Czechoslovak Mathematical Journal, 50 (125) (2000), 83–90

ON PRIME SUBMODULES AND PRIMARY DECOMPOSITION

Yücel Tiraş and Abdullah Harmanci, Ankara

(Received April 1, 1997)

Abstract. We characterize prime submodules of $R \times R$ for a principal ideal domain R and investigate the primary decomposition of any submodule into primary submodules of $R \times R$.

Keywords: Prime submodule, primary submodule, primary decomposition, Associated primes

MSC 2000: 13C13, 13C99

1. Introduction

Throughout this note all rings are commutative with identity and all modules are unital. Let R be a ring and M an R-module. A submodule K of M is called prime if $K \neq M$ and given $r \in R$, $m \in M$ then $rm \in K$ implies $m \in K$ or $rM \subseteq K$.

Definition 1.1. Let M be a module and K a submodule of M. Let n be a non-negative integer. We say that K has height n if there exists a chain

$$K = K_0 \supset K_1 \supset \ldots \supset K_n$$

of prime submodules K_i $(0 \leqslant i \leqslant n)$ of M, but no such chain that is longer. Otherwise, we say that K has infinite height.

For any submodule K of an R-module M let

$$(K : M) = \{r \in R \colon\ rM \subseteq K\}\,.$$

Clearly $(K : M)$ is an ideal of R. The following lemma is wellknown (see, for example, [2, Theorem 1]).

Lemma 1.2. *Let R be a commutative ring and let M be an R-module. Then a submodule K of M is prime if and only if $P = (K : M)$ is a prime ideal of R and M/K is a torsion-free (R/P)-module.*

Matsumura proved in [8] that all prime ideals of the ring $R_1 \times R_2 \times \ldots \times R_n$, where R_i is a ring for all $i = 1, \ldots, n$, are of the form $R_1 \times \ldots R_{i-1} \times P_i \times R_{i+1} \times \ldots \times R_n$ where P_i is a prime ideal of R_i. The natural question about prime submodules of $R_1 \times R_2 \times \ldots \times R_n$ is still open. Some of the prime submodules of $R^{(n)}$ where R is a PID were studied in [5]. Now we begin our investigation leading to a characterization of the prime submodules of $R \times R$ by giving some necessary definitions and useful lemmas.

From now on, we employ R to denote a principal ideal domain (PID) and M to denote $R \times R$.

For any prime element p in R, it is easy to see that $R \times pR$, $pR \times R$, $\{0\} \times R$ and $R \times \{0\}$ are all prime submodules of M. Also we can see that for unequal prime elements p and q, $pR \times qR$ is not a prime submodule of M. (Take $R = \mathbb{Z}$, the set of integers, $M = \mathbb{Z} \times \mathbb{Z}$, $p = 2$ and $q = 3$.) Also we note that, for any prime element p, $R \times pR$ and $pR \times R$ are maximal submodules of M.

Now let us consider the set $N = \{(x, x)\colon\ x \in R\}$. It is easy to see that N is a prime submodule of M. The remaining classes of prime submodules of M are given in the next section.

2. The prime submodules

Lemma 2.1. *Let a and b be non-zero elements in R. Let $N = (a, b)R$. Then N is a prime submodule of M if and only if the elements a and b are coprime.*

P r o o f. Let $N = (a, b)R$ be a prime submodule of M. Suppose the greatest common divisor (g.c.d.) of a and b is d which is not equal to 1. Then there exist coprime numbers a_1 and b_1 in R such that $a = da_1$ and $b = db_1$. Then $(a, b) = d(a_1, b_1) \in N$. Since N is prime, $(a_1, b_1) \in N$ or $dM \subseteq N$. Suppose that $dM \subseteq N$. From this we get $d(1, 0) \in N$ and $d(0, 1) \in N$. But if $d(1, 0) \in N$ we get $b = 0$ and if $d(0, 1) \in N$ we get $a = 0$, a contradiction. Thus $dM \nsubseteq N$. Then $(a_1, b_1) \in N$. This gives us $N = (a_1, b_1)R$. Conversely, let the g.c.d. of a and b be 1. Then we wish to prove that N is a prime submodule of M. Let $r \in R$ and $(m, n) \in M$ be a such that $r(m, n) \in N$. Then there exists $x \in R$ such that $rm = ax$ and $rn = bx$. From this we get $m = ab'$ and $n = bb'$ for some $b' \in R$. This completes the proof. □

The following lemma is wellknown. We give the proof for the sake of completeness.

Lemma 2.2. *Let $N = (a, b)R$ be a prime submodule of M. Then N is a direct summand of M.*

P r o o f. Assume that $N = (a, b)R$ is a prime submodule of M. Since $\{0\} \times R$ and $R \times \{0\}$ are prime submodules and direct summands of M we may assume that a and b are non-zero elements in R. By Lemma 2.1 there exist c, d in R such that $ad + bc = 1$. Let $K = (-c, d)R$. Then we have $M = N + K$. It is easy to see that $N \cap K = (0)$. This completes the proof. □

Proposition 2.3. *Let N be a prime submodule of M which is distinct from $R \times \{0\}$ and $\{0\} \times R$. Then*

(i) *if $(1, 0) \in N$ then $N = R \times pR$ for some prime element p in R,*

(ii) *if $(0, 1) \in N$ then $N = pR \times R$ for some prime element p in R.*

P r o o f. (i) Let $(a, b) \in N$. Suppose the g.c.d. of a and b is d. Then there exist a_1 and b_1 in R such that $(a, b) = d(a_1, b_1) \in N$. Since N is a prime submodule of M, either $(a_1, b_1) \in N$ or $dM \subseteq N$. Suppose that $(a_1, b_1) \in N$. From the hypothesis we get $(0, b_1) \in N$. This implies that $b_1 M \subseteq N$, otherwise $N = M$. There exists a prime element p in R such that $pM \subseteq N$. Therefore we get $N = R \times pR$. Now we suppose that $dM \subseteq N$. For some prime element p in R we get $pM \subseteq N$. This completes the proof of part (i).

(ii) This can be proved using the same argument as in (i). □

Proposition 2.4. *Let p be a prime element in R. Then pM is a prime submodule of M of height* 1.

P r o o f. Since $(pM : M) = p$, pM is a prime submodule of M by Lemma 1.2 or by the remark just before Lemma 3 in [6] . Suppose there exists a prime submodule N in M such that $pM \supset N \supset 0$. Let $(m, n) \in N$. Then $m = px$ and $n = py$ for some x and y in R. Since N is prime, either $(x, y) \in N$ or $pM \subseteq N$. Suppose $(x, y) \in N$. Then for each $r \in \mathbb{Z}^+$ (where $\mathbb{Z}^+$ is the set of positive integers), p^r divides m, which is a contradiction. So we get the desired result. □

The following proposition and Proposition 2.4 characterize all prime submodules of M of height 1.

Proposition 2.5. *Let N be a prime submodule of M of height* 1. *Then*

(i) *if N has an element (a, b) such that the g.c.d. of a and b is* 1 *then $N = (a, b)R$,*

(ii) *if there are no pairs in N whose g.c.d. is* 1 *then there is a prime element p in R such that $N = pM$.*

P r o o f. (i) This is easy by Lemma 2.1.

(ii) Suppose that for all (a,b) in N the g.c.d. of a and b is distinct from 1. Let $(a,b) \in N$ be such that the g.c.d. of a and b is d. Then we get $dM \subseteq N$. So the result follows from Proposition 2.4. □

The prime elements in R characterize, under some conditions, some of the prime submodules in M.

Proposition 2.6. *Let p be a prime element in R. Let $a, b \in R$ be such that the pairs a, b and a, p and b, p are coprime. Then*
(i) *$K = \{(c,d) \in M\colon\ p$ divides $ad - bc\}$ is a prime submodule of M,*
(ii) *the set $\{(c,d) \in M\colon\ ad = bc\}$ is a prime submodule of M.*

Proof. (i) It is clear that K is a proper submodule of M. Take $(u,v) \in M$ and $r \in R$ such that $r(u,v) \in K$ and $(u,v) \notin K$. The prime element p divides $rav - rbu$ but does not divide $av - bu$. This completes the proof.

(ii) This follows from [5, Lemma 4]. □

To find a new prime submodule of M, we assume that N is a submodule of M which is distinct from $pR \times R$ and $R \times pR$ for some prime element p in R.

Theorem 2.7. *Let the situation be as above. Suppose that N is a submodule of M and $(a,b) \in N$ with the g.c.d. of a and b being 1. Also assume that $pM \subseteq N$ for some prime element p in R. Then N is a prime submodule of M if and only if $N = \{(c,d) \in M\colon\ p$ divides $ad - bc\}$.*

Proof. Note that if p divides a then $(a,0) \in N$. Hence $b(0,1) \in N$. Since the g.c.d. of a and b is 1, p does not divide b and so $bM \nsubseteq N$. Hence by Proposition 2.3 (ii), $N = pR \times R$. This contradicts our hypothesis. Therefore p does not divide a. We may assume that the pairs a, p and b, p are coprime. Then there exist $a_1, b_1, a_2, b_2, p_1, p_2$ in R such that

$$(*) \qquad aa_1 + pp_1 = 1,\ bb_1 + pp_2 = 1 \quad \text{and} \quad aa_2 + bb_2 = 1\ldots$$

Set $K = \{(c,d) \in M\colon\ p \text{ divides } ad - bc\}$.

Let $(c,d) \in N$. Assume that p does not divide $ad - bc$. Since $(a,b), (c,d) \in N$, we get $(ad - bc, 0) \in N$. By assumption we have $(ad - bc)M \subseteq N$. But this leads to a contradiction. Hence p divides $ad - bc$ and so $(c,d) \in K$. Conversely, let $(c,d) \in K$. Then there exists $t \in R$ such that $ad - bc = pt$. From $(*)$ we have $(c,d) = (bb_1c + pp_2c, aa_1d + pp_1d)$. Since $pM \subseteq N$, to see that $(c,d) \in N$ it is enough to show that $(bb_1c, aa_1d) \in N$. Since $ad - bc = pt$, we have $(bb_1c,\ aa_1d) = (adb_1 + ptb_1,\ aa_1d)$. Hence it will be enough to show that $(adb_1,\ ada_1) \in N$. But since $(a,b) \in N$, we have $(aa_1, ba_1) \in N$. From $(*)$ we get $(1, ba_1) \in N$ and then $(bb_1, ba_1) \in N$. Since N is prime we conclude that $bM \subseteq N$ or $(b_1, a_1) \in N$. This completes the proof since the sufficiency is clear from Proposition 2.6. $\square$

We note that any submodule of M can be generated by 2-elements. Now we investigate such modules. Let $N = (a,b)R + (c,d)R$ be a proper submodule of M where a, b, c, d are elements in R. We define $\Delta = ad - bc$, and we may assume that $\Delta M \subseteq N$. The following proposition characterizes some of the prime submodules of M.

Proposition 2.8. *Let N and Δ be as above. If Δ is a prime element in R then N is a prime submodule of M.*

Proof. Let $K = \{(x,y) \in M \colon \Delta \text{ divides } ay - bx \text{ and } cy - dx\}$. Then it is easy to see that $N \subseteq K$. Let $(x,y) \in K$. Then $ay - bx = \Delta t$ and $cy - dx = \Delta t_1$ for some t, t_1 in R. Thus we get $x = -at_1 + ct$, $y = dt - bt_1$ and then $(x,y) \in N$. It follows that $N = K$. Hence, since K is prime, we see that N is a prime submodule of M. $\square$

Let N and Δ be as in Proposition 2.8. Also suppose that N is prime and $\Delta = p_1 \ldots p_n$ (all distincts primes). Then there is only one prime p_i $(1 \leqslant i \leqslant n)$ such that $p_i M \subseteq N$. In view of this fact we obtain the following

Proposition 2.9. *Let N and Δ be as in Proposition 2.8. Assume that, for some prime element p, $pM \subseteq N$ and $\Delta = pq$ where p and q are coprime. Then N is prime if and only if*

$$N = \{(x,y) \colon p \text{ divides } ay - bx \text{ and } cy - dx\}.$$

Proof. Let $K = \{(x,y) \in M \colon p \text{ divides } ay - bx \text{ and } ay - dx\}$. Suppose that N is prime. Then it is clear that $N \subseteq K$. For the converse, let $(x,y) \in K$. Then for some $t, t_1 \in R$ we have

$$ay - bx = pt \qquad \text{and} \qquad cy - dx = pt_1.$$

Then we get $qx = tc - at_1$ and $qy = dt - bt_1$. Hence $(qx, qy) \in N$. Since N is prime we get $(x,y) \in N$. Therefore we have $N = K$. This completes the proof since the necessity is clear. $\square$

Now we conclude this section by the following proposition.

Proposition 2.10. *Let N be a prime submodule of M distinct from both $R \times \{0\}$ and $\{0\} \times R$. Suppose that (a,b) and $(c,d) \in N$ are such that the g.c.d. of the pairs*

a, b and c, d is 1. Then N is either in the form $pR \times R$, $R \times pR$ for some prime element p in R or it is one of the prime submodules mentioned in Theorem 2.7.

Proof. We divide the proof into two parts. First suppose that $a \neq c$ but $b = d$. Then $(a - c, 0) \in N$. Then either $(a - c)M \subseteq N$ or $(1, 0) \in N$. If $(1, 0) \in N$ then, by Proposotion 2.3 (i), $N = R \times pR$. Otherwise there exists a prime element p in R such that $N = \{(c, d) \in M\colon\ p \text{ divides } ad - bc\ \}$ by Theorem 2.7. Secondly, $a \neq c$ but $b \neq d$. Then $(0, ad - bc) \in N$. Then either $(ad - bc)M \subseteq N$ or $(0, 1) \in N$. Now the result follows from Proclaim 2.3 (ii) or Theorem 2.7. □

3. Primary decomposition

In this section we investigate the primary decomposition of the submodules of M where we still take R as a principal ideal domain and M as $R \times R$. First we give the definition of the primary submodule. Let N be a proper submodule of M. Then we say that N is a primary submodule of M if $r \in R$, $m \in M$, $rm \in N$ implies $m \in N$ or $r^k M \subseteq N$ for some positive integer k. If N is a primary submodule of M then the radical of the ideal $(N : M)$ is a prime ideal of R. If the radical of $(N : M)$ which is denoted by $\sqrt{N : M}$ is equal to P then N is called a P-primary submodule of M.

Definition 3.1. Let N be a proper submodule of M. A primary decomposition of N in M is an expression for N as an intersection of finitely many primary submodules of M. Such a primary decomposition $N = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ with Q_i P_i-primary in M $(1 \leqslant i \leqslant n)$ of N in M is said to be minimal precisely when

(i) $P_1, \ldots, P_n$ are n different prime ideals of R; and
(ii) for all $j = 1, \ldots, n$, we have

$$Q_j \not\supseteq \bigcap_{\substack{i=1 \\ j \neq i}}^{n} Q_i.$$

Remark 3.2. Let N be a proper submodule of M. Then by [9, 9.27 and 9.31] N has a minimal primary decomposition in M. Let $N = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ with Q_i P_i-primary in M $(1 \leqslant i \leqslant n)$ be a minimal primary decomposition of N in M. Then by [9, 9.31], for a prime ideal P of R we have

$$P \in \{P_1, \ldots, P_n\} \Longleftrightarrow P \in \operatorname{Ass}_R(M/N).$$

Lemma 3.3. *Let p be a prime element in R. Then $p^r M$ (where r is positive integer) is a primary submodule of M.*

Now we can give the primary decomposition of the submodules of M in the form $(a,b)R$ where the g.c.d. of a and b is distinct from 1.

Proposition 3.4. *Let N be a cyclic submodule of M whose g.c.d. of the generators is different from* 1. *Then*

$$N=(p_1^{r_1}M)\cap(p_2^{r_2}M)\cap\ldots\cap(p_s^{r_s}M)\cap N_1$$

where $p_1,\ldots,p_s$ are distinct prime elements in R and N_1 is a prime submodule of M containing N.

P r o o f. Let $N=(a,b)R$ and suppose that the g.c.d. of a and b is d and that the distinct prime factors of d are $p_1,\ldots,p_s$. Then $d=p_1^{r_1}\ldots p_s^{r_s}$. Now we claim that the primary decomposition of N is $(p_1^{r_1}M)\cap\ldots\cap(p_s^{r_s}M)\cap((a_1,b_1)R)$ where $a=da_1$ and $b=db_1$. Let $(x,y)\in(p_1^{r_1}M)\cap\ldots\cap(p_s^{r_s}M)\cap((a_1,b_1)R)$. Then

$$x=p_1^{r_1}u_1=p_2^{r_2}u_2=\ldots=p_s^{r_s}u_s=a_1t_1,$$
$$y=p_1^{r_1}v_1=p_2^{r_2}v_2=\ldots=p_s^{r_s}v_s=b_1t_1$$

where $u_1,u_2,\ldots,u_s,v_1,\ldots,v_s$ are all in R. Hence we get $(x,y)\in(a,b)R=N$. This completes the proof since the reverse inclusion is clear. □

Corollary 3.5. *Let N be as in Proposition* 3.4. *Then*

$$\mathrm{Ass}_R(M/N)=\{0,P_1,\ldots,P_n\}$$

where P_i denotes the prime ideal which is generated by the prime element p_i in R for all $i=1,\ldots,n$.

P r o o f. This follows from Proposition 3.4, [9, (9.33)(ii)] and $\sqrt{(a_1,b_1)R:M}=0$. □

Now we take N with two generators. To get the primary decomposition of N we give the following lemma.

Lemma 3.6. *Let $N=(a,b)R+(c,d)R$, $a,b,c,d\in R$, be a proper submodule of M. Let $\Delta=ad-bc$ be a non-zero element in R. Then for any factor p^r of Δ with $r\in\mathbb{Z}^+$,*

$$Q=\{(x,y)\colon\ p^r \text{ divides } ay-bx \text{ and } cy-dx\}.$$

is a primary submodule of M.

Now we are ready to give the main theorem of this section.

Theorem 3.7 (Primary Decomposition). *Let the situation be as in Lemma* 3.6. *If* $\Delta = p_1^{r_1} \dots p_t^{r_t}$ *where* $p_1, \dots, p_t$ *are distinct prime elements in* R *and* $r_1, \dots, r_t \in \mathbb{Z}^+$ *then* N *has a primary decomposition*

$$N = \bigcap_{i=1}^{t} K_i$$

where $K_i = \{(x, y)\colon\ p_i^{r_i}$ *divides* $ay - bx$ *and* $cy - dx\}$ *for all* i $(1 \leqslant i \leqslant t)$.

P r o o f. Set $K = \cap_{i=1}^t K_i$. Then $N \subseteq K$ is clear.

Let $(x, y) \in K$. Then there exist $t_i, s_i \in R$ such that $ay - bx = p_i^{r_i} t_i$ and $cy - dx = p_i^{r_i} s_i$ for each i, $1 \leqslant i \leqslant t$. Then for some $t, s \in R$ we get

$$ay - bx = \Delta t \qquad \text{and} \qquad cy - dx = \Delta s$$

Now the result follows from Proposition 2.9. □

Corollary 3.8. *Let* N *be as in Theorem* 3.7. *Then* $\operatorname{Ass}_R(M/N) = \{P_1, \dots, P_t\}$ *where* P_i *denotes the prime ideal which is generated by the prime element* p_i *in* R *for all* $i = 1, \dots, n$.

P r o o f. This follows from [9, (9.33) (ii)]. □

References

[1] *J. Jenkins and P. F. Smith*: On the prime radical of a module over a commutative ring. Comm. Algebra *20 (12)* (1992), 3593–3602.

[2] *C. P. Lu*: Prime submodules of modules. Comm. Math. Univ. Sancti. Pauli *33* (1984), 61–69.

[3] *C. P. Lu*: M-radicals of submodules in modules. Math. Japon. 34 (1989), no. 2, 211–219.

[4] *C. P. Lu*: M-radicals of submodules in modules II. Math. Japon. 35 (1990), no. 5, 991–1001.

[5] *S. M. George, R. Y. McCasland and P. F. Smith*: A principal ideal theorem analogue for modules over commutative rings. Comm. Algebra *22 (6)* (1994), 2083–2099.

[6] *R. Y. McCasland and M. E. Moore*: On radicals of submodules of finitely generated modules. Canad. Math. Bull. *29 (1)* (1986).

[7] *R. Y. McCasland and P. F. Smith*: Prime submodules of Noetherian modules. Rocky Mountain J. Math. *23* (1993), no. 3.

[8] *H. Matsumura*: Commutative Ring Theory. Cambridge University Press, 1980.

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

Author's address: Hacettepe University, Department of Mathematics, 06532 Beytepe, Ankara, Turkey.