Czechoslovak Mathematical Journal

A. Amini; B. Amini; Habib Sharif

Prime and primary submodules of certain modules

Czechoslovak Mathematical Journal, Vol. 56 (2006), No. 2, 641–648

Persistent URL: `http://dml.cz/dmlcz/128093`

Czechoslovak Mathematical Journal, 56 (131) (2006), 641–648

PRIME AND PRIMARY SUBMODULES OF CERTAIN MODULES

A. Amini, B. Amini and H. Sharif, Shiraz

(Received November 25, 2003)

Abstract. In this paper we characterize all prime and primary submodules of the free R-module R^n for a principal ideal domain R and find the minimal primary decomposition of any submodule of R^n. In the case $n = 2$, we also determine the height of prime submodules.

Keywords: prime submodules, primary submodules, primary decomposition

MSC 2000: 13C13, 13C99

1. Introduction

Throughout this note all rings are commutative with identity and all modules are unitary.

Let S be a ring and M an S-module. A proper submodule N of M is called a prime submodule if $sm \in N$ for $s \in S$ and $m \in M$ implies that $m \in N$ or $s \in (N\colon M)$, where

$$(N\colon M) = \{t \in S\colon tM \subseteq N\}.$$

The following lemma is well-known (see for example [2]).

1.1 Lemma. *Let N be a submodule of an S-module M. Then*

i) *N is a prime submodule of M if and only if $P = (N\colon M)$ is a prime ideal of S and the S/P-module M/N is torsion-free.*

ii) *If $(N\colon M)$ is a maximal ideal of S, then N is a prime submodule of M.*

iii) *If N is a maximal submodule of M, then N is a prime submodule of M.*

Let K be a prime submodule of an S-module M. It is said that K has height n for some non-negative integer n, if there exists a chain

$$K_n \subset K_{n-1} \subset \ldots \subset K_1 \subset K_0 = K$$

of prime submodules K_i $(0 \leqslant i \leqslant n)$ of M, but no longer such chain.

Let M be a module over a ring S. Recall that a proper submodule Q of M is a primary submodule provided that for any $s \in S$ and $m \in M$, $sm \in Q$ implies that $m \in Q$ or $s^n \in (Q\colon M)$ for some positive integer n.

Let Q be a primary submodule of M, then the radical of the ideal $(Q\colon M)$ is a prime ideal of S, [4]. If $P = \sqrt{(Q\colon M)}$, then Q is called a P-primary submodule of M.

A submodule N of M has a primary decomposition if $N = Q_1 \cap \ldots \cap Q_t$ with each Q_i a P_i-primary submodule of M for some prime ideal P_i. If no Q_i contains $Q_1 \cap \ldots \cap Q_{i-1} \cap Q_{i+1} \cap \ldots \cap Q_t$ and if the ideals $P_1, \ldots, P_t$ are all distinct, then the primary decomposition is said to be minimal.

It is known that every prime ideal of the ring $S_1 \times S_2 \times \ldots \times S_n$, where S_i is a ring $(1 \leqslant i \leqslant n)$, is of the form $S_1 \times \ldots \times S_{i-1} \times P_i \times S_{i+1} \times \ldots \times S_n$ for some prime ideal P_i of S_i, [3]. Now it is natural to ask about the prime submodules of the S-module S^n for an arbitrary ring S.

Tiras and Harmanci in [5] studied prime submodules of the R-module $R \times R$ for a principal ideal domain (PID) R and investigated the primary decomposition of any submodule of $R \times R$. In Section 2 we will characterize all prime submodules of R^n where R is a PID and $n \geqslant 2$ is a positive integer. In Section 3 we find the height of prime submodules of $R \times R$ for a PID R. Finally, the primary decomposition of any submodule of R^n is discussed in Section 4.

2. Prime submodules of R^n

In this section R denotes a principal ideal domain and M the free R-module R^n for some positive integer $n \geqslant 2$.

Let N be a non-zero submodule of M. There exist a basis $\{x_1, \ldots, x_n\}$ of M and non-zero elements $d_1, \ldots, d_r$ $(r \leqslant n)$ of R such that $N = Rd_1x_1 + \ldots + Rd_rx_r$, [4]. Therefore any submodule of M can be generated by n elements.

Let $N = Ra_1 + \ldots + Ra_n$ be a submodule of M. Suppose that $a_i = (a_{i1}, \ldots, a_{in})$ $(1 \leqslant i \leqslant n)$. Put $A = (a_{ij}) \in M_{n\times n}(R)$ and $\Delta = \det A$. Let $A' = (a'_{ij})$ be the adjoint matrix of A. Then $AA' = A'A = \Delta I_n$, where I_n is the identity of the ring $M_{n\times n}(R)$. By considering all possible choices of Δ, we will characterize prime submodules of M. First we show that Δ is unique up to multiplication by a unit.

2.1 Lemma. *Let N be a submodule of M. Suppose that $N = Ra_1 + \ldots + Ra_n$ and also $N = Rb_1 + \ldots + Rb_n$ for some $a_i, b_i \in M$ $(1 \leqslant i \leqslant n)$. Let $A = (a_{ij})$ and*

$B = (b_{ij})$ *be as above. Then*

$$\det A = u(\det B)$$

for some unit u *of* R.

Proof. For each $1 \leqslant i \leqslant n$, there are $c_{ij} \in R$ $(1 \leqslant j \leqslant n)$ such that $a_i = \sum_{j=1}^{n} c_{ij} b_j$. Let $C = (c_{ij}) \in M_{n\times n}(R)$. Then $A = CB$. Therefore

$$\det A = \det(CB) = (\det C)(\det B)$$

and hence $\det B$ divides $\det A$. By symmetry $\det A$ divides $\det B$. Thus $\det A = u(\det B)$ for some unit $u \in R$, as required. □

Now we consider the submodules of M with non-zero Δ. For our purpose we need the following result.

2.2 Proposition. *Let* $N = Ra_1 + \ldots + Ra_n$ *be a submodule of* M *and let* $A = (a_{ij})$ *be as above. If* $\Delta = \det A \neq 0$, *then*

$$N = \Big\{(x_1, \ldots, x_n) \in M \colon \ \Delta \text{ divides } \sum_{i=1}^{n} x_i a'_{ij} \ (1 \leqslant j \leqslant n)\Big\},$$

where $A' = (a'_{ij})$ *is the adjoint matrix of* A. *Moreover,* $\Delta M \subseteq N$.

Proof. Let

$$K = \Big\{(x_1, \ldots, x_n) \in M \colon \ \Delta \text{ divides } \sum_{i=1}^{n} x_i a'_{ij} \ (1 \leqslant j \leqslant n)\Big\}.$$

Then K is a submodule of M. Since $AA' = \Delta I_n$, we have $a_i \in K$ $(1 \leqslant i \leqslant n)$ and hence $N \subseteq K$. On the other hand, suppose that $(x_1, \ldots, x_n) \in K$. There is $(y_1, \ldots, y_n) \in M$ such that

$$(x_1, \ldots, x_n)(a'_{ij}) = \Delta(y_1, \ldots, y_n).$$

Therefore

$$\Delta(x_1, \ldots, x_n) = (x_1, \ldots, x_n)(a'_{ij})(a_{ij}) = \Delta(y_1, \ldots, y_n)(a_{ij}).$$

Since $\Delta \neq 0$, we have $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)(a_{ij})$. Thus $(x_1, \ldots, x_n) = y_1 a_1 + \ldots + y_n a_n \in N$. Consequently, $K = N$. Now the last assertion follows immediately from the equality. □

2.3 Corollary. *Let $N = Ra_1 + \ldots + Ra_n$ be a submodule of M and let $A = (a_{ij})$. Then $N = M$ if and only if $\Delta = \det A$ is a unit of R.*

Proof. If Δ is a unit of R, then by Proposition 2.2, $M = \Delta M \subseteq N$.

Conversely, suppose that $N = M$. Then

$$N = R(1, 0, \ldots, 0) + R(0, 1, 0, \ldots, 0) + \ldots + R(0, \ldots, 0, 1).$$

Now Lemma 2.1 implies that Δ is a unit of R. □

Let $C \in M_{n\times n}(R)$ and let C' be the adjoint matrix of C. If $d = \det C \neq 0$, then $CC' = dI_n$ implies that

$$d(\det C') = (\det C)(\det C') = \det(CC') = \det(dI_n) = d^n.$$

Therefore, $\det C' = d^{n-1} = (\det C)^{n-1}$.

Now we are ready to characterize prime submodules of M with non-zero Δ.

2.4 Theorem. *Let $N = Ra_1 + \ldots + Ra_n$ be a submodule of M and let $A = (a_{ij})$. If $\Delta = \det A \neq 0$, then N is a prime submodule if and only if $\Delta = up^r$ for some unit $u \in R$, a prime element $p \in R$, and a positive integer $r \leqslant n$ and moreover, p^{r-1} divides a'_{ij} $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)$ where $A' = (a'_{ij})$ is the adjoint matrix of A.*

Proof. First suppose that N is a prime submodule of M. Since $N \neq M$, by Corollary 2.3, Δ is not a unit of R. Assume that $\Delta = st$ for some relatively prime elements $s, t \in R$. Proposition 2.2 implies that $st \in (N\colon M)$, which is a prime ideal of R. Thus $s \in (N\colon M)$ or $t \in (N\colon M)$. Suppose that $s \in (N\colon M)$. Thus for any $1 \leqslant i \leqslant n$, $(0, \ldots, 0, s, 0, \ldots, 0) \in sM \subseteq N$ with s as the ith component. Therefore by Proposition 2.2, $st = \Delta$ divides sa'_{ij} $(1 \leqslant j \leqslant n)$ and so t divides a'_{ij} $(1 \leqslant j \leqslant n)$. Hence t^n divides $\det(a'_{ij}) = (\det A)^{n-1} = s^{n-1}t^{n-1}$. Thus t divides s^{n-1}. Since s and t are relatively prime, t divides 1, i.e., t is a unit. Consequently, $\Delta = up^r$ for some unit $u \in R$, a prime element $p \in R$ and a positive integer r. Since $\Delta \in (N\colon M)$ and $(N\colon M)$ is a prime ideal of R, $p \in (N\colon M)$. As in the above case, up^r divides pa'_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ and so p^{r-1} divides a'_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$. Hence $p^{n(r-1)}$ divides $\det(a'_{ij}) = (\det A)^{n-1} = u^{n-1}p^{r(n-1)}$. Therefore, $n(r-1) \leqslant r(n-1)$ and so $r \leqslant n$.

Conversely, since Δ is not a unit, N is a proper submodule of M. We shall show that $(N\colon M)$ is a maximal ideal of R and hence by Lemma 1.1, N is a prime submodule of M. Let $(x_1, \ldots, x_n) \in pM$. Since p^{r-1} divides a'_{ij} $(1 \leqslant i \leqslant n,$ $1 \leqslant j \leqslant n)$, $\Delta = up^r$ divides $\sum\limits_{i=1}^{n} x_i a'_{ij}$ $(1 \leqslant j \leqslant n)$. Thus $(x_1, \ldots, x_n) \in N$ and so $pM \subseteq N$. Therefore, $p \in (N\colon M)$ and hence $Rp \subseteq (N\colon M) \subset R$. Consequently, $(N\colon M) = Rp$ is a maximal ideal of R, as required. □

Remark. Note that in the above theorem, if $\Delta = up$ for some unit $u \in R$ and a prime element $p \in R$, then N is a prime submodule of M (because the second condition holds trivially).

Now we consider the submodules of M with zero Δ.

2.5 Theorem. *Let $N = Ra_1 + \ldots + Ra_n$ be a submodule of M and let $\Delta = \det(a_{ij}) = 0$. Then N is a prime submodule of M if and only if N is a direct summand of M.*

Proof. Suppose that $M = N \oplus K$ for some submodule K of M. Since $\Delta = 0$, we have $N \neq M$. Let $r \in R$ and $m \in M$ be such that $rm \in N$. There are $m_1 \in N$ and $m_2 \in K$ with $m = m_1 + m_2$. If $r \neq 0$, then $rm_2 = rm - rm_1 \in N \cap K = 0$. Hence $m_2 = 0$ and so $m = m_1 \in N$. It follows that N is a prime submodule of M.

Conversely, suppose that N is a prime submodule of M. There exist a basis $\{x_1, \ldots, x_n\}$ of M and non-zero elements $d_1, \ldots, d_r$ of R $(r \leqslant n)$ such that $N = Rd_1x_1 + \ldots + Rd_rx_r$. Suppose that $x_i = (x_{i1}, \ldots, x_{in})$ $(1 \leqslant i \leqslant n)$, then $\det(x_{ij}) = u$ is a unit of R. If $r = n$, then $\det(d_ix_{ij}) = d_1 \ldots d_n u \neq 0$, which is impossible (because $N = Ra_1 + \ldots + Ra_n = Rd_1x_1 + \ldots + Rd_nx_n$ implies that $0 = \det(a_{ij}) = \det(d_ix_{ij})$, by Lemma 2.1). Therefore $r < n$. Note that $d_ix_i \in N$ and $d_iM \nsubseteq N$, thus $x_i \in N$ $(1 \leqslant i \leqslant r)$. Hence $N = Rx_1 + \ldots + Rx_r$. Let $K = Rx_{r+1} + \ldots + Rx_n$. Then $M = N \oplus K$. □

3. Some special cases

In this section we consider the module $M = R \times R$ over a principal ideal domain R.

Let N be a submodule of M. There are elements a, b, c, and d of R such that $N = R(a,b) + R(c,d)$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\Delta = \det A = ad - bc$. Then the adjoint matrix of A has the simple form $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Therefore we have the following result.

3.1 Proposition. *Let $N = R(a,b) + R(c,d)$ be a submodule of M and $\Delta = ad - bc \neq 0$. Then*

$$N = \{(x,y) \in M\colon \Delta \text{ divides both } ay - bx \text{ and } cy - \mathrm{d}x\}.$$

Let $N = R(a,b) + R(c,d)$ be a submodule of M and let $\Delta = ad - bc \neq 0$. If N is a prime submodule of M, then Theorem 2.4 implies that $\Delta = up$ or $\Delta = up^2$ for some unit $u \in R$ and a prime element $p \in R$. In the case $\Delta = up^2$, $p = p^{2-1}$ must divide the entries of the adjoint matrix of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Therefore p divides a, b, c and d and hence $N \subseteq pM$. On the other hand, $up^2 \in (N\colon M)$, which is a prime ideal of R. Thus $p \in (N\colon M)$ so that $pM \subseteq N$. Hence $N = pM$ and by [5, Proposition 2.4], N is of height one. The height of prime submodules of M with $\Delta = up$ will be discussed later.

3.2 Lemma. *Let $N = R(a,b) + R(c,d)$ be a submodule of M. Then N is cyclic if and only if $\Delta = 0$.*

P r o o f. Suppose that N is cyclic. Then $N = R(x,y)$ for some $(x,y) \in M$. There are $r, s \in R$ such that $(a,b) = r(x,y)$ and $(c,d) = s(x,y)$ and so $\Delta = ad - bc = rxsy - rysx = 0$.

Conversely, suppose that $\Delta = 0$. If one of the elements a, b, c or d is zero, then the result is clear. (Indeed, if $a = 0$, then $0 = ad - bc = -bc$. Therefore $b = 0$ or $c = 0$. If $b = 0$, then $N = R(c,d)$ and we are done. Now if $c = 0$, then $N = R(0,b) + R(0,d) = R(0,e)$, where $Re = Rb + Rd$.) Now suppose that a, b, c and d are all non-zero. Let f be the greatest common divisor (gcd) of the elements a and c and let g be the gcd of the elements b and d, so that $a = a'f$, $c = c'f$, $b = b'g$ and $d = d'g$ for some $a', b', c', d' \in R$. Since $ad = bc$, we have $a'd'fg = b'c'fg$ and so $a'd' = b'c'$. As a' and c' are coprime, a' divides b' and b' divides a'. Hence $a' = b'u$ for some unit $u \in R$. Therefore, $c' = d'u$. Now it is easy to show that $N = R(uf, g)$. □

The proof of the following result can be found in [1] and [5].

3.3 Proposition. *Let $N = R(a,b)$ be a cyclic submodule of M. Then N is prime if and only if either $a = b = 0$ or a and b are coprime.*

Suppose that $N = R(a,b)$ is a non-zero prime submodule of M. Since $N \cong R$, every submodule of N is of the form $R(ta, tb)$ for some $t \in R$ and by the above proposition N is of height one.

3.4 Corollary. *Let $N = R(a,b) + R(c,d)$ be a submodule of M and $\Delta = ad - bc = up$ for some unit $u \in R$ and a prime element $p \in R$. Then N is a prime submodule of height two.*

P r o o f. By the remark after Theorem 2.4, N is a prime submodule of M. Let K be a non-zero prime submodule of M contained in N. Then $K = R(x,y) + R(z,w)$ for some (x,y) and $(z,w) \in M$. There are $q, r, s,$ and $t \in R$ such that $(x,y) =$

$q(a,b)+r(c,d)$ and $(z,w)=s(a,b)+t(c,d)$. Hence

$$xw-yz=(qt-rs)(ad-bc)=up(qt-rs).$$

Since K is a prime submodule of M, there are three choices for $qt-rs$.

i) If $qt-rs=0$, then $xw-yz=0$ and so K is a cyclic prime submodule of M. Therefore, K is of height one.

ii) If $qt-rs=u'p$ for some unit $u'\in R$, then $xw-yz=uu^rp^2$ and so $K=pM$. Therefore, K is of height one.

iii) If $qt-rs=v$ is a unit of R, then it is easy to check that $N=K$.

Consequently, N is of height two. □

4. Primary decomposition in R^n

As in Section 2, let M be the free module R^n over a principal ideal domain R for some integer $n\geqslant 2$.

We know that every submodule of a Noetherian module has a primary decomposition, [4], and also that M is a Noetherian R-module.

We begin our investigation by the following result.

4.1 Theorem. *Let $N=Ra_1+\ldots+Ra_n$ be a proper submodule of M. Let $A=(a_{ij})$ and $\Delta=up_1^{\alpha_1}\ldots p_s^{\alpha_s}$ for some distinct prime elements $p_k\in R$, positive integers α_k, and unit $u\in R$. Then N has a minimal primary decomposition $N=Q_1\cap\ldots\cap Q_s$ where $Q_k=\{(x_1,\ldots,x_n)\in M\colon\, p_k^{\alpha_k}$ divides $\sum\limits_{i=1}^{n}x_ia'_{ij}$ $(1\leqslant j\leqslant n)\}$. Note that $A'=(a'_{ij})$ is the adjoint matrix of A.*

Proof. It is easy to check that Q_k is a primary submodule of M with $\sqrt{(Q_k\colon M)}=Rp_k$ $(1\leqslant k\leqslant s)$. By Proposition 2.2, $N\subseteq Q_1\cap\ldots\cap Q_s$. Now let $x=(x_1,\ldots,x_n)\in Q_1\cap\ldots\cap Q_3$. Then for each $1\leqslant k\leqslant s$, $p_k^{\alpha_k}$ divides $\sum\limits_{i=1}^{n}x_ia'_{ij}$ $(1\leqslant j\leqslant n)$. Consequently, Δ divides $\sum\limits_{i=1}^{n}x_ia'_{ij}$ $(1\leqslant j\leqslant n)$. Again by Proposition 2.2, $x\in N$. □

4.2 Corollary. *Let N be a proper submodule of M with $\Delta\neq 0$. Then N is a primary submodule of M if and only if $\Delta=up^{\alpha}$ for some unit $u\in R$, a prime element $p\in R$, and a positive integer α.*

Suppose that $N\neq 0$ is a submodule of M with $\Delta=0$. There exist a basis $\{x_1,\ldots,x_n\}$ of M and non-zero elements $d_1,\ldots,d_r$ $(r\leqslant n)$ of R such that $N=$

$Rd_1x_1 + \ldots + Rd_rx_r$. Let $x_i = (x_{i1}, \ldots, x_{in})$, then by Corollary 2.3, $\det(x_{ij}) = u$ for some unit u of R. Since $\Delta = 0$, $r < n$. Suppose that $d_i = u_ip_1^{\alpha_{i1}} \ldots p_s^{\alpha_{is}}$ $(1 \leqslant i \leqslant r)$, where u_i is a unit of R, p_k is a prime element of R and $\alpha_{ik} \geqslant 0$ $(1 \leqslant k \leqslant s)$. Let $Q = Rx_1 + \ldots + Rx_r$. Theorem 2.5 implies that Q is a prime and hence a primary submodule of M. Now set $Q_k = Rp_k^{\alpha_{1k}}x_1 + \ldots + Rp_k^{\alpha_{rk}}x_r + Rx_{r+1} + \ldots + Rx_n$ $(1 \leqslant k \leqslant s)$. Then by Corollary 4.2, Q_k is a primary submodule of M. It is clear that $N \subseteq Q \cap Q_1 \cap \ldots \cap Q_s$. Now let $y \in Q \cap Q_1 \cap \ldots \cap Q_s$ and suppose that $y = a_1x_1 + \ldots + a_nx_n$ for some $a_i \in R$. Since $y \in Q$, we have $a_{r+1} = \ldots = a_n = 0$. Also since $y \in Q_k$ $(1 \leqslant k \leqslant s)$, we conclude that for each $1 \leqslant i \leqslant r$, $p_k^{\alpha_{ik}}$ divides a_i and hence d_i divides a_i. Therefore $y \in N$. Thus we have proved:

4.3 Theorem. *Let $N \neq 0$ be a submodule of M with $\Delta = 0$. Then $N = Q \cap Q_1 \cap \ldots \cap Q_s$ is a minimal primary decomposition of N, where $Q, Q_1, \ldots, Q_s$ are as above.*

4.4 Corollary. *Let N be a submodule of M with $\Delta = 0$. Then N is a primary submodule if and only if N is a prime submodule.*

References

[1] *S. M. George, R. Y. McCasland and P. F. Smith*: A principal ideal theorem analogue for modules over commutative rings. Comm. Algebra *22* (1994), 2083–2099. Zbl 0795.13001

[2] *C. P. Lu*: Prime submodules of modules. Comment. Math. Univ. St. Paul *33* (1984), 61–69. Zbl 0575.13005

[3] *H. Matsumura*: Commutative Ring Theory. Cambridge University Press, 1986. Zbl 0603.13001

[4] *R. Y. Sharp*: Steps in Commutative Algebra. Cambridge University Press, 1990. Zbl 0703.13001

[5] *Y. Tiras and A. Harmanci*: On prime submodules and primary decomposition. Czechoslovak Math. J. *50* (2000), 83–90. Zbl 1036.13010

Author's address: Department of Mathematics, College of Science, Shiraz University, Shiraz 71454, Iran, e-mail: `bamini@shirazu.ac.ir`, `sharif@susc.ac.ir`.