Houston Journal of Mathematics
© 2006 University of Houston
Volume 32, No. 2, 2006

# PRIME AND RADICAL SUBMODULES OF FREE MODULES OVER A PID

S. HEDAYAT AND R. NEKOOEI

Communicated by Jutta Hausen

Abstract. In this paper the notion of prime matrix is introduced. It is shown that if $R$ is a PID then every full rank prime submodule of $R^{(n)}$ is the row space of a prime matrix. Hence the notion of a prime matrix may be regarded as a generalization of the notion of a prime element. Finally, using prime matrices, we obtain the radical of submodules of $R^{(n)}$, as well as the radical submodules.

## 1. Introduction

Throughout this paper $R$ denotes a principal ideal domain (PID). Note that every PID is a UFD and so a greatest common divisor (GCD) of any collection of elements always exists. Also for every $a, b \in R$ and prime element $p \in R$ such that $p \not| a$ the congruence equation $ax \equiv b \ (mod\ p)$ has a solution. These and other basic results related to PID's which may be found in [1], are essential for the proofs of the results of this article. Now let $M$ be a unitary $R$-module. A submodule $N$ of $M$ is called prime if $N \neq M$ and given $r \in R$, $m \in M$, $rm \in N$ implies $m \in N$ or $r \in (N : M)$, where $(N : M) = \{r \in R : rM \subseteq N\}$. The radical of $N \leq M$ is given by $\text{rad}_M(N) = \cap P$, where the intersection is over all prime submodules of $M$ containing $N$. If there is no prime submodule containing $N$, then we put $\text{rad}_M(N) = M$. $N$ is called a radical submodule if $\text{rad}_M(N) = N$. Let $m$ and $n$ be positive integers and let $A = (a_{ij}) \in M_{m\times n}(R)$. Let $F$ be the free $R$-module $R^{(n)}$. We shall use the notation $< A >$ for the submodule $N$ of $F$ generated by the rows of $A$, and the notation $(r_1, \ldots, r_m)A$, $r_i \in R$ ,for an element of $N$. Let $B \in M_m(R)$. We denote the adjoint matrix of $B$ by $B'$, so

2000 *Mathematics Subject Classification.* 13C13, 13C99.
*Key words and phrases.* Prime submodules, radical of a submodule.

that $BB' = B'B = (\det B)I_m$, where $I_m$ is the $m \times m$ identity matrix. In [5], a characterization of prime submodules is given by prime ideals of $R$ and certain finite systems of equations. We state below another characterization, valid only for PID's, which will be needed in the sequel.

**Theorem 1.1.** *Let $R$ be a PID, $F = R^{(n)}$ and $N$ be a submodule of $F$ with rank $N = m$. Let $N =< A >$ for some $A \in M_{m\times n}(R)$. Then*

*i) If $m < n$, then $N$ is prime if and only if a $GCD$ of the determinants of all $m \times m$ submatrices of $A$ is 1.*

*ii) If $m = n$, then $N$ is prime if and only if there exist an irreducible element $p \in R$, a unit $u \in R$ and a positive integer $\alpha \leq n$, such that $detA = up^{\alpha}$ and a $GCD$ of entries of $A'$ is $p^{\alpha-1}$.*

Proof. Theorem 2.6 in [2]. □

The next result will be widely used in the sequel. The proof is straightforward.

**Lemma 1.2.** *Let $A \in M_n(R)$ , $det(A) \neq 0$ and $A' = (a'_{ij})$ be the adjoint matrix of $A$. Then $(x_1, \ldots, x_n) \in< A >$, for some $x_i \in R$ $(1 \leq i \leq n)$ if and only if $det(A) \mid \sum_{i=1}^{n} x_i a'_{ij}$, for every $j$, $1 \leq j \leq n$.*

Finally, to avoid technical problems, we accept the following convention. If $A = (a_{ij}) \in M_{m\times n}(R)$ then $a_{i0} = a_{0j} = 0$ for all $1 \leq i \leq m, 1 \leq j \leq n$. Also if $(r_1, \ldots, r_n) \in R^{(n)}$ then $r_0 = 0$.

## 2. Prime matrices

In this section we introduce the notion of a prime matrix. As will be shown later, prime matrices provide a useful tool for studying the radical of submodules of $R^{(n)}$. Let $J = \{j_1, \ldots, j_\alpha\}$ be a subset of $\{1, \ldots, n\}$ and let $p \in R$ be a prime element. A matrix $A \in M_n(R), A = (a_{ij})$, is said to be a $p$-prime matrix (or simply prime) if $A$ satisfies the following conditions:

i) $A$ is upper triangular.

ii) For all $i$, $1 \leq i \leq n$, $a_{ii} = p$ if $i \in J$ and $a_{ii} = 1$ if $i \notin J$.

iii) For all $i, j$, $1 \leq i < j \leq n$, $a_{ij} = 0$ except possibly when $i \notin J$ and $j \in J$.

Sometimes we call $J$ the set of integers associated with $A$ and denote it by $J_A$. By (i) and (ii) it is clear that $\det(A) = p^{\alpha}$.

**Lemma 2.1.** *Let $n$ be a positive integer and let $r_i \in R$, $1 \leq i \leq n$. Let $p \in R$ be a prime element and $J = \{j_1, \ldots, j_\alpha\}$ be a subset of $\{1, \ldots, n\}$. Let $J_k = \{0, 1, \ldots, j_k\} - J$, $1 \leq k \leq \alpha$. Then $(r_1, \ldots, r_n) \in< A >$, for some $p$-prime* *matrix* $A \in M_n(R)$ *with* $J_A = J$ *if and only if for every* $k,\ 1 \leq k \leq \alpha$, *the equation* $\sum_{j \in J_k} r_j x_j \equiv r_{j_k}$ $(mod\ p)$ *has a solution.*

Proof. Let $A = (a_{ij})$ be a $p$-prime matrix with $J_A = \{j_1, \ldots, j_\alpha\}$ and let $A' = (a'_{ij})$. For all $i, j,\ 1 \leq i, j \leq n$, it is easy to see that $a'_{ii} = p^{\alpha-1}$ if $i \in J_A$, $a'_{ii} = p^\alpha$ if $i \notin J_A$ and $a'_{ij} = -p^{\alpha-1} a_{ij}$ if $i \neq j$. Hence by Lemma 1.2, $(r_1, \ldots, r_n) \in< A >$ if and only if $p^\alpha \mid \sum_{j=1}^{n} r_j a'_{jl},\ 1 \leq l \leq n$, if and only if $p^\alpha \mid \sum_{j=0}^{l-1} r_j(-p^{\alpha-1} a_{jl}) + p^{\alpha-1} r_l$, for every $l \in J_A$, if and only if $p \mid \sum_{j \in J_k} -r_j a_{jj_k} + r_{j_k},\ 1 \leq k \leq \alpha$, if and only if $\sum_{j \in J_k} r_j a_{jj_k} \equiv r_{j_k}$ $(mod\ p)$ for every $k,\ 1 \leq k \leq \alpha$. □

**Lemma 2.2.** *Let* $m$ *and* $n$ *be positive integers such that* $m < n$. *Suppose that* $B \in M_{n \times m}(R), Y \in M_{n \times 1}(R)$ *and* $X = (x_1, \ldots, x_m)^t$. *Let* $C \in M_{n \times (m+1)}(R)$ *be the augmented matrix* $[B \vdots Y]$. *Let* $p \in R$ *be a prime element. If* $p$ *does not divide the determinant of at least one* $m \times m$ *submatrix of* $B$, *then the system of equations* $BX \equiv Y$ $(mod\ p)$ *has a solution if and only if* $p$ *divides the determinants of all* $(m+1) \times (m+1)$ *submatrices of* $C$.

Proof. Suppose $BX \equiv Y$ $(mod\ p)$ has a solution. Suppose that $C_0$ is an $(m+1) \times (m+1)$ submatrix of $C$. If $Y_0$ is the last column of $C_0$ and $B_0$ consists of all columns of $C_0$ except for $Y_0$, then $B_0 X \equiv Y_0$ $(mod\ p)$, so that $C'_0 B_0 X \equiv C'_0 Y_0$ $(mod\ p)$. The last equation of this system is $0 \equiv \det(C_0)$ $(mod\ p)$. Hence $p \mid \det(C_0)$. Conversely, assume that $p$ divides the determinants of all $(m+1) \times (m+1)$ submatrices of $C$. Let $B_0$ be an $m \times m$ submatrix of $B$ such that $p \nmid \det(B_0)$.Without loss of generality, we may assume that $B_0$ consists of the first $m$ rows of $B$. If $Y_0$ consists of the first $m$ rows of $Y$ then it is easy to see that the system $B_0 X \equiv Y_0$ $(mod\ p)$ has a solution, say $x_i = r_i$ for some $r_i \in R,\ 1 \leq i \leq m$. Let $k$ be an arbitrary positive integer, $m < k \leq n$. Let $C_1 = (c_{ij})$ be the $(m+1) \times (m+1)$ submatrix of $C$ consisting of the first $m$ rows of $C$ and row $k$. If $C'_1 = (c'_{ij})$, then $c'_{(m+1)(m+1)} = \det(B_0)$ and we have $\sum_{j=1}^{m+1} c'_{(m+1)j} c_{ji} = 0$ for every $i,\ 1 \leq i \leq m$. Thus $c'_{(m+1)(m+1)}(\sum_{i=1}^{m} c_{(m+1)i} r_i) = \sum_{i=1}^{m} (c'_{(m+1)(m+1)} c_{(m+1)i}) r_i = \sum_{i=1}^{m} (\sum_{j=1}^{m} -c'_{(m+1)j} c_{ji}) r_i = -\sum_{j=1}^{m} c'_{(m+1)j} (\sum_{i=1}^{m} c_{ji} r_i)$.

As $\sum_{i=1}^{m} c_{ji}r_i \equiv c_{j(m+1)}$ $(mod\ p)$ for all $j, 1 \leq j \leq m$, $-\sum_{j=1}^{m} c'_{(m+1)j}(\sum_{i=1}^{m} c_{ji}r_i) \equiv -\sum_{j=1}^{m} c'_{(m+1)j}c_{j(m+1)}$ $(mod\ p)$. Note that by hypothesis $p \mid \det(C_1)$. Therefore $-\sum_{j=1}^{m} c'_{(m+1)j}c_{j(m+1)} \equiv c'_{(m+1)(m+1)}c_{(m+1)(m+1)}$ $(mod\ p)$.

As $p \not| c'_{(m+1)(m+1)} = \det(B_0)$, the above calculation implies that $\sum_{i=1}^{m} c_{(m+1)i}r_i \equiv c_{(m+1)(m+1)}$ $(mod\ p)$. Since $k$ is arbitrary, we conclude that $x_i = r_i, 1 \leq i \leq m$, is a solution for the system $BX \equiv Y$ $(mod\ p)$. $\square$

The method used in the proof of the following basic result is in fact an algorithm for calculating the prime matrices and finding a generating set of the radical of a submodule [see Theorem 3.4].

**Theorem 2.3.** *Let $m, n$ and $\alpha$ be positive integers such that $m \leq n$ and $1 \leq \alpha \leq n$. Let $B \in M_{m\times n}(R)$ and let $p \in R$ be a prime element. Then $< B > \subseteq < A >$ for some prime matrix $A \in M_n(R)$ with $det(A) = p^{\alpha}$ if and only if $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B$.*

Proof. Let $< B > \subseteq < A >$ for some prime matrix $A$ with $\det(A) = p^{\alpha}$. So there exists $C \in M_{m\times n}(R)$ such that $B = CA$. Let $B_0$ be an $(n-\alpha+1)\times(n-\alpha+1)$ submatrix of $B$. Thus there exist an $(n-\alpha+1)\times n$ submatrix $C_0$ of $C$ and an $n\times(n-\alpha+1)$ submatrix $A_0$ of $A$ such that $B_0 = C_0A_0$. Suppose that $A_1$ is an $(n-\alpha+1)\times(n-\alpha+1)$ submatrix consisting of rows $i_1, \ldots, i_{n-\alpha+1}$ of $A_0$. Since $J_A$ has $\alpha$ elements, hence $i_k \in J_A$ for some $k, 1 \leq k \leq n-\alpha+1$. It follows that the entries of row $i_k$ of $A_0$ are 0 or $p$. Thus $p \mid \det(A_1)$. Hence $p \mid \det(B_0)$, because by the Binet-Cauchy formula [3, Theorem 1], $\det(B_0)$ may be expressed as a linear combination of the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $A_0$. Conversely, assume that $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B$. By adding some zero rows to $B$ if necessary, we may suppose that $B \in M_n(R)$. We use induction on $\alpha$. For $\alpha = 1$, by assumption $p \mid \det(B)$. Let $k$ be the smallest integer such that $p$ divides the determinants of all $k\times k$ submatrices of $B_k$ where $B_k \in M_{n\times k}(R)$ consists of the first $k$ columns of $B$. If $B = (b_{ij})$ then by Lemma 2.2, the system of equations $\{\sum_{j=0}^{k-1} b_{ij}x_j \equiv b_{ik}$ $(mod\ p) \mid 1 \leq i \leq n\}$ has a solution. Therefore by Lemma 2.1, there exists a prime matrix $A$ with $J_A = \{k\}$ such that $< B >\subseteq< A >$. Now suppose that the assertion is true for some $\alpha$, $1 \leq \alpha \leq n-1$. Assume that $p$ divides the determinants of all $(n-\alpha)\times(n-\alpha)$ submatrices of $B = (b_{ij})$. Hence $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B$. Therefore by the induction hypothesis there exists a prime matrix $A$ with $\det(A) = p^{\alpha}$ such that $< B >\subseteq< A >$. Let $J_A = \{j_1,\dots,j_\alpha\}$ and let $J_k = \{0,1,\dots,j_k\} - J_A$, $1 \leq k \leq \alpha$. Fix $k$ for the moment. By Lemma 2.1, the system of equations $\{\sum_{j\in J_k} b_{ij}x_j \equiv b_{ij_k}\ (mod\ p) |\ 1 \leq i \leq n\}$ has a solution, say $x_j = r_j$ for some $r_j \in R, j \in J_k$. Thus we have

$$\sum_{j\in J_k} b_{ij}r_j \equiv b_{ij_k}\ (mod\ p)\ \forall i,\ 1 \leq i \leq n. \tag{1}$$

Let $B_0$ be the $n\times(n-\alpha)$ submatrix obtained by deleting columns $j_1,\dots,j_\alpha$ from $B$. Let $l$ be the smallest integer such that $p$ divides the determinants of all $l\times l$ submatrices of $B_l$ where $B_l \in M_{n\times l}(R)$ consists of the first $l$ columns of $B_0$. Assume that $j_0$ is the integer such that column $l$ of $B_0$ is column $j_0$ of $B$. Clearly $j_0 \notin J_A$. Let $J_0 = \{0,\dots,j_0-1\} - J_A$. By Lemma 2.2, It follows that the system of equations $\{\sum_{j\in J_0} b_{ij}x_j \equiv b_{ij_0}\ (mod\ p) |\ 1 \leq i \leq n\}$ has a solution, say $x_j = s_j$ for some $s_j \in R, j \in J_0$. Therefore we have

$$\sum_{j\in J_0} b_{ij}s_j \equiv b_{ij_0}\ (mod\ p)\ \forall i,\ 1 \leq i \leq n. \tag{2}$$

Put $J' = \{j_1,\dots,j_\alpha,j_0\}$ and let $J'_k = \{0,1,\dots,j_k\} - J'$. If $j_k > j_0$, then combining (1) and (2) yields $b_{ij_k} \equiv \sum_{j\in J'_k} b_{ij}r_j + (\sum_{j\in J_0} b_{ij}s_j)r_{j_0}\ (mod\ p)$ for every $i, 1 \leq i \leq n$. Hence the system of equations $\{\sum_{j\in J'_k} b_{ij}x_j \equiv b_{ij_k}\ (mod\ p) |\ 1 \leq i \leq n\}$ has a solution. On the other hand, if $j_k \leq j_0$, then obviously the above system has a solution by (1). Since $k$ is arbitrary, hence by Lemma 2.1, there exists a prime matrix $A_0$ with $\det(A_0) = p^{\alpha+1}$ such that $< B >\subseteq< A_0 >$ and $J_{A_0} = J'$. Thus the assertion is true for $\alpha+1$ and hence by induction for every $\alpha$, $1 \leq \alpha \leq n$. $\square$

**Proposition 2.4.** *Let $n$ be a positive integer and let $B \in M_n(R)$. Let $p \in R$ be a prime element and let $\alpha$ , $1 \leq \alpha \leq n$ , be the greatest integer such that $p^{\alpha} \mid det(B)$ and $p^{\alpha-1}$ divides all entries of $B'$. Then $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B$.*

Proof. By Theorem 3.2 in [1], there exist a diagonal matrix $C=(c_{ij})$ and invertible matrices $P,Q\in M_n(R)$ such that $BQ=PC$, so that $Q'B'=C'P'$. By hypothesis, $p^{\alpha-1}$ divides all entries of $B'$ and hence those of $C'P'$. Let $C'=(c'_{ij})$. If $p^2\mid c_{jj}$ for some $j,\ 1\le j\le n$, then $p^{\alpha-1}\nmid c'_{jj}$. Hence $p$ divides all entries of row $j$ of $P'$. Thus $p\mid \det(P')$ which contradicts the fact that $P$ is invertible. Since $p^\alpha\mid\det(C)$, hence $p$ divides at least $\alpha$ entries of the diagonal of $C$. Therefore we conclude that $p$ divides entries of at least one column of every $(n-\alpha+1)\times(n-\alpha+1)$ submatrix of $PC$. Thus $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $PC$ and by the Binet-Cauchy formula it is easy to see that $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B=(PC)Q^{-1}$. □

The next theorem is the main result of this section.

**Theorem 2.5.** *Every full rank prime submodule of $R^{(n)}$ is the row space of a prime matrix and vice versa.*

Proof. Let $N$ be a prime submodule of $R^{(n)}$ with rank $N=n$. Then $N$ is free and so there exists $B\in M_n(R)$ such that $N=<B>$. By Theorem 1.1, $\det(B)=up^\alpha$ for some prime $p\in R$, unit $u\in R$ and integer $\alpha,\ 1\le\alpha\le n$; also a $GCD$ of entries of $B'$ is $p^{\alpha-1}$. Hence by Proposition 2.4, $p$ divides the determinants of all $(n-\alpha+1)\times(n-\alpha+1)$ submatrices of $B$ and hence by Theorem 2.3, $N\subseteq<A>$ for some prime matrix $A$ with $\det(A)=p^\alpha$. Thus $B=CA$ for some $C\in M_n(R)$ and therefore $up^\alpha=\det(B)=\det(C)\det(A)=\det(C)p^\alpha$. Thus $\det(C)=u$ and so $C$ is invertible. Hence $C^{-1}B=A$. It follows that $<A>\subseteq<B>=N$. Therefore $N=<A>$. That the row space of every prime matrix is a prime submodule, is clear by Theorem 1.1. □

For example, for every prime element $p\in\mathbb{Z}$, the prime submodules $N$ of $\mathbb{Z}^{(3)}=\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}$ such that $(N:\mathbb{Z}^{(3)})=p\mathbb{Z}$ are as follows:

$$<\begin{pmatrix} p&0&0\\0&1&0\\0&0&1\end{pmatrix}>,<\begin{pmatrix} 1&a_{12}&0\\0&p&0\\0&0&1\end{pmatrix}>,<\begin{pmatrix} 1&0&a_{13}\\0&1&a_{23}\\0&0&p\end{pmatrix}>,<\begin{pmatrix} p&0&0\\0&p&0\\0&0&1\end{pmatrix}>,$$

$$<\begin{pmatrix} p&0&0\\0&1&a_{23}\\0&0&p\end{pmatrix}>,<\begin{pmatrix} 1&a_{12}&a_{13}\\0&p&0\\0&0&p\end{pmatrix}>,<\begin{pmatrix} p&0&0\\0&p&0\\0&0&p\end{pmatrix}>,$$

where $0\le a_{ij}\le p-1,\ 1\le i<j\le 3$. Thus it is easily seen that for every prime integer $p$, there exist exactly $2p^2+2p+3$ prime submodules $N$ of $\mathbb{Z}^{(3)}$ such that $(N:\mathbb{Z}^{(3)})=p\mathbb{Z}$.

## 3. Radicals of Submodules

In this section we shall try to identify the radical of submodules of $R^{(n)}$ as far as possible. We first state some useful results about prime matrices.

**Proposition 3.1.** *Let $n$ be a positive integer and let $p \in R$ be a prime element. Let $A, B \in M_n(R)$ be $p$-prime matrices such that $< A > \subseteq < B >$. Then $J_B \subseteq J_A$.*

Proof. Let $\det(B) = p^\alpha$ for some positive integer $\alpha$, $1 \leq \alpha \leq n$. Suppose that there exists some $j_0 \in J_B - J_A$. By hypothesis row $j_0$ of $A$ belongs to $< B >$. Hence by Lemma 1.2, $p^\alpha$ divides the product (row $j_0$ of $A$)(column $j_0$ of $B'$)$= p^{\alpha-1}$, a contradiction. Therefore $J_B \subseteq J_A$. □

**Proposition 3.2.** *Let $n$ be a positive integer and let $p \in R$ be a prime element. Let $A, B \in M_n(R)$ be $p$-prime matrices. Then $< A > = < B >$ if and only if $J_A = J_B$ and the corresponding entries of $A$ and $B$ are equivalent modulo $p$.*

Proof. Let $A = (a_{ij})$ and $B = (b_{ij})$. Suppose that $J_A = J_B$. Let $\det(A) = p^\alpha = \det(B)$. Note that by Lemma 1.2, $< A > \subseteq < B >$ if and only if for all $i \notin J_A$ and $j \in J_A$, $1 \leq i < j \leq n$, $p^\alpha \mid \sum_{k=1}^{n} a_{ik} b'_{kj} = a_{ii} b'_{ij} + a_{ij} b'_{jj} = -p^{\alpha-1} b_{ij} + a_{ij} p^{\alpha-1}$; if and only if $a_{ij} \equiv b_{ij} \ (mod\ p)$ . By symmetry, this is equivalent to $< B > \subseteq < A >$. Now the result follows from Proposition 3.1. □

**Proposition 3.3.** *Let $m \leq n$ be positive integers and let $B \in M_{m \times n}(R)$. Let $p \in R$ be a prime element and let $\alpha$ be the greatest integer such that $p$ divides the determinants of all $(n - \alpha + 1) \times (n - \alpha + 1)$ submatrices of $B$. Then there exists a $p-$prime matrix $A \in M_n(R)$ with $det(A) = p^\alpha$ such that $< A >$ is minimum among all prime submodules $N$ of $R^{(n)}$ containing $< B >$ such that $p \in (N : R^{(n)})$.*

Proof. By Theorem 2.3, there exists a prime matrix $A \in M_n(R)$ with $\det(A) = p^\alpha$ such that $< B > \subseteq < A >$. Let $N$ be any prime submodule of $R^{(n)}$ such that $< B > \subseteq N$ and $p \in (N : R^{(n)})$. Thus $pR^{(n)} \subseteq N$, so that rank $N = n$. By Theorem 2.5, there exists a prime matrix $C \in M_n(R)$ such that $N = < C >$. Since $pR^{(n)} \subseteq N$, hence $C$ is $p-$prime. It is easy to see that $< A > \cap < C >$ is a prime submodule of $R^{(n)}$ and so again by Theorem 2.5, there exists a prime matrix $D \in M_n(R)$ such that $< A > \cap < C > = < D >$. By Proposition 3.1, since $< D > \subseteq < A >$, hence $J_A \subseteq J_D$. By hypothesis and Theorem 2.3, $J_D$ may have at most $\alpha$ element(s). Thus $J_D = J_A$. By the proof of Proposition 3.2, since $< D > \subseteq < A >$, hence $< A > = < D > = < A > \cap < C >$. Therefore $< A > \subseteq < C >$ . □

Let $m \leq n$ be positive integers and let $B \in M_{m\times n}(R)$. By Theorem 3.2 in [1], $B$ is equivalent to a diagonal matrix $C$; i.e. there exist invertible matrices $P \in M_m(R)$ and $Q \in M_n(R)$ such that $B = PCQ$. If $C_0 \in M_m(R)$ is the submatrix consisting of the first $m$ columns of $C$, then $C = C_0 I$ where $I \in M_{m\times n}(R)$ consists of the first $m$ rows of $I_n$. Put $D = PC_0$ and $B_0 = IQ$. Hence $B = DB_0$ and it is easily seen that $\det(D)$ is a $GCD$ of the determinants of all $m \times m$ submatrices of $B$ and a $GCD$ of the determinants of all $m \times m$ submatrices of $B_0$ is 1. If $\det(D)$ is a unit, then $D$ is invertible so that $< B >=< B_0 >$. Thus for $m < n$ by Theorem 1.1, $< B >$ is a prime submodule of $F = R^{(n)}$ and hence $\mathrm{rad}_F(< B >) =< B >$. The following theorem characterizes the radical of submodules of $R^{(n)}$. A characterization has been carried out in [6] in the general case; however, when $R$ is a PID, the characterization given below seems to be more practical.

**Theorem 3.4.** *Let $m \leq n$ be positive integers and let $F = R^{(n)}$. Suppose that $B \in M_{m\times n}(R)$ and $D$ and $B_0$ are as above. Let $d = det(D) = up_1^{\beta_1} \dots p_t^{\beta_t}$ be a prime decomposition. If $A_k = (a_{kij}),\ 1 \leq k \leq t$, is the $p_k-$prime matrix as in Proposition 3.3, then $rad_F(< B >) =< C > \cap < B_0 >$ where $C = (c_{ij}) \in M_n(R)$ is an upper triangular matrix such that for all $i, k,\ 1 \leq i \leq n, 1 \leq k \leq t$,*

*i) $c_{ii} = p_1^{\delta_1} \dots p_t^{\delta_t}$ where $\delta_k = 1$ if $i \in J_{A_k}$ and $\delta_k = 0$ if $i \notin J_{A_k}$.*

*ii) $c_{ij} \equiv \displaystyle\sum_{l=0,\ l\notin J_{A_k}}^{j-1} c_{il} a_{klj}\ (mod\ p_k)\ \forall j \in J_{A_k}$.*

Proof. That there exists such a matrix $C$ satisfying (i) and (ii) is guaranteed by the Chinese remainder theorem. Now assume that $N$ is a prime submodule of $F$ containing $< B >$. Hence the rows of $D'B = D'DB_0 = \det(D)I_m B_0 = dB_0$ belong to $N$. Thus $d < B_0 >\subseteq N$. If $N$ does not contain $< B_0 >$, then $d \in (N : F)$. Note that $(N : F)$ is a prime ideal of $R$. Therefore $p_k \in (N : F)$ for some $k,\ 1 \leq k \leq t$. Note that by Theorem 1.1, if $m < n$ then $< B_0 >$ is a prime submodule of $F$. Thus by Proposition 3.3, it is easy to see that $\mathrm{rad}_F(< B >)$ $= \displaystyle\bigcap_{k=1}^{t} < A_k > \cap < B_0 >$. Now it remains to show that $\displaystyle\bigcap_{k=1}^{t} < A_k >=< C >$. By the proof of Lemma 2.1, condition (ii) is equivalent to $< C >\subseteq< A_k >$ for every $k,\ 1 \leq k \leq t$, so that $< C >\subseteq \displaystyle\bigcap_{k=1}^{t} < A_k >$. Conversely, suppose that

$(r_1,\ldots,r_n)\in\bigcap_{k=1}^{t}<A_k>$. Therefore for every $k,\ 1\le k\le t$, we have

$$\sum_{i=0,\,i\notin J_{A_k}}^{j-1} r_i a_{kij}\equiv r_j\ (mod\ p_k)\quad \forall j\in J_{A_k}. \tag{3}$$

Let $C'=(c'_{ij})$. Note that $C'$ is an upper triangular matrix. By Lemma 1.2, to prove that $(r_1,\ldots,r_n)\in<C>$, we have to show that $\det(C)\mid\sum_{i=1}^{n} r_i c'_{ij}=\sum_{i=1}^{j} r_i c'_{ij}$ for every $j,\ 1\le j\le n$. Let $\det(A_k)=p_k^{\alpha_k},\ 1\le k\le t$. By (i), it follows that $\det(C)=p_1^{\alpha_1}\ldots p_t^{\alpha_t}$. Let $k,\ 1\le k\le t$, be fixed and arbitrary. Hence it is enough to show that $p_k^{\alpha_k}\mid\sum_{i=1}^{j} r_i c'_{ij}$ for every $j,\ 1\le j\le n$. We use induction on $j$. For $j=1$, if $1\notin J_{A_k}$, then $p_k\not| c_{11}$. Since $p_k^{\alpha_k}\mid\det(C)$, hence $p_k^{\alpha_k}\mid r_1c_{11}c'_{11}$ and so $p_k^{\alpha_k}\mid r_1c'_{11}$. If $1\in J_{A_k}$, then by (3), $r_1\equiv 0\ (mod\ p_k)$, so $p_k\mid r_1$. Since $p_k^{\alpha_k-1}\mid\dfrac{\det(C)}{c_{11}}=c'_{11}$, hence $p_k^{\alpha_k}\mid r_1c'_{11}$. Thus the assertion is true for $j=1$. Assume inductively that $p_k^{\alpha_k}\mid\sum_{i=1}^{j} r_i c'_{ij}$ for every $j,\ 1\le j\le j_0-1$. We have to show that $p_k^{\alpha_k}\mid\sum_{i=1}^{j_0} r_i c'_{ij_0}$. We have $\sum_{j=1}^{j_0} c_{jj_0}(\sum_{i=1}^{j} r_i c'_{ij})=\sum_{j=1}^{j_0}\sum_{i=1}^{j_0} r_i c'_{ij}c_{jj_0}=\sum_{i=1}^{j_0} r_i(\sum_{j=1}^{j_0} c'_{ij}c_{jj_0})=r_{j_0}\det(C)$. Therefore

$$c_{j_0j_0}\sum_{i=1}^{j_0} r_i c'_{ij_0}=r_{j_0}\det(C)-\sum_{j=1}^{j_0-1} c_{jj_0}(\sum_{i=1}^{j} r_i c'_{ij}) \tag{4}$$

Now two cases may occur: **Case 1.** $j_0\notin J_{A_k}$. Thus $p_k\not| c_{j_0j_0}$. Hence (4) and the induction hypothesis imply that $p_k^{\alpha_k}\mid c_{j_0j_0}\sum_{i=1}^{j_0} r_i c'_{ij_0}$. Since $p_k\not| c_{j_0j_0}$, hence $p_k^{\alpha_k}\mid\sum_{i=1}^{j_0} r_i c'_{ij_0}$. **Case 2.** $j_0\in J_{A_k}$. Let $J_0=\{0,1,\ldots,j_0\}-J_{A_k}$. By (ii),

$p_k \mid \sum_{l\in J_0} c_{jl}a_{klj_0} - c_{jj_0}$, so that by induction hypothesis,

$p_k^{\alpha_k+1} \mid (\sum_{i=1}^{j} r_i c'_{ij})(\sum_{l\in J_0} c_{jl}a_{klj_0} - c_{jj_0})$ for every $j, 1 \le j \le j_0 - 1$. Thus

$$
\begin{aligned}
&p_k^{\alpha_k+1} \mid \sum_{j=1}^{j_0-1}[(\sum_{i=1}^{j} r_i c'_{ij})(\sum_{l\in J_0} c_{jl}a_{klj_0} - c_{jj_0})] \\
&\Rightarrow p_k^{\alpha_k+1} \mid \sum_{j=1}^{j_0-1}[\sum_{i=1}^{j_0-1}\sum_{l\in J_0} r_i c'_{ij}c_{jl}a_{klj_0} - c_{jj_0}\sum_{i=1}^{j} r_i c'_{ij}] \\
&\Rightarrow p_k^{\alpha_k+1} \mid \sum_{j=1}^{j_0-1}\sum_{i=1}^{j_0-1}\sum_{l\in J_0} r_i c'_{ij}c_{jl}a_{klj_0} - \sum_{j=1}^{j_0-1} c_{jj_0}(\sum_{i=1}^{j} r_i c'_{ij}) \\
&\Rightarrow p_k^{\alpha_k+1} \mid \sum_{j=1}^{j_0-1}\sum_{i=1}^{j_0-1} r_i(\sum_{l\in J_0} c'_{ij}c_{jl})a_{klj_0} - \sum_{j=1}^{j_0-1} c_{jj_0}(\sum_{i=1}^{j} r_i c'_{ij}) \\
&\Rightarrow p_k^{\alpha_k+1} \mid \sum_{l\in J_0} r_l(\det(C))a_{klj_0} - r_{j_0}\det(C) + r_{j_0}\det(C) - \sum_{j=1}^{j_0-1} c_{jj_0}(\sum_{i=1}^{j} r_i c'_{ij}) \\
&\Rightarrow p_k^{\alpha_k+1} \mid (\det(C))(\sum_{l\in J_0} r_l a_{klj_0} - r_{j_0}) + c_{j_0j_0}\sum_{i=1}^{j_0} r_i c'_{ij_0}.
\end{aligned}
$$

By (3), $p_k \mid \sum_{l\in J_0} r_l a_{klj_0} - r_{j_0}$. Thus $p_k^{\alpha_k+1} \mid (\det(C))(\sum_{l\in J_0} r_l a_{klj_0} - r_{j_0})$. Hence by above
$p_k^{\alpha_k+1} \mid c_{j_0j_0}\sum_{i=1}^{j_0} r_i c'_{ij_0}$. Therefore $p_k^{\alpha_k} \mid \sum_{i=1}^{j_0} r_i c'_{ij_0}$ and so by induction $p_k^{\alpha_k} \mid \sum_{i=1}^{j} r_i c'_{ij}$ for all $j,\ 1 \le j \le n$. □

In the previous theorem, if $m = n$, we can simply choose $D = B$ and $B_0 = I_n$ and therefore we have $\mathrm{rad}_F(< B >) =< C >$. Some results concerning radical submodules may be found in [4]. Now let $r \in R$ and $B \in M_{m\times n}(R)$. By the notation $r \mid B$, we mean $r$ divides all entries of $B$. The following notation defined in [3], is used in the next result. Let $1 \le i_1 < \cdots < i_t \le m$ and $1 \le j_1 < \cdots < j_t \le n$ be some integers and $1 \le t \le min(m, n)$. Then $B\begin{bmatrix} i_1 & \ldots & i_t \\ j_1 & \ldots & j_t \end{bmatrix}$ denotes the determinant of the $t \times t$ submatrix of $B$ consisting of rows $i_1, \ldots, i_t$ and columns $j_1, \ldots, j_t$.

**Theorem 3.5.** *Let $m \leq n$ be positive integers and let $F = R^{(n)}$. Suppose that $B \in M_{m\times n}(R)$ and that $d$ is a $GCD$ of the determinants of all $m \times m$ submatrices of $B$. Then $< B >$ is a radical submodule of $F$ if and only if for every prime element $p \in R$ and positive integer $\beta$, $p^\beta \mid d$ implies that $p$ divides the determinants of all $(m-\beta+1) \times (m-\beta+1)$ submatrices of $B$.*

Proof. Suppose that $d = up_1^{\beta_1} \dots p_t^{\beta_t}$ is a prime decomposition. By Theorem 3.4, there exist $D \in M_m(R), B_0 \in M_{m\times n}(R)$ and $A_k \in M_n(R)$, $1 \leq k \leq t$, such that $B = DB_0$, $\det(D) = d$ and $\mathrm{rad}_F(< B >) =< B_0 > \cap \bigcap_{k=1}^{t} < A_k >$. Assume that $\mathrm{rad}_F(< B >) =< B >$. If $q = p_1 \dots p_t$, then by Lemma 1.2, $(0, \dots, 0, q, 0, \dots, 0)B_0 \in< B_0 > \cap \bigcap_{k=1}^{t} < A_k >$ with the $q$ as the $i$th component $(1 \leq i \leq m)$. Thus $(0, \dots, 0, q, 0, \dots, 0)B_0 \in \mathrm{rad}_F(< B >) =< B >$. Therefore there exist $s_i \in R$, $1 \leq i \leq m$, such that $(0, \dots, 0, q, 0, \dots, 0)B_0 = (s_1, \dots, s_m)B = (s_1, \dots, s_m)DB_0$, whence $(0, \dots, 0, q, 0, \dots, 0) = (s_1, \dots, s_m)D$. It follows that $(0, \dots, 0, q, 0, \dots, 0)D' = (s_1, \dots, s_m)\det(D)I_m = (s_1, \dots, s_m)d$. Hence $d \mid (0, \dots, 0, q, 0, \dots, 0)D'$ with the $q$ as the $i$th component $(1 \leq i \leq m)$. Let $k, 1 \leq k \leq t$, be arbitrary. Then $p_k^{\beta_k-1} \mid D'$. Thus $p_k^{(\beta_k-1)m} \mid \det(D') = d^{m-1}$ and hence $(\beta_k - 1)m \leq \beta_k(m-1)$ whence $\beta_k \leq m$. Also by Proposition 2.4, since $p_k^{\beta_k-1}$ divides all entries of $D'$, hence $p_k$ divides the determinants of all $(m-\beta_k+1) \times (m-\beta_k+1)$ submatrices of $D$. Since $B = DB_0$, we conclude by the Binet-Cauchy formula that $p_k$ divides the determinants of all $(m-\beta_k+1) \times (m-\beta_k+1)$ submatrices of $B$ .
Conversely, assume that for every $k$, $1 \leq k \leq t$, $\beta_k \leq m$ and $p_k$ divides the determinants of all $(m-\beta_k+1) \times (m-\beta_k+1)$ submatrices of $B$. Fix $k$ for the moment. Since $m - \beta_k + 1 = n - (n - m + \beta_k) + 1$, hence by Theorem 2.3, $< B >\subseteq< A >$ for some prime matrix $A$ with $\det(A) = p_k^{n-m+\beta_k}$. Let $\alpha = n - m + \beta_k$ and $C = \frac{1}{p_k^\alpha}BA'$. Since $< B >\subseteq< A >$, by Lemma 1.2, $C \in M_{m\times n}(R)$. Let $(x_1 \dots x_n) \in \mathrm{rad}_F(< B >)$ be arbitrary. Since $\mathrm{rad}_F(< B >) \subseteq< B_0 >$, hence $(x_1 \dots x_n) = (r_1 \dots r_m)B_0$ for some $r_i \in R$, $1 \leq i \leq m$. Also since $\mathrm{rad}_F(< B >) \subseteq< A >$, hence $(x_1 \dots x_n) = (r_1 \dots r_m)B_0 \in< A >$. Again by Lemma 1.2, $p_k^\alpha \mid (r_1 \dots r_m)B_0A'$, so that $p_k^\alpha d \mid (r_1 \dots r_m)D'(BA')$. Therefore $d$ and so $p_k^{\beta_k}$ divides all components of $(r_1 \dots r_m)D'C$. If we show that there exists an $m \times m$ submatrix $C_0$ of $C$ such that $p_k \nmid \det(C_0)$, then we may conclude that $p_k^{\beta_k} \mid (r_1 \dots r_m)D'C_0$ and hence $p_k^{\beta_k} \mid (r_1 \dots r_m)D'C_0C_0' =$

$(r_1 \dots r_m)D'\det(C_0)I_m$. It will follow that $p_k^{\beta_k} \mid (r_1 \dots r_m)D'$. Since $k$ is arbitrary, hence $d \mid (r_1 \dots r_m)D'$. Thus there exist $s_i \in R$, $1 \leq i \leq m$, such that $d(s_1, \dots, s_m) = (r_1, \dots, r_m)D'$. Hence $d(s_1, \dots, s_m)B = (r_1, \dots, r_m)D'B = (r_1, \dots, r_m)dB_0$, so that $(x_1 \dots x_n) = (r_1 \dots r_m)B_0 = (s_1, \dots, s_m)B \in <B>$. Therefore $\mathrm{rad}_F(<B>) = <B>$. Now suppose on the contrary that $p_k$ divides the determinants of all $m \times m$ submatrices of $C$. We shall show that $p_k^{\beta_k+1}$ divides the determinants of all $m \times m$ submatrices of $B$. Let $j_1 < \cdots < j_m$ be some arbitrary integers between 1 and $n$. Since $C = (\frac{1}{p_k}B)(\frac{1}{p_k^{\alpha-1}}A')$, hence by the Binet-Cauchy formula, we have

(5)

$$C\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix} = \frac{1}{p_k^m}\sum_{i_1<\cdots<i_m} B\begin{bmatrix} 1 & \dots & m \\ i_1 & \dots & i_m \end{bmatrix}(\frac{1}{p_k^{\alpha-1}}A')\begin{bmatrix} i_1 & \dots & i_m \\ j_1 & \dots & j_m \end{bmatrix}$$

Note that $\dfrac{1}{p_k^{\alpha-1}}A' = -A + (1+p_k)I_n$. By the definition of prime matrices, it follows that $(\dfrac{1}{p_k^{\alpha-1}}A')\begin{bmatrix} i_1 & \dots & i_m \\ j_1 & \dots & j_m \end{bmatrix} = 0$ except possibly when the following two conditions are satisfied:

(i) $\{i_1, \dots, i_m\} \cap J_A \subseteq \{j_1, \dots, j_m\}$ and (ii) $\{j_1, \dots, j_m\} - J_A \subseteq \{i_1, \dots, i_m\}$.

Let $J = \{j_1, \dots, j_m\} \cup J_A$ have $(n-l+1)$ element(s). We use induction on $l$. For $l = 1$, we have $J = \{1, \dots, n\}$. For every $i \in \{i_1, \dots, i_m\}$, if $i \notin J_A$ then $i \in J - J_A \subseteq \{j_1, \dots, j_m\}$ and if $i \in J_A$ then by (i), again $i \in \{j_1, \dots, j_m\}$. Thus $\{i_1, \dots, i_m\} = \{j_1, \dots, j_m\}$. Hence by (5), we have

$$C\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix} = \frac{1}{p_k^m}B\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix}(\frac{1}{p_k^{\alpha-1}}A')\begin{bmatrix} j_1 & \dots & j_m \\ j_1 & \dots & j_m \end{bmatrix}$$

$$= \frac{1}{p_k^m}B\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix}p_k^{m-\beta_k} = \frac{1}{p_k^{\beta_k}}B\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix}.$$

Since $p_k \mid C\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix}$, hence $p_k^{\beta_k+1} \mid B\begin{bmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{bmatrix}$. Thus the assertion is true for $l = 1$. Assume inductively that $p_k^{\beta_k+1} \mid B\begin{bmatrix} 1 & \dots & m \\ i_1 & \dots & i_m \end{bmatrix}$ whenever $\{i_1, \dots, i_m\} \cup J_A$ has at least $(n-l+1)$ elements. Suppose that $J = \{j_1, \dots, j_m\} \cup J_A$ has $(n-l)$ element(s). If $\{i_1, \dots, i_m\} \subseteq J$ then $\{i_1, \dots, i_m\} - J_A \subseteq J - J_A \subseteq \{j_1, \dots, j_m\}$ whence by (i), $\{i_1, \dots, i_m\} = \{j_1, \dots, j_m\}$. If $\{i_1, \dots, i_m\} \nsubseteq J$ then by (ii), we have $J = (\{j_1, \dots, j_m\} - J_A) \cup J_A \subset \{i_1, \dots, i_m\} \cup J_A$, so that

$\{i_1, \ldots, i_m\} \cup J_A$ has at least $(n-l+1)$ elements. Hence by the induction hypothesis $p_k^{\beta_k+1} \mid B\begin{bmatrix} 1 & \ldots & m \\ i_1 & \ldots & i_m \end{bmatrix}$ whenever $\{i_1, \ldots, i_m\} \not\subseteq J$. Thus by (5), we conclude that $C\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix} = \frac{1}{p_k^m} \sum B\begin{bmatrix} 1 & \ldots & m \\ i_1 & \ldots & i_m \end{bmatrix} (\frac{1}{p_k^{\alpha-1}} A')\begin{bmatrix} i_1 & \ldots & i_m \\ j_1 & \ldots & j_m \end{bmatrix}$ $+ \frac{1}{p_k^m} B\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix} (\frac{1}{p_k^{\alpha-1}} A')\begin{bmatrix} j_1 & \ldots & j_m \\ j_1 & \ldots & j_m \end{bmatrix}$ where the summation is over all $i_1 < \cdots < i_m$ such that $\{i_1, \ldots, i_m\} \not\subseteq J$. Thus since $p_k \mid C\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix}$, hence

$p_k^{m+1} \mid \sum B\begin{bmatrix} 1 & \ldots & m \\ i_1 & \ldots & i_m \end{bmatrix} (\frac{1}{p_k^{\alpha-1}} A')\begin{bmatrix} i_1 & \ldots & i_m \\ j_1 & \ldots & j_m \end{bmatrix}$

$+ B\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix} p_k^{m-\beta_k-l}$. By (ii), we have $p_k^{m-\beta_k-l} \mid (\frac{1}{p_k^{\alpha-1}} A')\begin{bmatrix} i_1 & \ldots & i_m \\ j_1 & \ldots & j_m \end{bmatrix}$. It follows that $p_k^{m-l+1} \mid \sum B\begin{bmatrix} 1 & \ldots & m \\ i_1 & \ldots & i_m \end{bmatrix} (\frac{1}{p_k^{\alpha-1}} A')\begin{bmatrix} i_1 & \ldots & i_m \\ j_1 & \ldots & j_m \end{bmatrix}$ and so $p_k^{m-l+1} \mid B\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix} p_k^{m-\beta_k-l}$ whence $p_k^{\beta_k+1} \mid B\begin{bmatrix} 1 & \ldots & m \\ j_1 & \ldots & j_m \end{bmatrix}$. Hence by induction, $p_k^{\beta_k+1}$ divides the determinants of all $(m \times m)$ submatrices of $B$ and so $p_k^{\beta_k+1} \mid d$, a contradiction. □

**Acknowledgement.** The authors would like to thank the referee for his/her useful suggestions that improved the presentation of this paper.

## References

[1] P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, Basic Abstract Algebra, Cambridge University Press, New York, 1986.

[2] S. Hedayat and R. Nekooei, Characterization of prime submodules of a finitely generated free module over a PID, Houston Journal of Mathematics, 31(1), 2005, 75-85.

[3] P. Lancaster and M. Tismenetsky, The Theory of Matrices second edition with applications, Academic Press, San Diego, New York, 1985.

[4] M.E. Moore and S.J. Smith, Prime and radical submodules of modules over commutative rings, Comm. Algebra, 30 (10), (2002), 5037-5064.

[5] Y. Tiras, A. Harmanci and P.F. Smith, A characterization of prime submodules, Journal of Algebra 212, (1999), 743-752.

[6] D.P. Yilmaz and P.F. Smith, Radicals of submodules of free modules, Comm. Algebra, 27 (5), (1999), 2253-2266.

Received March 26, 2004

Revised version received September 19, 2004

Department of Mathematics, Shahid Bahonar University of Kerman, Kerman, Iran.

*E-mail address*: rnekooei@mail.uk.ac.ir