume that $K \cap L = I$. Hence $|R/I|$ divides 4. If R has four elements then suppose firstly that the additive group of R is of exponent 2 (i.e. R has characteristic 2); then $R = \{0, \rho, a, b\}$ with $a + b = \rho$.

If $K \cup L = R$, we get (d). Thus we can assume $a\rho = \rho = \rho a$; hence $b\rho = (a + \rho)\rho = a\rho + \rho^2 = \rho$; similarly $\rho b = \rho$, just yielding a^2, $b^2 \in \{a, b\}$. If $\{x, y\} = \{a, b\}$ and $x^2 = y$ then $y^2 = (\rho + x)^2 = \rho^2 + \rho + \rho + x^2 = x^2 = y$; thus $a^2 = a$ can be assumed; whence $b^2 = a$, $ab = ba = (a + \rho)a = a + \rho = b$, and R is isomorphic to the following ring of matrices over the 2-element field: $\left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right\}$. R is commutative and $p(R\backslash\{0\}) = \left\{\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right\}$. Suppose now the additive group of R to be cyclic, i.e. $R = \{0, a, -a, 2a = \rho\}$. Again we have $a\rho = \rho = \rho a$, so $a^2 = a$ can be assumed; thus R turns out to be isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This shows, in particular, $p(R\backslash\{0\}) = \{\bar{2}\}$.

Let us now suppose that $|R| = 8$, and the additive group of R/I is of exponent 2:

$$R = I \cup (I + a) \cup (I + b) \cup (I + a + b).$$

Since $K \cap L = I$, one can assume $a\rho = \rho = \rho a$ and $b\rho = \rho$; then $\rho b = 0$. As $\rho a = \rho$, $a^2 \in (I + a) \cup (I + a + b)$. Suppose $a^2 \in I + a + b$; then $\rho = a^2\rho = (a + b)\rho = 0$, a contradiction; hence $a^2 \in I + a$. Similarly $b^2 \in (I + a) \cup (I + b)$ as $b\rho = \rho$, and $b^2 \in I \cup (I + b)$ as $\rho b = 0$; thus $b^2 \in I + b$. One can get $(a + b)^2 \in I + a + b$ in the same way as well as ba, $ab \in I + b$. Suppose that $b^2 = b + \rho$; then $\rho = b^2 - b$ and b commute, contradicting $b\rho = \rho \neq 0 = \rho b$; thus $b^2 = b$, and for the same reason $2b = 0$. Suppose that $ab = \rho + b$; then $\rho = ab - b$; hence $0 = \rho b = (ab - b)b = ab^2 - b^2 = ab - b = \rho$, a contradiction; so $ab = b$. Should $ba \neq ab$; then $ba = b + \rho$, and we can replace a by $a + \rho = a'$ to get $a'b = b = ba'$. Let $a'^2 = a' + x$ $(x \in I)$; then $b = ba' = b(a')^2 = b(a' + x) = b + bx$; hence $x = 0$ and $a'^2 = a'$. Suppose that $2a' = \rho$; then ρ and b commute, a contradiction; thus $2a' = 0$, i.e. R is of characteristic 2, and the mapping

$$a' \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, b \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \rho \mapsto \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{extends to an isomorphism.}$$

After identification we obviously have $p(R\backslash\{0\}) = \left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right\}$. If at last the additive group of R/I is cyclic then R is commutative, whence $p(R\backslash\{0\}) = \{0\}$ since $K \neq I$.

REFERENCES

1. J. A. Bondy and U. S. R. Murty, *Graph theory with applications* (Macmillan, 1976).

2. J. Dénes and P. Z. Hermann, On the product of all elements in a finite group, *Ann. Discrete Math.* **15** (1982), 105–109.

3. G. A. Dirac, Some theorems on abstract graphs, *Proc. Lond Math. Soc.* (3) **2** (1952), 69–81.

Department of Algebra and Number Theory
Eötvös Loránd University
H-1088 Budapest
Múzeum Krt. 6–8
Hungary

https://doi.org/10.1017/S0017089500007412 Published online by Cambridge University Press