PRIME MATRIX RINGS

R. E. JOHNSON[1]

If F is a ring, then an obvious way to construct subrings of $(F)_n$, the ring of all $n\times n$ matrices over F, is to choose additive subgroups F_{ij} of F such that

$$F_{ij}F_{jk}\subset F_{ik},\qquad i,j,k=1,\cdots,n, \tag{1}$$

and then form the ring

$$R=\sum_{i,j=1}^{n}F_{ij}e_{ij} \tag{2}$$

where the e_{ij} are the usual unit matrices. For example, we could select n left ideals $A_1,\cdots,A_n$ of either F or a subring of F and then let $F_{ij}=A_j$, $i,j=1,\cdots,n$.

If F is a (skew) field and the F_{ij} satisfying (1) are all nonzero, then R defined by (2) is easily shown to be a prime ring. The main result of this paper (1.3) is that if F is a right ring of quotients of F_{11} then $(F)_n$ is a right ring of quotients of R and there exists a subring K of F and a nonzero diagonal matrix $d\in R$ such that $(K)_n$ is a subring of dRd^{-1} and F is a ring of quotients of K. This result is used to give new proofs of the Faith-Utumi theorem [2] and of Goldie's theorem [1].

1. **Prime matrix rings.** If A is a subset of a ring, then let $A'=\{x\in A\mid x\neq 0\}$. If A and B are subsets of a field, then denote by $AB^{-1}=\{ab^{-1}\mid a\in A, b\in B'\}$. The notation $R\leqq S$ is used to show that S is a right ring of quotients of R; that is, that R is a subring of S and $aR\cap R\neq 0$ for all $a\in S'$. It is readily seen that if F is a field and K is a subring of F, then $K\leqq F$ iff $KK^{-1}=F$.

1.1. LEMMA. *Let F be a field and A be a subring of F for which $AA^{-1}=F$. If B and C are nonzero right A-modules contained in F, then $B\cap C\neq 0$ and $BC^{-1}=F$.*

PROOF. For any $f\in F'$, $b\in B'$, and $c\in C'$, there exist $a_i\in A$ such that $b^{-1}fc=a_1a_2^{-1}$. Hence, $f=(ba_1)(ca_2)^{-1}\in BC^{-1}$. We conclude that $BC^{-1}=F$. If $f=1$, then $ba_1=ca_2$ and evidently $B\cap C\neq 0$.

1.2. THEOREM. *Let F be a field, $\{F_{ij}\mid i,j=1,\cdots,n\}$ be a set of*

Received by the editors July 30, 1964.

[1] Research supported in part by NSF Grant G-24155.

nonzero additive subgroups of F satisfying (1), *and R be the prime ring defined by* (2). *Then $R \leqq (F)_n$ iff $F_{11} \leqq F$.*

PROOF. If $R \leqq (F)_n$, then for every $d \in F'$ there exists $a \in R$ such that $(de_{11})a \in R'$. If $a = \sum a_{ij}e_{ij}$, where $a_{ij} \in F_{ij}$, then $da_{1j} \in F'_{1j}$ and $d \in F_{1j}F_{1j}^{-1}$ for some j. Since $fg^{-1} = (fh)(gh)^{-1}$ for all $f, g \in F_{1j}$ and $h \in F_{j1}$, evidently $F_{1j}F_{1j}^{-1} \subset F_{11}F_{11}^{-1}$ for all j. Hence, $F \subset F_{11}F_{11}^{-1}$ and $F_{11} \leqq F$.

Conversely, if $F_{11} \leqq F$ then $F_{i1}F_{j1}^{-1} = F$ for all i and j by 1.1. Actually, $fg^{-1} = (fh)(gh)^{-1}$ for all $f \in F'_{i1}$, $g \in F'_{j1}$, $h \in F'_{1k}$ so that $F_{ik}F_{jk}^{-1} = F$ for all i, j, k. Since each F_{ik} is a right F_{kk}-module, the F_{kk}-module $F_k = \bigcap_{i=1}^n F_{ik}$ is nonzero and $F_kF_k^{-1} = F$ by 1.1. Clearly each F_k is a subring of F. Thus, R contains a subring S of the form

$$S = \sum_{i,j=1}^{n} F_j e_{ij} \tag{3}$$

where the F_j are subrings of F satisfying

$$F_iF_j \subset F_j, \qquad F_i \leqq F, \qquad i, j = 1, \cdots, n. \tag{4}$$

To complete the proof of 1.2, we need only prove that $S \leqq (F)_n$. Let $a = \sum a_{ij}e_{ij} \in (F)_n$, with $a_{rs} \neq 0$. Then there exist $b_i \in F'_s$ such that $a_{is}b_i \in F_s$ for each i. Since $b_1F_s \cap \cdots \cap b_nF_s \neq 0$ by 1.1, there exists some $b \in F'_s$ such that $a_{is}b \in F_s$ for each i. Hence, $a(be_{ss}) = \sum a_{is}be_{is} \in S$. Therefore, $S \leqq (F)_n$ and 1.2 is proved.

It is easy to give an example showing that $F_1 \cap \cdots \cap F_n$ might be zero in ring S of (3). Thus, if D is a right Ore domain having right field of quotients F (i.e., $DD^{-1} = F$) but D is not a left Ore domain (i.e., $D^{-1}D \neq F$), then there exist nonzero left ideals F_i of D such that $F_1 \cap \cdots \cap F_n = 0$. Still, $S \leqq (F)_n$ if S is defined by (3). Although the intersection of the F_k might be zero, the intersection of the corresponding subrings of F in some isomorphic image of S in $(F)_n$ is nonzero as we shall now show.

Let S be a subring of $(F)_n$ defined by (3) and (4) above, and let $g_i \in F'_i$, $i = 1, \cdots, n$. If $f_k = g_1g_2 \cdots g_k$, $k = 1, \cdots, n$, then clearly each $f_k \in F'_k$ and $d = \sum f_ie_{ii}$ has inverse $d^{-1} = \sum f_i^{-1}e_{ii}$ in $(F)_n$. Let

$$T = dSd^{-1} = \sum_{i,j=1}^{n} (f_iF_jf_j^{-1})e_{ij},$$

an isomorphic image of S. Evidently $T \leqq (F)_n$. Since $f_naf_1^{-1} = f_ig_{i+1} \cdots g_nag_2 \cdots g_jf_j^{-1} \in f_iF_jf_j^{-1}$ for all $a \in F_1$, clearly

$$\bigcap_{i,j=1}^{n} f_iF_jf_j^{-1} = f_nF_1f_1^{-1}.$$

If we let $K = f_n F_1 f_1^{-1}$, then K is a subring of F for which $KK^{-1} = F$ by 1.1. Evidently $(K)_n \subset T$ and also $(K)_n \leqq (F)_n$ by 1.2. We have proved the following result.

1.3. THEOREM. *Let F be a field, F_{ij} be nonzero additive subgroups of F satisfying* (1), *and R be the prime ring defined by* (2). *If $F_{11} \leqq F$, then there exists a subring K of F and a nonsingular diagonal matrix $d \in R$ such that $KK^{-1} = F$ and $(K)_n \leqq dRd^{-1} \leqq (F)_n$.*

2. **The annihilator ideal lattice.** In order to apply the theorems of §1 to prime rings in general, we need the following lattice-theoretic results. Since we wish to use these results in another context [7], we shall state them in as general terms as possible.

Let R be a ring, L_r be the lattice of right ideals of R, and R_r^Δ be the right singular ideal of R. Thus, $b \in R_r^\Delta$ iff $b^r = \{x \in R \mid bx = 0\}$ is a large right ideal; i.e., $b^r \cap A \neq 0$ for all nonzero $A \in L_r$. If $R_r^\Delta = 0$, then we denote the lattice of closed right ideals of R by L_r^*. Thus, $A \in L_r^*$ iff A is the only essential extension of A in L_r. It is well-known that L_r^* is a complete complemented modular lattice.

If L is a lattice containing 0 and I, then a minimal (maximal) element of $L - \{0\}(L - \{I\})$ is called an atom (coatom). If $R_r^\Delta = 0$ and L_r^* is atomic (i.e., every nonzero element of L_r^* contains an atom), then let us denote by R_r^0 the union in L_r of all atoms of L_r^*. A ring R is called (right) *stable* [6] iff $R_r^\Delta = 0$, L_r^* is atomic, and $(R_r^0)^r = 0$. Not only is every prime ring (for which L_r^* is atomic) stable, but so also is every $n \times n$ triangular matrix ring over a right Ore domain.

Another lattice associated with a ring R is the lattice J_r of annihilating right ideals of R. If $R_r^\Delta = 0$ then J_r is a subset, although not necessarily a sublattice, of L_r^*. However, intersections are set-theoretic in both lattices.

Needless to say, the corresponding left structure of a ring R is indicated by replacing each "r" above by an "l".

The following lemma, due to Koh [3], is basic to the work of this section. Our proof is a paraphrase of Koh's proof for prime rings.

2.1. LEMMA. *If R is a stable ring then $R_l^\Delta = 0$.*

PROOF. If $R_l^\Delta \neq 0$ and $d \in (R_l^\Delta)'$, then $Ad \neq 0$ for some atom $A \in L_r^*$ and $ad \neq 0$ for some $a \in A'$. Since $Ra \cap d^l \neq 0$, $xa \neq 0$ and $xad = 0$ for some $x \in R'$. However, a^r is a coatom of L_r^* by [4, 6.9] and therefore $(xa)^r = a^r$. This contradiction proves the lemma.

The lattices J_r and J_l are dual isomorphic under the correspondence $A \to A^l$, $A \in J_r$. If R is a stable ring then the lattice J_l is atomic. Actually, let us show that if A, $B \in J_l$ with $A \cap B \neq B$, then there exists an atom $C \in J_l$ such that $C \subset B$ and $C \cap A = 0$. By 2.1, $L_l^* \supset J_l$ and there exists some nonzero $D \in L_l^*$ such that $D \subset B$ and $D \cap A = 0$. Since R is stable, $ED \neq 0$ and hence $E \cap D \neq 0$ for some atom $E \in L_r^*$. If $d \in (E \cap D)'$, then d^r is a coatom of L_r^* by [4, 6.9]. Therefore, d^r is a coatom of J_r and $C = d^{rl}$ is an atom of J_l. Clearly $C \subset B$ and $C \cap A = 0$.

If B is any atom of J_l then B^r is a coatom of L_r^* by the proof above. Thus, if B covers 0 in J_l then $0^r = R$ covers B^r in L_r^*. This is a special case of the following result.

2.2. Lemma. *Let R be a stable ring and A, $B \in J_l$. Then B is a cover of A in J_l iff A^r is a cover of B^r in L_r^*.*

Proof. If A^r is a cover of B^r in L_r^*, then A^r is a cover of B^r in J_r and B is a cover of A in J_l. Conversely, if B is a cover of A in J_l then there exists an atom $C \in J_l$ such that $C \subset B$ and $C \cap A = 0$. Clearly $B = A \cup C$ in J_l. Hence, $B^r = A^r \cap C^r$. Since C^r is a coatom of L_r^* and $A^r \not\subset C^r$, evidently $A^r \cup C^r = R$ in L_r^*. Therefore, the intervals $[C^r, R]$ and $[A^r \cap C^r, A^r]$ are isomorphic and A^r covers $A^r \cap C^r = B^r$.

The main result of this section is as follows.

2.3. Theorem. *If R is a stable ring then the lattice J_l is upper semimodular.*

Proof. Let A, $B \in J_l$ be covers of $A \cap B$. Then $(A \cap B)^r$ covers A^r and B^r in L_r^* by 2.2. Hence, $(A \cap B)^r = A^r \cup B^r$ in L_r^*. By the modularity of L_r^*, A^r and B^r cover $A^r \cap B^r$. Therefore, $A \cup B$ $[= (A^r \cap B^r)^l]$ covers A and B in J_l by 2.2. This proves 2.3.

If the lattice L_r^* has a finite dimension n, then we call n the (right) *dimension* of R and write $\dim R = n$.

2.4. Corollary. *If R is a stable ring such that* $\dim R = n$, *then J_l is a complemented lattice of dimension n.*

Proof. Every maximal chain in J_l has length by 2.2, and therefore $\dim J_l = n$. To show that J_l is complemented, let A, $B \in J_l$ with $A \cap B = 0$ and $A \cup B \neq R$. Then there exists an atom $C \in J_l$ such that $C \cap (A \cup B) = 0$. We claim that $A \cap (B \cup C) = 0$ in J_l. If this is so, then by induction there exists some $D \in J_l$ such that $A \cap D = 0$ and $A \cup D = R$. Hence, J_l is complemented.

If $A \cap (B \cup C) \neq 0$, then there exists an atom $E \in J_l$ such that $E \subset A \cap (B \cup C)$. Then $E \cap B = 0$, $E^r \supset A^r$, and $E^r \supset B^r \cap C^r$. Clearly $C^r \cup (A^r \cap B^r) = R$ in L_r^*. Hence, $B^r = B^r \cap [C^r \cup (A^r \cap B^r)] = (B^r \cap C^r) \cup (A^r \cap B^r)$ and $E^r \supset B^r$, contrary to the fact that $E \cap B = 0$. Hence, $A \cap (B \cup C) = 0$.

The lattice J_l of a stable ring R is not necessarily modular, as the following example shows.

2.5. EXAMPLE. Let D be a right Ore domain which is not a left Ore domain, F be the right field of quotients of D, and $R=(D)_3$. Clearly R is a prime ring of dimension 3. Select $g, h\in D'$ such that $Dg\cap Dh=0$, and let $u=ge_{11}+e_{21}$, $v=e_{21}+he_{31}$ in R. Then $u^l=Re_{33}+R(e_{11}-ge_{21})$ and $v^l=Re_{11}+R(he_{12}-e_{13})$. Since re_{11} and re_{33} are atoms of J_l, evidently u^l and v^l are coatoms of J_l. However, $u^l\cup v^l=R$ and $U^l\cap v^l=0$, and therefore J_l is not modular (since it is not lower semi-modular).

3. **Goldie prime rings.** A prime ring R such that $R_r^\Delta=0$ and dim $R=n>1$ is called a *Goldie prime ring*. Such rings were studied by Goldie in [1]. By 2.4, J_l is a complemented, upper semi-modular lattice for such a ring.

Let R be a Goldie prime ring and $n=\dim R$. By 2.4, there exists an independent set $\{B_1, \cdots, B_n\}$ of atoms of J_l (i.e., $(B_1\cup\cdots\cup B_i)\cap B_{i+1}=0$, $i=1,\cdots,n-1$). Hence, $\{B_1^r,\cdots,B_n^r\}$ is an independent set of coatoms of L_r^* (i.e., $(B_1^r\cap\cdots\cap B_i^r)\cup B_{i+1}^r=R$, $i=1,\cdots,n-1$). If we let

$$A_j=\bigcap_{i=1;\, i\neq j}^{n} B_i^r,\qquad j=1,\cdots,n,$$

then we may show lattice-theoretically that $\{A_1,\cdots,A_n\}$ is an independent set of atoms of L_r^*. What is more important, the A_i are in J_r. Clearly

$$B_i^r=\bigcup_{j=1;\, j\neq i}^{n} A_i,\qquad i=1,\cdots,n.$$

A Goldie prime ring R of dimension n has a full ring Q of linear transformations of an n dimensional vector space over a field as a ring of quotients. This is a weaker result than Goldie's theorem [1, Theorem 11]. It is well-known that the lattices $L_r^*(Q)$ and $L_r^*(R)$ are isomorphic under the correspondence $B\rightarrow B\cap R$, $B\in L_r^*(Q)$. (See [5] for proofs.)

Corresponding to the independent set $\{A_1,\cdots,A_n\}$ of atoms of $L_r^*(R)$ defined above is an independent set $\{C_1,\cdots,C_n\}$ of atoms of $L_r^*(Q)$. By [8, Proposition 5, p. 52], there exists a set $\{e_{ij}\}$ of n^2 matrix units in Q such that $C_i=e_{ii}Q$, $i=1,\cdots,n$. Hence, $A_i=(e_{ii}Q)\cap R$ and $B_i^r=(\sum_{j\neq i}e_{jj}Q)\cap R$, $i=1,\cdots,n$. Relative to the chosen set of matrix units of Q, we can find a field F commuting with the e_{ij} such that [5, Proposition 6, p. 52]

$$Q = \sum_{i,j=1}^{n} Fe_{ij} \cong (F)_n.$$

Since B_i^r (in R) $= [B_i^r$ (in Q)$]\cap R$ and B_i^r (in Q)$\in L_r^*(Q)$, evidently B_i^r (in Q) $= \sum_{j\neq i} e_{jj}Q$. Hence, $B_i \subset Qe_{ii}\cap R$ for each i. Actually, $B_i = Qe_{ii}\cap R$ for each i since $[Qe_{ii}\cap R]B_i^r = 0$. Since $A_iB_j \neq 0$ for all i and j, we see that

$$A_i \cap B_j = F_{ij}e_{ij}, \qquad i, j = 1, \cdots, n$$

for some nonzero additive subgroups F_{ij} of F satisfying (1). Hence,

$$S = \sum_{i,j=1}^{n} F_{ij}e_{ij}$$

is a prime subring of R.

Each nonzero left ideal of R has R as a right ring of quotients. In particular, $B_1 \leqq R$ and $L_r^*(B_1) \cong L_r^*(R)$. Therefore, $\{F_{11}e_{11}, \cdots, F_{n1}e_{n1}\}$ is an atomic basis of $L_r^*(B_1)$ and $F_{11}e_{11} + \cdots + F_{n1}e_{n1} \leqq B_1 \leqq R$. Consequently, $S \leqq R \leqq (F)_n$. Now we can apply 1.3 to obtain the following result.

3.1. Faith-Utumi Theorem. *Every Goldie prime ring R of dimension n has associated with it a field F and a subring K of F such that $K \leqq F$ and $(K)_n \leqq R \leqq (F)_n$.*

An immediate corollary of 3.1 is Goldie's theorem, which states that $(F)_n = \{ab^{-1} \mid a, b \in R, b \text{ regular}\}$. In fact, the following stronger result (due to Faith) holds.

3.2. Theorem. *If R is a Goldie prime ring of dimension n and F is its associated field, then there exists a subring K of F such that*

$$(F)_n = \{ak^{-1} \mid a \in R, k \in K'\}.$$

Proof. If $c \in (F)_n$, say $c = \sum a_{ij}b_{ij}^{-1}e_{ij}$ where $a_{ij}, b_{ij} \in K$, then $ck = a \in (K)_n$ for any nonzero $k \in \bigcap b_{ij}K$ and $c = ak^{-1}$ as desired.

Bibliography

1. A. W. Goldie, *The structure of prime rings under ascending chains conditions*, Proc. London Math. Soc. **8** (1958), 589–608.

2. C. Faith and Y. Utumi, *On noetherian prime rings*, Trans. Amer. Math. Soc. **114** (1965), 53–60.

3. K. Koh, *On one sided ideals which are prime rings*, Amer. Math. Monthly (to appear).

4. R. E. Johnson, *Structure theory of faithful rings*. II, Trans. Amer. Math. Soc. **84** (1957), 523–544.

5. ———, *Quotient rings of rings with zero singular ideal*, Pacific J. Math. **11** (1961), 1385–1392.

6. ———, *Rings with zero right and left singular ideals*, Trans. Amer. Math. Soc. **118** (1965), 150–157.

7. ———, *Potent rings*, Trans. Amer. Math. Soc. **119**(1965), 524–534.

8. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. **37**, Amer. Math. Soc., Providence, R. I., 1956.

UNIVERSITY OF ROCHESTER

POWERS IN EIGHTH-GROUPS

SEYMOUR LIPSCHUTZ

1. Introduction. The purpose of this paper is to give an algorithm which decides whether or not an element in an eighth-group is a power. A group G is an eighth-group if it is finitely presented in the form

$$G = \text{gp}(a_1, \cdots, a_n;\ R_1(a_\lambda) = 1, \cdots, R_m(a_\lambda) = 1),$$

where (i) each defining relator is cyclically reduced and (ii) if B_i and B_j are cyclic transforms of R_i and R_j, then less than one-eighth of the length of the shorter one cancels in the product $B_i^{\pm 1}B_j^{\pm 1}$, unless the product is unity. The notation in this paper is the same as that in [**3**]. Note that Lemma 3 and Lemma 4 in [**3**] hold for eighth-groups.

Reinhart [**4**] gives an algorithm to decide, among other things, whether or not elements in certain Fuchsian groups are powers. Note that the Fuchsian group $F(p;\ n_1, \cdots, n_d;\ m)$, see Greenberg [**1**], is an eighth-group if

$$4p + d + m,\ n_1, \cdots, n_d > 8.$$

Hence our algorithm holds for a somewhat wider class of groups and, furthermore, is purely algebraic.

REMARK. Given any word V in a finitely presented group, it is possible to find a cyclically fully reduced word V^* conjugate to V by writing the word V in a circle and then reducing. Such a word V^* will be called a *reduced cyclic transform* of V.

2. The algorithm. First we prove a lemma about eighth-groups G. Here r denotes the length of the largest defining relator in G.

Received by the editors April 3, 1964.