PRIME MATRIX RINGS

R. E. JOHNSON

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

\[
F_{ij} F_{jk} \subset F_{ik}, \quad i, j, k = 1, \ldots, n,
\]

and then form the ring

\[
R = \sum_{i,j=1}^{n} F_{ij} e_{ij}
\]

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

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 \( F_1 \) 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 \( d R d^{-1} \) 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 \( R \leq S \) is used to show that \( S \) is a right ring of quotients of \( R \); that is, that \( R \) is a subring of \( S \) and a \( R \cap S \neq 0 \) for all \( a \in S' \). It is readily seen that if \( F \) is a field and \( K \) is a subring of \( F \), then \( K \leq F \) 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 \( b^{-1} fc = a_0 a_1^{-1} \). 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, \( \{ F_{ij} \mid i, j = 1, \ldots, n \} \) 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 $R \subseteq (F)_n$ iff $F_1 \subseteq F$.

Proof. If $R \subseteq (F)_n$, then for every $d \in F'$ there exists $a \in R$ such that $(de_1)a \in R'$. If $a = \sum a_{ij}e_{ij}$ where $a_{ij} \in F_{ij}$, then $da_{ij} \subseteq F'_{ij}$ and $d \subseteq F_{ij}F_{ij}^{-1}$ for some $j$. Since $f_{g^{-1}} = (fh)(gh)^{-1}$ for all $f, g \in F_{ij}$ and $h \in F_{ji}$, evidently $F_1F_{ij}^{-1} \subseteq F_1F_{ii}^{-1}$ for all $j$. Hence, $F \subseteq F_1F_{ii}^{-1}$ and $F_1 \subseteq F$.

Conversely, if $F_1 \subseteq F$ then $F_1F_{ii}^{-1} = F$ for all $i$ and $j$ by 1.1. Actually, $fg^{-1} = (fh)(gh)^{-1}$ for all $f \in F_{ii}', g \in F_{ii}', h \in F_{ki}$ so that $F_1F_{ki}^{-1} = F$ 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 $F_kF_{kk}^{-1} = F$ by 1.1. Clearly each $F_k$ is a subring of $F$. Thus, $R$ contains a subring $S$ of the form

\begin{equation}
S = \sum_{i,j=1}^n F_{ij}e_{ij}
\end{equation}

where the $F_{ij}$ are subrings of $F$ satisfying

\begin{equation}
F_iF_j \subseteq F_{ij}, \quad F_i \subseteq F, \quad i, j = 1, \ldots, n.
\end{equation}

To complete the proof of 1.2, we need only prove that $S \subseteq (F)_n$. Let $a = \sum a_{ij}e_{ij} \in (F)_n$, with $a_{ij} \neq 0$. Then there exist $b_i \in F_{ii}'$ such that $a_{ii}b_i \in F_i$ for each $i$. Since $b_1F_i \cap \cdots \cap b_nF_i \neq 0$ by 1.1, there exists some $b \in F_i'$ such that $a_{ii}b \in F_i$ for each $i$. Hence, $a(be_{ii}) = \sum a_{ii}be_{ii} \in S$. Therefore, $S \subseteq (F)_n$ 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, $S \subseteq (F)_n$ 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 $g_i \in F_i', \ i = 1, \ldots, n$. If $f_k = g_1g_2 \cdots g_k, \ k = 1, \ldots, n$, then clearly each $f_k \in F_k'$ and $d = \sum f_{i}e_{ii}$ has inverse $d^{-1} = \sum f_{i}^{-1}e_{ii}$ in $(F)_n$. Let

\[ T = dsd^{-1} = \sum_{i,j=1}^n (f_iF_{jj}^{-1})e_{ij} \]

an isomorphic image of $S$. Evidently $T \subseteq (F)_n$. Since $f_iaF_{ii}^{-1} = f_ig_{i+1} \cdots g_nag_2 \cdots g_1F_{jj}^{-1}$ for all $a \in F_i$, clearly

\[ \bigcap_{i,j=1}^n f_iF_{jj}^{-1} = f_nF_1F_1^{-1}. \]
If we let $K = f_n F f^{-1}$, then $K$ is a subring of $F$ for which $KK^{-1} = F$ by 1.1. Evidently $(K)_n \subseteq T$ and also $(K)_n \subseteq (F)_n$ by 1.2. We have proved the following result.

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

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 $R^*_r$ be the right singular ideal of $R$. Thus, $b\in R^*_r$ iff $br = \{x\in R | bx = 0\}$ is a large right ideal; i.e., $b^r \cap A \neq 0$ for all nonzero $A \in L_r$. If $R^*_r = 0$, 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 $L - \{0\}$ (of $L - \{I\}$) is called an atom (coatom). If $R^*_r = 0$ and $L^*_r$ is atomic (i.e., every nonzero element of $L^*_r$ contains an atom), then let us denote by $R^*_0$ the union in $L_r$ of all atoms of $L^*_r$. A ring $R$ is called (right) stable [6] iff $R^*_0 = 0$, $L^*_r$ is atomic, and $(R^*_r)^r = 0$. 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 $R^*_r = 0$ 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 $R^*_0 = 0$.

Proof. If $R^*_0 \neq 0$ and $d \in (R^*_0)'$, then $Ad \neq 0$ for some atom $A \in L^*_r$ and $ad \neq 0$ for some $a \in A'$. Since $Ra \cap d'A \neq 0$, $xa \neq 0$ and $xad = 0$ for some $x \in R'$. However, $a^*$ is a coatom of $L^*_r$ by [4, 6.9] and therefore $(xa)^* = a^*$. This contradiction proves the lemma.

The lattices $J_r$ and $J_l$ are dual isomorphic under the correspondence $A \rightarrow (A')^r$, $A \in J_r$. 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 \( C \in J_i \) such that \( C \subseteq B \) and \( C \cap A = 0 \). By 2.1, \( L_i^* \supset J_i \) and there exists some nonzero \( D \in L_i^* \) such that \( D \subseteq B \) and \( D \cap A = 0 \).

Since \( R \) is stable, \( ED \neq 0 \) and hence \( E \cap D \neq 0 \) for some atom \( E \in L_i^* \). If \( d \in (E \cap D)^* \), then \( d^* \) is a coatom of \( L_i^* \) by \([4, 6.9]\). Therefore, \( d^* \) is a coatom of \( J_i \) and \( C = d^* \) is an atom of \( J_i \). Clearly \( C \subseteq B \) and \( C \cap A = 0 \).

If \( B \) is any atom of \( J_i \) then \( B^* \) is a coatom of \( L_i^* \) by the proof above. Thus, if \( B \) covers \( 0 \) in \( J_i \) then \( 0^* = R \) covers \( B^* \) in \( L_i^* \). This is a special case of the following result.

2.2. Lemma. Let \( R \) be a stable ring and \( A, B \in J_i \). Then \( B \) is a cover of \( A \) in \( J_i \) iff \( A^* \) is a cover of \( B^* \) in \( L_i^* \).

Proof. If \( A^* \) is a cover of \( B^* \) in \( L_i^* \), then \( A^* \) is a cover of \( B^* \) in \( J_i \), and \( B \) is a cover of \( A \) in \( J_i \). Conversely, if \( B \) is a cover of \( A \) in \( J_i \) then there exists an atom \( C \in J_i \) such that \( C \subseteq B \) and \( C \cap A = 0 \). Clearly \( B = A \cup C \) in \( J_i \). Hence, \( B^* = A^* \cap C^* \). Since \( C^* \) is a coatom of \( L_i^* \) and \( A^* \subseteq C^* \), evidently \( A^* \cup C^* = R \) in \( L_i^* \). Therefore, the intervals \([C^*, R]\) and \([A^* \cap C^*, A^*]\) are isomorphic and \( A^* \) covers \( A^* \cap C^* = B^* \).

The main result of this section is as follows.

2.3. Theorem. If \( R \) is a stable ring then the lattice \( J_i \) is upper semimodular.

Proof. Let \( A, B \in J_i \) be covers of \( A \cap B \). Then \( (A \cap B)^* \) covers \( A^* \) and \( B^* \) in \( L_i^* \) by 2.2. Hence, \( (A \cap B)^* = A^* \cup B^* \) in \( L_i^* \). By the modularity of \( L_i^* \), \( A^* \) and \( B^* \) cover \( A^* \cap B^* \). Therefore, \( A \cup B \) covers \( A \) and \( B \) in \( J_i \) by 2.2. This proves 2.3.

If the lattice \( L_i^* \) 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 \( J_i \) is a complemented lattice of dimension \( n \).

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

If \( A \cap (B \cup C) \neq 0 \), then there exists an atom \( E \in J_i \) such that \( E \subseteq A \cap (B \cup C) \). Then \( E \cap B = 0 \), \( E^* \supset A^* \), and \( E^* \cup B^* \cap C^* \). Clearly \( C^* \cup (A^* \cap B^*) = R \) in \( L_i^* \). Hence, \( B^* = B^* \cap [C^* \cup (A^* \cap B^*)] = (B^* \cap C^*) \cup (A^* \cap B^*) \) and \( E^* \cup B^* \), contrary to the fact that \( E \cap B = 0 \). Hence, \( A \cap (B \cup C) = 0 \).
The lattice $J_1$ 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 $R = (D)_Z$. Clearly $R$ is a prime ring of dimension 3. Select $g, h \in D'$ such that $Dg \cap Dh = 0$, and let 

\[ u = ge_{11} + e_{12}, \quad v = e_{11} + he_{11} \in R. \]

Then $u^i = Re_{33} + R(e_{11} - ge_{22})$ and $v^i = Re_{11} + R(he_{11} - e_{13})$. Since $re_{11}$ and $re_{33}$ are atoms of $J_1$, evidently $u^i$ and $v^i$ are coatoms of $J_1$. However, $u^i \cup v^i = R$ and $U^i \cap v^i = 0$, and therefore $J_1$ is not modular (since it is not lower semi-modular).

3. Goldie prime rings. A prime ring $R$ such that $R^2 = 0$ and $\dim R = n > 1$ is called a Goldie prime ring. Such rings were studied by Goldie in [1]. By 2.4, $J_1$ 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 \{ $B_i, \cdots, B_n$ \} of atoms of $J_1$ (i.e., $(B_i \cup \cdots \cup B_i) \cap B_{i+1} = 0$, $i = 1, \cdots, n - 1$). Hence, \{ $B_i, \cdots, B_n$ \} is an independent set of coatoms of $L^*_1$ (i.e., $(B_i \cap \cdots \cap B_i) \cup B_{i+1} = R$, $i = 1, \cdots, n - 1$). If we let

\[ A_j = \bigcap_{i=1, i \neq j}^n B_i, \quad j = 1, \cdots, n, \]

then we may show lattice-theoretically that \{ $A_1, \cdots, A_n$ \} is an independent set of atoms of $L^*_1$. What is more important, the $A_i$ are in $J_r$. Clearly

\[ B_i = \bigcup_{j=1, j \neq i}^n A_i, \quad i = 1, \cdots, n. \]

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 $L^*_1(Q)$ and $L^*_1(R)$ are isomorphic under the correspondence $B \mapsto B \cap R$, $B \in L^*_1(Q)$. (See [5] for proofs.)

Corresponding to the independent set \{ $A_1, \cdots, A_n$ \} of atoms of $L^*_1(R)$ defined above is an independent set \{ $C_1, \cdots, C_n$ \} of atoms of $L^*_1(Q)$. 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 $B_i = (\sum_{j \neq i} e_{ij}Q) \cap R$, $i = 1, \cdots, n$. Relative to the chosen set of matrix units of $Q$, we can find a field $F$ commuting with the $e_{ij}$ such that [8, Proposition 6, p. 52]
\[ Q = \sum_{i,j=1}^{n} F_{ij}e_{ij} \cong (F)_n. \]

Since \( B'_t \) (in \( R \)) = \( [B'_t \) (in \( Q \)] \cap R \) and \( B'_t \) (in \( Q \)) \( \subseteq L^*_t(Q) \), evidently \( B'_t \) (in \( Q \)) \( \subseteq \sum_{i=1}^{n} e_{ij}Q \). Hence, \( B_i \cap Qe_{ij} \cap R \) for each \( i \). Actually, \( B_i = Qe_{ij} \cap R \) for each \( i \) since \( [Qe_{ij} \cap R]B'_t = 0 \). Since \( A_iB_j \neq 0 \) for all \( i \) and \( j \), we see that

\[ \bigcap_{i,j} A_i \cap B_j = F_{ij}e_{ij}, \quad i, j = 1, \ldots, n \]

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, \( B_i \subseteq R \) and \( L^*_t(B_i) \cong L^*_t(R) \). Therefore, \( \{F_{t1}e_{i1}, \ldots, F_{n1}e_{n1}\} \) is an atomic basis of \( L^*_t(B_i) \) and \( F_{t1}e_{i1} + \cdots + F_{n1}e_{n1} \subseteq B_i \subseteq R \). Consequently, \( S \subseteq R \subseteq (F)_n \). 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 \( K \subseteq F \) and \( (K)_n \subseteq R \subseteq (F)_n \).*

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 \( k \in b_{ij}K \) and \( c = ak^{-1} \) as desired.

### Bibliography


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

$$G = \langle a_1, \ldots, a_n; R_1(a_1) = 1, \ldots, R_m(a_n) = 1 \rangle,$$

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 $B_i^{-1}B_j$, 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 $F(p; n_1, \ldots, n_d; m)$, see Greenberg [1], is an eighth-group if

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

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.