Turk J Math
27 (2003) , 329 – 342.

On Prime Submodules of Finitely Generated Free Modules

Dilek Pusat-Yılmaz

Abstract

The aim of this work is to investigate prime submodules of finitely generated free modules over commutative domains in some special cases.

Throughout this work all rings will be commutative with identity. Let M be an R-module. For any submodule N of M we set $(N : M) = \{r \in R : rM \subseteq N\}$. A submodule K of M is said to be *prime* if $K \neq M$ and whenever $r \in R, m \in M$ and $rm \in K$ then $m \in K$ or $r \in (K : M)$. It is well known that a submodule K of M is prime if and only if $\mathcal{P} = (K : M)$ is a prime ideal of R and the $(R/\mathcal{P})$-module M/K is torsion-free [2, Lemma 1]. We say that K is a $\mathcal{P}$-*prime* submodule of M if K is a prime submodule of M with $\mathcal{P} = (K : M)$.

1. Modules over Special Rings

We point out that for certain rings R we can say a good deal about prime submodules of any R-module M. First we recall the following result.

Lemma 1.1 *[3, Proposition 2] If N is a submodule of an R-module M with $(N:M)$ a maximal ideal of R, then N is a prime submodule. In particular, $\mathcal{M}M$ is a prime submodule of an R-module M for every maximal ideal $\mathcal{M}$ of R such that $\mathcal{M}M \neq M$.*

1991 *AMS subject classification:* 16D10, 13C10.

Proposition 1.2 *Let R be a 0-dimensional ring (i.e. every prime ideal is maximal) and let M be an R-module. Then a proper submodule N of M is prime if and only if $\mathcal{P}M \subseteq N$ for some prime ideal $\mathcal{P}$ of R.*

Proof. By Lemma 1.1. □

Given a commutative domain R it is well known that any finitely generated torsion-free R-module is projective if and only if R is a Prüfer domain (see [6, Theorem 4.22]).

Proposition 1.3 *Let R be a Prüfer domain and let M be a finitely generated R-module. Then a proper submodule N of M is a 0-prime submodule if and only if $M = N \oplus N'$ for some torsion-free submodule N' of M.*

Proof. Suppose first that $M = N \oplus N'$ for some torsion-free submodule N' of M. Then $M/N \cong N'$ so that M/N is torsion-free. Thus N is a 0-prime submodule of M.

Conversely, suppose that N is a 0-prime submodule of M. Then the R-module M/N is finitely generated torsion-free so that M/N is projective and hence $M = N \oplus N'$ for some submodule N'. Clearly N' is torsion-free. □

Dedekind domains are precisely Noetherian Prüfer domains and have the property that every non-zero prime ideal is maximal. Combining Lemma 1.1 and Proposition 1.3 we have the following result.

Proposition 1.4 *Let R be a Dedekind domain and let M be a finitely generated R-module. Then a proper submodule N of M is prime if and only if $M = N \oplus N'$ for some torsion-free submodule N' of M or $\mathcal{P}M \subseteq N$ for some maximal ideal $\mathcal{P}$ of R.*

2. Cyclic Submodules of F

We now fix the following notation. Let R be a commutative domain, $n \geqslant 3$ be an integer and F be the free module $R^{(n)}$.

Lemma 2.1 *Let N be an m-generated submodule of F for some positive integer $m < n$. Then $(N : F) = 0$.*

Proof. Suppose that $(N : F) \neq 0$, i.e. $rF \subseteq N$ for some $0 \neq r \in R$. Let $S = R\backslash\{0\}$ and let K denote the field of fractions of R. Then the n-dimensional K-vector space $K^{(n)} \cong S^{-1}F = S^{-1}N$ and $S^{-1}N$ is generated by m elements as a vector space over the field K. Thus $n \leqslant m$, a contradiction. □

Corollary 2.2 *Let N be an m-generated submodule of F for some positive integer $m < n$. Then N is a prime submodule of F if and only if the R-module F/N is torsion-free.*

Proposition 2.3 *Let $a_i \in R$ $(1 \leqslant i \leqslant n)$ such that $R = Ra_1 + \cdots + Ra_n$. Then $R(a_1, \ldots, a_n)$ is a direct summand of the free R-module $F = R^{(n)}$. Moreover, $R(a_1, \ldots, a_n)$ is a 0-prime submodule of F.*

Proof. There exist $s_i \in R$ $(1 \leqslant i \leqslant n)$ such that $1 = s_1a_1 + \cdots + s_na_n$. Let

$$N = \{(x_1, \ldots, x_n) \in F : s_1x_1 + \cdots + s_nx_n = 0\}.$$

Consider the functions $\psi : R \to R^{(n)}$ defined by $r \mapsto r(a_1, \ldots, a_n)$ and $\varphi : R^{(n)} \to R$ defined by $(r_1, \ldots, r_n) \mapsto r_1s_1 + \cdots + r_ns_n$. Since $\varphi\psi$ is the identity map, $R^{(n)} = \mathrm{im}\psi \oplus \ker\varphi = R(a_1, \ldots, a_n) \oplus N$. Since F is free it is torsion-free and the factor module $F/R(a_1, \ldots, a_n)$ is torsion-free. This implies $(R(a_1, \ldots, a_n) : F) = 0$, and hence $R(a_1, \ldots, a_n)$ is a 0-prime submodule of F. □

Corollary 2.4 *Let $a_i \in R$ $(1 \leqslant i \leqslant n)$ and let $\mathcal{P}$ be a prime ideal of R such that $R = Ra_1 + \cdots + Ra_n + \mathcal{P}$. Then $R(a_1, \ldots, a_n) + \mathcal{P}F$ is a $\mathcal{P}$-prime submodule of F.*

Proof. The module $F/\mathcal{P}F$ is a free module over the domain $R/\mathcal{P}$. Let $N = R(a_1, \ldots, a_n) + \mathcal{P}F$. Then $N/\mathcal{P}F = R(a_1 + \mathcal{P}, \ldots, a_n + \mathcal{P})$. By Proposition 2.3, $N/\mathcal{P}F$ is a $\mathcal{P}$-prime submodule of the $(R/\mathcal{P})$-module $F/\mathcal{P}F$. Clearly it follows that N is a $\mathcal{P}$-prime submodule of F. □

Let $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero. By a *common divisor* of the elements a_i $(1 \leqslant i \leqslant n)$ we mean an element $d \in R$ such that $a_i = db_i$ $(1 \leqslant i \leqslant n)$ for some elements b_i $(1 \leqslant i \leqslant n)$. Clearly d is a common divisor of a_i $(1 \leqslant i \leqslant n)$ if and only if $Ra_1 + \cdots + Ra_n \subseteq Rd$. Corollary 2.2 has the following consequence.

Lemma 2.5 *Let $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero, such that $N = R(a_1, \ldots, a_n)$ is a prime submodule of $F = R^{(n)}$. Then every common divisor of a_i $(1 \leqslant i \leqslant n)$ is a unit in R.*

Proof. Let d be a common divisor of a_i $(1 \leqslant i \leqslant n)$. For each $1 \leqslant i \leqslant n$ there exists $b_i \in R$ such that $a_i = db_i$. Clearly $d \neq 0$ and $d(b_1, \ldots, b_n) = (a_1, \ldots, a_n) \in N$. By Corollary 2.2, $(b_1, \ldots, b_n) \in N$, i.e. $(b_1, \ldots, b_n) = r(a_1, \ldots, a_n)$ for some $r \in R$. It follows that $a_i = dra_i$ $(1 \leqslant i \leqslant n)$ and hence $dr = 1$. □

Theorem 2.6 *Let R be a UFD and let $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero. Then $N = R(a_1, \ldots, a_n)$ is a prime submodule of $F = R^{(n)}$ if and only if every common divisor of a_i $(1 \leqslant i \leqslant n)$ is a unit in R.*

Proof. The necessity is proved in Lemma 2.5.

Conversely, suppose that every common divisor of a_i $(1 \leqslant i \leqslant n)$ is a unit in R. Let $0 \neq r \in R, b_i \in R$ $(1 \leqslant i \leqslant n)$ such that $r(b_1, \ldots, b_n) \in N$, i.e. $r(b_1, \ldots, b_n) = s(a_1, \ldots, a_n)$ for some $s \in R$. Hence $rb_i = sa_i$ $(1 \leqslant i \leqslant n)$.

There exists $1 \leqslant j \leqslant n$ such that $a_j \neq 0$. Suppose that a_j is a unit in R. Then $s = rb_j a_j^{-1}$ and hence $rb_i = rb_j a_j^{-1} a_i$ giving $b_i = b_j a_j^{-1} a_i$ $(1 \leqslant i \leqslant n)$. In this case $(b_1, \ldots, b_n) = b_j a_j^{-1}(a_1, \ldots, a_n) \in N$. Now suppose that a_j is not a unit in R. Let p be any prime divisor of a_j. There exists $1 \leqslant k \leqslant n$ such that p does not divide a_k. However $rb_k = sa_k$ and $rb_j = sa_j$ together give $ra_j b_k = ra_k b_j$, so that $a_j b_k = a_k b_j$ and hence p divides b_j. Now $rb_j = sa_j$ gives $r(b_j/p) = s(a_j/p)$. Repeating this argument we conclude that a_j divides b_j, i.e. $b_j = ca_j$ for some $c \in R$. For each $1 \leqslant i \leqslant n$, $ra_i b_j = ra_j b_i$ gives $b_i = ca_i$. Hence $(b_1, \ldots, b_n) = c(a_1, \ldots, a_n) \in N$. It follows that N is a prime submodule of F. □

We shall call a submodule N of F a *cyclic prime* if N is a prime submodule of F and N is a cyclic R-module.

Corollary 2.7 *Let R be a UFD and let N be any prime submodule of $F = R^{(n)}$ with (N:F)=0. Then N is a sum of cyclic prime submodules of F.*

Proof. Let $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero, such that $(a_1, \ldots, a_n) \in N$. Let d be a greatest common divisor of the elements a_i $(1 \leqslant i \leqslant n)$. Then $a_i = db_i$ $(1 \leqslant i \leqslant n)$ for some elements b_i $(1 \leqslant i \leqslant n)$ of R. Clearly any common divisor of the elements b_i $(1 \leqslant i \leqslant n)$ is a unit in R. By Theorem 2.6, $R(b_1, \ldots, b_n)$ is a cyclic prime submodule of F. Moreover, $R(a_1, \ldots, a_n) \subseteq R(b_1, \ldots, b_n) \subseteq N$. The result follows. □

Given a submodule N of M the *prime radical* $\mathrm{rad}_M(N)$ is defined to be the intersection of all prime submodules of M containing N, and in case N is not contained in any prime submodule then $\mathrm{rad}_M(N)$ is defined to be M.

For the particular submodule in Theorem 2.6, the prime radical can be expressed in a simple form.

Proposition 2.8 *With the notation in Theorem 2.6, $rad_F(N) = R(b_1, \ldots, b_n)$, where $b_i = (p_1 \cdots p_m a_i)/d$ $(1 \leqslant i \leqslant n)$, d is a greatest common divisor* (gcd) *of $a_1, \ldots, a_n$; and either d is not a unit and $p_1, \ldots, p_m$ are the pairwise non-associate prime divisors of d, or d is a unit and $p_1 = \cdots = p_m = 1$.*

Proof. Suppose that d is a gcd of a_i $(1 \leqslant i \leqslant n)$. If d is a unit in R then N is prime by Theorem 2.6 and hence $\mathrm{rad}_F(N) = N = R(a_1, \ldots, a_n)$. Now suppose that d is not a unit in R. Then $d = p_1^{k_1} \cdots p_m^{k_m}$ for pairwise non-associate primes p_i $(1 \leqslant i \leqslant m)$ and positive integers k_i $(1 \leqslant i \leqslant m)$. For each $1 \leqslant i \leqslant n$ there exists $x_i \in R$ such that $a_i = dx_i$. Thus $(a_1, \ldots, a_n) = d(x_1, \ldots, x_n) = p_1^{k_1} \cdots, p_m^{k_m}(x_1, \ldots, x_n)$.

Let K be any prime submodule of F such that $N = R(a_1, \ldots, a_n) \subseteq K$. Then $p_1^{k_1} \cdots p_m^{k_m} R(x_1, \ldots, x_n) \subseteq K$ and hence $p_1 \cdots p_m R(x_1, \ldots, x_n) \subseteq K$. But $p_1 \cdots p_m R(x_1, \ldots, x_n) = R(p_1 \cdots p_m x_1, \ldots, p_1 \cdots p_m x_n) = R(b_1, \ldots, b_n)$. We have proved that $R(b_1, \ldots, b_n) \subseteq \mathrm{rad}_F(N)$. Note also that $N \subseteq R(b_1, \ldots, b_n)$.

Next we prove that $R(b_1, \ldots, b_n) = R(x_1, \ldots, x_n) \cap p_1 F \cap \cdots \cap p_m F$. Clearly $R(b_1, \ldots, b_n) \subseteq R(x_1, \ldots, x_n) \cap p_1 F \cap \cdots \cap p_m F$. Conversely, let $r \in R$ such that $r(x_1, \ldots, x_n) \in p_1 F \cap \cdots \cap p_m F$. For each $1 \leqslant i \leqslant m$, p_i divides rx_j $(1 \leqslant j \leqslant n)$ and hence p_i divides r, because $x_1, \ldots, x_n$ have no common prime divisor. Since $p_1, \ldots, p_m$ are pairwise nonassociates it follows that $p_1 \cdots p_m$ divides r. Thus $r(x_1, \ldots, x_n) \in R(b_1, \ldots, b_n)$, as required.

Since $(p_iF : F) = (p_i)$ is a prime ideal of R and F/p_iF is a torsion-free $R/(p_i)$-module, p_iF is a prime submodule of F $(1 \leqslant i \leqslant m)$. By Theorem 2.6, $R(x_1, \ldots, x_n)$ is prime. Hence the proof is completed. □

A submodule S of M is called *semiprime* if S is an intersection of prime submodules of M, i.e. $\mathrm{rad}_M(S) = S$. A non-zero element r of a UFD R will be called *square-free* if there does not exist a prime p in R such that $r = p^2 s$ for some $s \in R$. Compare the next result with Theorem 2.6.

Corollary 2.9 *Let R be a UFD, let n be a positive integer, let $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero, and let N be the submodule $R(a_1 \ldots, a_n)$ of $F = R^{(n)}$. Then N is a semiprime submodule of F if and only if any greatest common divisor of a_i $(1 \leqslant i \leqslant n)$ is square-free.*

Proof. Let d be a greatest common divisor of a_i $(1 \leqslant i \leqslant n)$. Suppose that d is square-free. If d is a unit then N is prime by Theorem 2.6. Suppose that d is not a unit. Then in the notation of Proposition 2.8, $d = up_1 \cdots p_m$ for some unit u in R and hence $b_i = u^{-1}a_i$ $(1 \leqslant i \leqslant n)$. In this case, $N = \mathrm{rad}_F(N)$, by Proposition 2.8, and hence N is semiprime.

Conversely, suppose that N is semiprime. If d is a unit then square-free. Suppose that d is not a unit. Then Proposition 2.8 gives $N = \mathrm{rad}_F(N) = R(b_1, \ldots, b_n)$ where $b_i = (p_1 \cdots p_m a_i)/d$ $(1 \leqslant i \leqslant n)$. There exists $r \in R$ such that $(b_1, \ldots, b_n) = r(a_1, \ldots, a_n)$ and there exists $1 \leqslant j \leqslant n$ such that $a_j \neq 0$. Hence $(p_1 \cdots p_m a_j)/d = ra_j$, so that $p_1 \cdots p_m = dr$ and hence d is square-free. □

3. 2-Generated Submodules of F

In this section we are interested when $N = R(a_1, \ldots, a_n) + R(b_1, \ldots, b_n)$ is a prime submodule of $F = R^{(n)}$, where $R = Rb_1 + \cdots + Rb_n$. Consider the submodules

$$L = R(b_1, \ldots, b_n) \text{ and } L' = \{(x_1, \ldots, x_n) \in F : s_1x_1 + \cdots + s_nx_n = 0\}$$

of F, where $s_i \in R$ $(1 \leqslant i \leqslant n)$ and $1 = s_1b_1 + \cdots + s_nb_n$. Note first that $F = L \oplus L'$ by the proof of Proposition 2.3. Now $N = N \cap (L \oplus L') = L \oplus (N \cap L')$. Let $c = s_1a_1 + \cdots + s_na_n$. Then $N \cap L' \supseteq R(\mathbf{a} - c\mathbf{b})$, where $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots b_n)$, and $N = R(\mathbf{a} - c\mathbf{b}) \oplus R\mathbf{b}$, so that $N \cap L' = R(\mathbf{a} - c\mathbf{b})$.

Lemma 3.1 *Let R be a commutative domain and let N be a submodule of an R-module M such that the module M/N is torsion-free. Let L be a proper submodule of N. Then L is a 0-prime submodule of N if and only if L is a 0-prime submodule of M.*

Proof. Suppose first that L is a 0-prime submodule of M. Then the module M/L is torsion-free and hence the module N/L is torsion-free, i.e. L is a 0-prime submodule of N. Conversely, suppose that L is a 0-prime submodule of N. Then N/L and M/N are both torsion-free R-modules, so that M/L is torsion-free and L is a 0-prime submodule of M. □

Theorem 3.2 *Let R be a UFD, let $n \geqslant 3$ be a positive integer and $a_i, b_i \in R$ $(1 \leqslant i \leqslant n)$ such that $R = Rb_1 + \cdots + Rb_n$. Let $c = s_1a_1 + \cdots + s_na_n$ where $s_i \in R$ $(1 \leqslant i \leqslant n)$ and $1 = s_1b_1 + \cdots + s_nb_n$. Then $N = R(a_1, \ldots, a_n) + R(b_1, \ldots, b_n)$ is a prime submodule of $F = R^{(n)}$ if and only if either $a_i = cb_i$ $(1 \leqslant i \leqslant n)$ or every common divisor of $a_i - cb_i$ $(1 \leqslant i \leqslant n)$ is a unit in R.*

Proof. With the above notation, N is a prime submodule of F if and only if $N \cap L'$ is a prime submodule of L', because $F = L \oplus L'$ and $N = L \oplus (N \cap L')$ together give $F/N \cong L'/(N \cap L')$. Moreover, $(N \cap L' : L') = (N : F) = 0$ by Lemma 2.1. By Lemma 3.1, $N \cap L'$ is a prime submodule of L' if and only if $N \cap L'$ is a prime submodule of F. Now $N \cap L' = R(\mathbf{a} - c\mathbf{b})$. Thus $N \cap L'$ is a prime submodule of F if and only if $N \cap L' = 0$, i.e. $a_i = cb_i$ $(1 \leqslant i \leqslant n)$, or every common divisor of $a_i - cb_i$ $(1 \leqslant i \leqslant n)$ is a unit in R by Theorem 2.6. □

Remark: Note that if $N = R(a_1, \ldots, a_n) + R(b_1, \ldots, b_n)$ where $a_i, b_i \in R$ $(1 \leqslant i \leqslant n)$ and $R = Ra_1 + \cdots + Ra_n = Rb_1 + \cdots + Rb_n$ then in general N is not a prime submodule of F as the following example shows.

Example 3.3 *The submodule $N = \mathbb{Z}(2,3,5) + \mathbb{Z}(2,1,3)$ of the free $\mathbb{Z}$-module $F = \mathbb{Z}^{(3)}$ is not prime.*

Proof. Suppose that N is a prime submodule of F. The element $(4,4,8) = (2,3,5) + (2,1,3) \in N$. Thus $4(1,1,2) \in N$ and hence $(1,1,2) \in N$ by Lemma 2.1. It is easy to check that $(1,1,2) \neq s(2,3,5) + t(2,1,3)$ for any $s,t \in \mathbb{Z}$, a contradiction. Thus N is not prime. □

Theorem 3.2 deals only with the case $n \geqslant 3$. If $n = 1$ then $N = Ra_1 + Rb_1 = R$ which is not prime. We now deal with the case $n = 2$.

Proposition 3.4 *Let R be a commutative ring and let $a_i, b_i \in R$ $(i = 1,2)$ such that $R = Rb_1 + Rb_2$. Then $N = R(a_1,a_2) + R(b_1,b_2)$ is a prime submodule of $F = R^{(2)}$ if and only if $R(a_1b_2 - a_2b_1)$ is a prime ideal of R.*

Proof. There exist elements $s_1, s_2 \in R$ such that $1 = s_1b_1 + s_2b_2$. Then $F = L \oplus L'$ where $L = R(b_1,b_2)$ and $L' = \{(x,y) \in F : s_1x + s_2y = 0\}$. Clearly $R(-s_2,s_1) \subseteq L'$. Moreover,

$$(1,0) = s_1(b_1,b_2) + (-b_2)(-s_2,s_1) \text{ and } (0,1) = s_2(b_1,b_2) + b_1(-s_2,s_1)$$

together imply $F = L + R(-s_2,s_1)$. It follows that $L' = (L \cap L') + R(-s_2,s_1) = R(-s_2,s_1)$.

As before, $N = L \oplus (N \cap L')$ and $N \cap L' = R(a_1 - cb_1, a_2 - cb_2)$ where $c = s_1a_1 + s_2a_2$. Note that $(a_1 - cb_1, a_2 - cb_2) = (a_2b_1 - b_2a_1)(-s_2,s_1)$ because

$$\begin{aligned} -s_2(a_2b_1 - b_2a_1) &= -s_2a_2b_1 + s_2b_2a_1 \\ &= -s_2a_2b_1 + (1 - s_1b_1)a_1 \\ &= a_1 - (s_1a_1 + s_2a_2)b_1 \\ &= a_1 - cb_1, \text{ and} \end{aligned}$$

$$\begin{aligned} s_1(a_2b_1 - b_2a_1) &= s_1a_2b_1 - s_1b_2a_1 \\ &= (1 - s_2b_2)a_2 - s_1b_2a_1 \\ &= a_2 - (s_1a_1 + s_2a_2)b_2 \\ &= a_2 - cb_2. \end{aligned}$$

Note also that if $r \in R$ and $r(-s_2, s_1) = 0$ then $rs_2 = 0$, $rs_1 = 0$ and hence

$$r = r1 = r(s_1 b_1 + s_2 b_2) = (rs_1)b_1 + (rs_2)b_2 = 0.$$

Let $d = a_1 b_2 - a_2 b_1$. Now $F = L \oplus L'$ and $N = L \oplus (N \cap L')$ give that

$$F/N \cong L'/(N \cap L') = R(-s_2, s_1)/Rd(-s_2, s_1) \cong R/Rd.$$

Thus N is a prime submodule of F if and only if Rd is a prime ideal of R. □

In Proposition 3.4 it is crucial that $R = Rb_1 + Rb_2$. For, let N denote submodule $\mathbb{Z}(6,6) + \mathbb{Z}(10,10)$ of the free $\mathbb{Z}$-module $\mathbb{Z} \oplus \mathbb{Z}$. Then $N = \mathbb{Z}(2,2)$ and $2(1,1) \in N$, $(1,1) \notin N$, so that N is not prime (Corollary 2.2). However $a_1 = a_2 = 6$, $b_1 = b_2 = 10$ gives $\mathbb{Z}(a_1 b_2 - a_2 b_1) = 0$ which is a prime ideal of $\mathbb{Z}$.

We fix the following notation. Let n be a positive integer, let $a_{ij} \in R$ $(1 \leqslant i, j \leqslant n)$ and let $\mathbf{a}_i = (a_{i1}, \ldots, a_{in}) \in R^{(n)} = F$ for all $1 \leqslant i \leqslant n$. Let $N = R\mathbf{a}_1 + \cdots + R\mathbf{a}_n$ be a proper submodule of F. Let A denote the $n \times n$ matrix (a_{ij}) over R. Proposition 3.4 suggests that it might be the case that N is a prime submodule of F if and only if $R(\det A)$ is a prime ideal of R, provided that

$$R = Ra_{i1} + \cdots + Ra_{in} \quad (2 \leqslant i \leqslant n).$$

The next two examples show that in fact neither of these implications are true.

Example 3.5 *With the above notation,* $\mathbb{Z}(3,5,7) + \mathbb{Z}(0,2,1) + \mathbb{Z}(0,1,2)$ *is a prime submodule of* $F = \mathbb{Z}^{(3)}$ *but detA=9.*

Proof. Note that $A = \begin{bmatrix} 3 & 5 & 7 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$ so that clearly det$A$=9. Moreover,

$3(1,0,0) = (3,5,7) - (0,2,1) - 3(0,1,2) \in N$,
$3(0,1,0) = 0(3,5,7) + 2(0,2,1) - (0,1,2) \in N$,
$3(0,0,1) = 0(3,5,7) - (0,2,1) + 2(0,1,2) \in N$,
and $(1,0,0) \notin N$. Thus $3F \subseteq N \neq F$. It follows that N is a prime submodule of F by Lemma 1.1. □

Example 3.6 *With the above notation,* $\mathbb{Z}(3,5,7)+\mathbb{Z}(0,2,1)+\mathbb{Z}(0,2,1)$ *is not a prime submodule of* $F=\mathbb{Z}^{(3)}$ *but detA=0, which is a prime ideal of* $\mathbb{Z}$.

Proof. In this case, $A=\begin{bmatrix} 3 & 5 & 7 \\ 0 & 2 & 1 \\ 0 & 2 & 1 \end{bmatrix}$ and clearly det$A$=0.

Since $N=\mathbb{Z}(3,5,7)+\mathbb{Z}(0,2,1)$, it follows that $(N:F)=0$. Suppose that N is a prime submodule of F, i.e. the $\mathbb{Z}$-module F/N is torsion-free. Now $3(1,1,2)=(3,3,6)=(3,5,7)-(0,2,1)\in N$ gives that $(1,1,2)\in N$, i.e. $(1,1,2)=a(3,5,7)+b(0,2,1)$ for some $a,b\in\mathbb{Z}$ and hence $3a=1$, a contradiction. Thus N is not prime. □

We note the following general fact.

Proposition 3.7 *Let* R *be commutative ring, let* n *be a positive integer, let* $a_{ij}\in R$ $(1\leqslant i,j\leqslant n)$*, let* $\mathbf{a}_i=(a_{i1},\ldots,a_{in})\in F=R^{(n)}$ $(1\leqslant i\leqslant n)$ *and let* $N=R\mathbf{a}_1+\cdots+R\mathbf{a}_n$. *Let* A *denote the* $n\times n$ *matrix* (a_{ij}) *over* R. *Then*

$$R(detA)\subseteq(N:F)\subseteq\sqrt{R(\mathrm{det}A)}$$

Proof. Let B=adj$A$, the adjugate of the matrix A. Then $(\mathrm{det}A)I_n=BA$, where I_n denotes the $n\times n$ identity matrix over R. Suppose that B is the $n\times n$ matrix (b_{ij}) over R. Then

$$(\mathrm{det}A)\mathbf{e}_i=b_{i1}\mathbf{a}_1+\cdots+b_{in}\mathbf{a}_n\in N$$

for each $1\leqslant i\leqslant n$, where $\mathbf{e}_i$ is the i th row of the identity matrix. It follows that $(\mathrm{det}A)F\subseteq N$, i.e. $R(\mathrm{det}A)\subseteq(N:F)$.

Let $r\in(N:F)$. There exist elements $c_{ij}\in R$ $(1\leqslant i,j\leqslant n)$ such that $r\mathbf{e}_i=c_{i1}\mathbf{a}_1+\cdots+c_{in}\mathbf{a}_n$ for all $1\leqslant i\leqslant n$. Let C denote the $n\times n$ matrix (c_{ij}) over R. Then $rI_n=CA$. Taking determinants we have

$$r^n=\mathrm{det}(CA)=(\mathrm{det}C)(\mathrm{det}A)\in R(\mathrm{det}A).$$

It follows that $(N:F)\subseteq\sqrt{R(\mathrm{detA})}$. □

Corollary 3.8 *With the above notation, if R(detA) is a maximal ideal of R then N is a prime submodule of F.*

Proof. By Lemma 1.1 and Proposition 3.7. □

Next we consider what happens when $R(\det A)$ is a prime ideal of R. We have the following result.

Proposition 3.9 *With the notation of Proposition 3.7, let R be a domain and let $R(\det A)$ be a non-zero prime ideal of R. Then N is a prime submodule of F.*

Proof. Let $r \in R$, $x_i \in R$ $(1 \leqslant i \leqslant n)$ such that $r(x_1, \ldots, x_n) \in N$. Then

$$r(x_1, \ldots, x_n) = s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n$$

for some elements $s_i \in R$ $(1 \leqslant i \leqslant n)$. In matrix notation, we have

$$r[x_1 \cdots x_n] = [s_1 \cdots s_n]A.$$

Let $B = \operatorname{adj}A$. Then $r[x_1 \cdots x_n]B = [s_1 \cdots s_n]AB = d[s_1 \cdots s_n]$, where $d = \det A$. If $B = (b_{ij})$ then $r(x_1 b_{1j} + \cdots + x_n b_{nj}) = s_j d \in Rd$ for all $1 \leqslant j \leqslant n$. Since Rd is prime it follows that $r \in Rd$ and hence $rF \subseteq N$ by Proposition 3.7, or there exist $t_j \in R$ $(1 \leqslant j \leqslant n)$ such that $x_1 b_{1j} + \cdots + x_n b_{nj} = t_j d$ $(1 \leqslant j \leqslant n)$. In matrix terms, we have

$$[x_1 \cdots x_n]B = d[t_1 \cdots t_n]$$

and hence $[x_1 \cdots x_n]BA = d[t_1 \cdots t_n]A$ i.e. $d[x_1 \cdots x_n] = d[t_1 \cdots t_n]A$. Since R is a domain and $d \neq 0$ it follows that $[x_1 \cdots x_n] = [t_1 \cdots t_n]A$ and hence $(x_1, \ldots, x_n) = t_1\mathbf{a}_1 + \cdots + t_n\mathbf{a}_n \in N$. It follows that N is a prime submodule of F. □

Note that Example 3.5 shows that the converse of Proposition 3.9 is false in general, and Example 3.6 shows that in general Proposition 3.9 is false in case $\det A = 0$.

We now consider 2-generated submodules N of F of the form

$$N = R(a_1, \ldots, a_n) + R(b, \ldots, b),$$

where $b, a_i \in R$ $(1 \leqslant i \leqslant n)$. More generally, we shall consider when a submodule N of the form $R(a_1, \ldots, a_n) + I(1, \ldots, 1)$ is prime , where I is an ideal of R. First we prove a result which deals with the case $a_i = 0$ $(1 \leqslant i \leqslant n)$.

Lemma 3.10 *Let R be a commutative domain. Let I be an ideal of R. Then $I(1, \ldots, 1)$ is a prime submodule of $F = R^{(n)}$ (where $n \geqslant 2$) if and only if I=0 or I=R.*

Proof. Suppose that $I = 0$. Then $I(1, \ldots, 1) = 0$ and hence $I(1, \ldots, 1)$ is a 0-prime submodule of F. If $I = R$ then $I(1, \ldots, 1)$ is a 0-prime submodule of F since $F = I(1, \ldots, 1) \oplus G$, where $G = \{(x_1, x_2, \ldots, x_n) \in R^{(n)} : x_1 = 0\}$.

Conversely, suppose that $N = I(1, \ldots, 1)$ is a prime submodule of F. Now $I(1, \ldots, 1) \subseteq N$ implies that $R(1, \ldots, 1) \subseteq N$, so that $N = R(1, \ldots, 1)$ and hence $R = I$, or $IF \subseteq N$. Suppose that $IF \subseteq N$. Let $a \in I$. Then there exists $b \in I$ such that $a(1, 0, \ldots, 0) = b(1, \ldots, 1)$. Hence $a = b = 0$. It follows that $I = 0$. □

We now suppose that R is a commutative domain, $a_i \in R$ $(1 \leqslant i \leqslant n)$, not all zero, I is a non-zero ideal of R and $N = R(a_1, \ldots, a_n) + I(1, \ldots, 1)$.

Lemma 3.11 *Suppose that N is a prime submodule of $F = R^{(n)}$. Then either*

(i) I=R, or

(ii) $a_1 = \cdots = a_n$ and $R = Ra_1 + I$.

In any case, $N = R(a_1, \ldots, a_n) + R(1, \ldots, 1)$.

Proof. Note first that $I(1, \ldots, 1) \subseteq N$ gives that $IF \subseteq N$ or $(1, \ldots, 1) \in N$. Suppose first that $IF \subseteq N$. Let $0 \neq c \in I$. Then

$$(c, 0, \ldots, 0) = c(1, 0, \ldots, 0) = r(a_1, \ldots, a_n) + s(1, \ldots, 1)$$

for some $r \in R$, $s \in I$. Since $c \neq 0$ it follows that $r \neq 0$. Then $c = ra_1 + s$, $0 = ra_i + s$ $(2 \leqslant i \leqslant n)$, and hence $0 = r(a_2 - a_i)$, for all $2 \leqslant i \leqslant n$. It follows that $a_2 = a_3 = \cdots = a_n$. By considering $(0, c, 0, \ldots, 0) \in N$, we obtain $a_1 = a_2$. Thus $a_1 = a_2 = \cdots = a_n$. But we now have

$$(c, 0, \ldots, 0) = r(a_1, \ldots, a_1) + s(1, \ldots, 1),$$

which implies $c = 0$, a contradiction. Thus $IF \nsubseteq N$. Hence $(1, \ldots, 1) \in N$, and hence

$$(1, \ldots, 1) = x(a_1, \ldots, a_n) + y(1, \ldots, 1)$$

for some $x \in R, y \in I$. If $x = 0$ then $y = 1$ and hence $I = R$. Suppose that $x \neq 0$. Then $x(a_i - a_j) = 0$ $(1 \leqslant i < j \leqslant n)$ and hence $a_i = a_j$ $(1 \leqslant i < j \leqslant n)$. Moreover, $1 = xa_1 + y \in Ra_1 + I$. Thus $R = Ra_1 + I$.

If $I = R$ then clearly $N = R(a_1, \ldots, a_n) + R(1, \ldots, 1)$. Now suppose that $a_i = a_j$ $(1 \leqslant i < j \leqslant n)$ and $1 = xa_1 + y$ (as above). Then

$$(1, \ldots, 1) = x(a_1, \ldots, a_n) + y(1, \ldots, 1) \in N.$$

Thus $N = R(a_1, \ldots, a_n) + R(1, \ldots, 1)$. □

Theorem 3.12 *With the above notation, let R be a UFD. Then $N = R(a_1, \ldots, a_n) + I(1, \ldots, 1)$ is a prime submodule of F if and only if*

(a) I=R and every common divisor of the elements $a_i - a_1$ $(2 \leqslant i \leqslant n)$ is a unit in R, or

(b) $a_1 = \cdots = a_n$ and $R = Ra_1 + I$.

Proof. Suppose first that N is a prime submodule of F. By Lemma 3.11, $I = R$ or $a_1 = \cdots = a_n$ and $R = Ra_1 + I$. Suppose that $I = R$ then

$$N = R(a_1, \ldots, a_n) + R(1, \ldots, 1)$$

By Theorem 3.2, $a_1 = \cdots = a_n$ or every common divisor of $a_i - a_1$ $(2 \leqslant i \leqslant n)$ is a unit in R.

Conversely, if (b) holds then $N = R(1, \ldots, 1)$ and if (a) holds then $N = R(a_1, \ldots, a_n) + R(1, \ldots, 1)$ where any common factor of $a_i - a_1$ $(2 \leqslant i \leqslant n)$ is a unit. By Proposition 2.3 and Theorem 3.2, N is a prime submodule of F. □

References

[1] George, S.M., McCasland, R.L. and Smith, P.F.: A Principal Ideal Theorem analogue for modules over commutative rings, *Comm. Algebra* **22**(1994), 2083-2099.

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

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

[4] —— : Prime submodules, *Comm. Algebra* **20**(1992), 1803-1817.

[5] McCasland, R.L. and Smith, P.F.: Prime submodules of Noetherian modules, *Rocky Mtn. J.* **23**(1993), 1041-1062.

[6] Rotman, J.J.: *Notes on Homological Algebra*, Litton Educational Publishing 1970.

Dilek PUSAT-YILMAZ
Department of Mathematics,
Abant Izzet Baysal University,
14280 Bolu-TURKEY

Received 02.09.2002