YILDIZ TECHNICAL UNIVERSITY

Commutative Algebra

S-prime Submodules

Author:
Murat Rüzgar
POYRAZ

Supervisor
Dr. Eda YILDIZ
YILMAZ

May 19, 2026

1 Introduction

A module is similar to vector spaces but defined on rings.

Definition. *Let R be a ring and M an Abelian group. Define $f : R \times M \longrightarrow M$ satisfying the following conditions:*

- $f(s + r, m) = f(s, m) + f(r, m)$
- $f(r, m + m') = f(r, m) + f(r, m')$
- $f(r, f(s, m)) = f(rs, m)$
- $f(1_R, m) = m$

*M is called a **left R-module**. Here the operation f is called scalar multiplication and frequently denoted as $f(r, m) = r \cdot m$. If these conditions were satisfied by a multiplication on the right, like $m \cdot r$, we would call the set M a **right R-module**.*

If the multiplication is commutative, we simply say $R-$module. For the rest of this paper, R will be a commutative ring with unity. Mind that if R is a field, then M is a vector space in the definition.

For example, let $R = \mathbb{Z}$ and $M = \mathbb{Z} \times \mathbb{Z}$. Define the scalar multiplication as $n \cdot (k, m) = (nk, nm)$. M is a $R-$module. The polynomial ring $R[x]$ is a $R-$module. If $\phi : R \longrightarrow S$ is a ring homomorphism, define the scalar multiplication as $r \cdot m = \phi(r) \cdot m$. Then every S-module is an $R-$module.

Definition. *Let M be an $R-$module. Let M' be a subgroup of M. If $r \cdot m \in M'$ for every $m \in M'$ and $r \in R$, then M' is called a **submodule** of M.*

Let I be an ideal of R, then $I \times I$ is a submodule of $R \times R$.

Let $X \subseteq M$, then the set $\{\sum r_i m_i : r_i \in R,\ m_i \in X\}$ is called the submodule of M generated by X and is denoted as $\langle X \rangle$. We call the set X linearly independent if $r_i = 0$ for all, $r_i \in R$ whenever $\sum_{r_i \in R,\, m_i \in X} r_i \cdot m_i = 0$.

Lemma 1. *There is a maximal linearly independent set.*

Proof. If there are no such elements, the maximal independent set is $\emptyset$ itself. Let τ be a collection of all linearly independent sets. Take any chain of τ on the relation "$\subseteq$", say $\mu \subseteq \tau$. Since μ is a chain, every set in μ is included by each other. Thus, the set $\bigcup_{X \in \mu} X$ is linearly independent and is a supremum of μ. The result follows from Zorn's Lemma. $\square$

Lemma 2. *A finite maximal independent set of a vector space generates the space.*

Proof. Let V be an $\mathbb{F}-$module and X be a finite maximal linearly independent set. Suppose $V \neq 0$, so there are non-empty linearly independent sets. Take any $m \in V - X$. Then the set $X \cup \{m\}$ is linearly dependent by maximality of X. Thus, there are not all zero $r_i \in R$ and a non-zero $r \in \mathbb{F}$ such that

$$(\sum_{m_i \in X} r_i m_i) - rm = 0.$$

$$m = r^{-1} \sum_{m_i \in X} r_i m_i$$

Since m is arbitrary, the result follows. □

These results are fundamentals of modules. Unlikely to vector spaces, modules may not have a basis. For example, consider the quotient group $\mathbb{Q}/\mathbb{Z}$. This is a $\mathbb{Z}-$module. However, it does not have a linearly independent generator set. Even one point sets $\{\frac{a}{b}\}$ are not linearly independent since $b \cdot \frac{a}{b} = 0$. If a module has a basis, the module is said to be **freely generated**. For example, every vector space is a freely generated $F-$module where F is a field. If a module has at least one generator set with cardinality 1, that module is called **cyclic**. If $\langle m \rangle$ is an $R-$module, we can denote it as Rm.

Theorem 1. *Every finitely generated vector space is freely generated. Furthermore, each basis has a definite amount of elements.*

Proof. Let V be a vector space over a field $\mathbb{F}$ and suppose that $\langle X \rangle = V$ with $|X| = n$. If $n = 0$, then there is nothing to prove. Suppose that $n \neq 0$. Suppose that Y is a linearly independent set with $|Y| = k$. Write $X = \{v_1, ..., v_n\}$ and $Y = \{u_1, ..., u_k\}$. Since X is a generator set, there are $a_1, ..., a_n \in \mathbb{F}$ such that:

$$u_1 = a_1 v_1 + ... + a_n v_n.$$

Here, we can assume that $u_1 \neq \mathbf{0}$. So, at least one of a_i's is non-zero. Without loss of generality, assume $a_1 \neq 0$. So write $v_1 = a_1^{-1}(u_1 - a_2 v_2 - ... a_n v_n)$. This yield $\{u_1, v_2, ..., v_n\}$ is a generator set. Continuing the pattern yields $\{u_1, ..., u_k, v_{k+1}, ..., v_n\}$ is a generator set. So we have $n \geq k$. Suppose A and B are both linearly independent and generator sets. Then $|A| \geq |B|$ since A

is a generator set and B is a linearly independent set. Similarly, $|B| \geq |A|$. So, $|A| = |B|$ and we conclude that V has a basis.

□

Another Proof. Let X be a minimal generator set. Then we claim that X is linearly independent. Suppose not; then $a_1v_1 + ... + a_nv_n = 0$ has a non-zero solution. Suppose $a_i \neq 0$. Then we can write:

$$v_i = a_i^{-1}(-a_1v_1 - a_{i-1}v_{i-1} - a_{i+1}v_{i+1} - ... - a_nv_n).$$

So the set $X - \{v_i\}$ still generates V which is a contradiction with minimality. The set X also is a maximal linearly independent set. By Lemma 2, the converse is true. If Y is a maximal linearly independent set, then it is a generator set. What if X were a both linearly independent set and generator set? Then $X - v$ would not be a generator set since X is still linearly independent and $v \notin \langle X - \{v\} \rangle$. So X is the minimal generator set. If $X \cup u$ for some $u \in V - X$, then $u = a_1v_1 + ... + a_nv_n$ for some non-zero $a_i \in \mathbb{F}$. Thus, X is linearly dependent and we conclude that X is a maximal linearly independent set.

Let A and B be both linearly independent and generator subsets of V. Assume that $|A| = n, |B| = m$. If $|A| > |B|$, then the set $A_{|B}\{u_1, .., u_m, v_{m+1}, ..., v_n\}$ would be a generator set where $u_i \in B$ and $v_j \in A$ for the corresponding i's and j's. The usual calculations of linear algebra show that the set $A_{|B}$ is linearly independent, which contradicts the maximality of B. So we must have $|A| \leq |B|$. However, the statement is symmetrical, so we have $|B| \leq |A|$. This yields $|A| = |B|$. □

Indeed, Theorem 1 is true for every vector space; however, this is beyond the scope of this paper.

A Counter Example Lemma 2 is not true for modules in general. Take $M = R = \mathbb{Z}$ in the module definition. The scalar multiplication of M will be the multiplication of R itself. So the set $\{2\}$ is a maximal linearly independent set. To see this, consider $\{2, m\}$ for any non-zero integer m:

$$2a + bm = 0$$

has a non-zero solution $a = m$ and $b = -2$. Therefore, the set $\{2, m\}$ is linearly dependent. Thus, the set $\{2\}$ must be maximal linearly independent. Because it is clear that $2a = 0$ if and only if $a = 0$. However, the set $\{2\}$ does not generate $\mathbb{Z}$.

2 Colon Submodules

Let M be an $R-$module and K, L be submodules of M and I be an ideal of R.

$$(K :_R L) := \{r \in R : \ r \cdot m \in K, \, \forall m \in L\}$$

$$(K :_M I) := \{m \in M : \ r \cdot m \in K, \, \forall r \in I\}$$

Check that whether these sets ideal of R, submodules of M or neither of them. It is easy to see that $1 \in (K :_M L)$ since $1 \cdot m = m \in K$ for every $m \in K$. Take $a, r \in (K :_M L)$. Then $a \cdot m \in K$ and $r \cdot m \in K$ by definition, but, $(a+r) \cdot m = a \cdot m + r \cdot m \in K$. Now, suppose that $r \in (K :_M L)$ and take any $b \in R$. So, br is an element of R. Since $r \cdot m \in K$, then $(br) \cdot m = b \cdot (r \cdot m)$ is also in K. Thus, $(br) \in (K :_M L)$. This proves that $(K :_M L)$ is an ideal of R.

What if the set $(K :_M I)$? Is it a submodule of M? Firstly, observe that $0_M \in (K :_M I)$. So, if $a, b \in (K :_M I)$, then $(a - b) \cdot r = (a \cdot r - b \cdot r) \in K$ for any $r \in I$ since $a \cdot r$, $b \cdot r \in K$ and K is a submodule. Hence, $(K :_M I)$ is a subgroup of M. Furthermore, if $m \in (K :_M I)$ and if $r \in R$ any element, then $ri \in I$ for every $i \in I$, and $(ri) \cdot m \in (K :_M I)$ by definition. Thus, $i \cdot (r \cdot m) \in K$ for every $i \in I$. Therefore, $r \cdot m \in (K :_M I)$. This yields to that $(K :_M I)$ is a submodule of M.

Here are some useful notations:

- $(0 :_R M) = ann(M)$ (called annihilator)
- $(P :_M Rs) = (P :_M s)$
- $(0 :_M Rm) = ann(m)$ (also called annihilator)
- We will use $(K : L)$ instead of $(K :_M L)$ if M is clear from context.
- A module is called $S-$torsion-free if $ann(M) \cap S = \emptyset$ and $am = 0$ implies $sa = 0$ or $sm = 0$ for an $s \in S$.
- If $0 = \{m \in M : ann_R(m) \neq 0\}$, we say that M is a torsion-free module. This means that if $am = 0$, then $ann(m) = 0$ (so $a = 0$) or $m = 0$.

3 S-prime Submodules

From now on, R will be a commutative ring with identity and M will be an $R-$module. Let S be a multiplicative subset of R. An $S-$prime ideal of R is an ideal P satisfying if $ab \in P$ then $sa \in P$ or $sb \in P$ for any $s \in S$ when $S \cap P = \emptyset$. If it were $S \cap P \neq \emptyset$, it would be trivial for any couple $a, b \in R$ and $s \in S \cap P$, $sa \in P$ or $sb \in P$ since P is an ideal and $s \in P$. Thus, the case $S \cap P = \emptyset$ is important. There are some relations between colon ideal $(P : s)$ and being $S-$prime. From Proposition 1 in [1], $(P : s)$ is prime for some $s \in S$ if and only if P is $S-$prime. This is the motivation of our colon submodule definition from the previous section.

Definition. *A submodule K of M with $(K : M) \cap S = \emptyset$ is called $S-$**prime** if $sr \in (K : M)$ or $sm \in K$ whenever $rm \in K$.*

Removing the condition $(K : M) \cap S = \emptyset$ would make a difference since if $rm \in K$, then $sr \in (K : M)$ is trivial since $(K : M)$ is an ideal of R and $sm \in K$ is trivial since K is a submodule of M. If S consists of units of R, then K is called a **prime submodule**.

Lemma 3. *Let K be a prime submodule of M. Then $(K : M)$ is a prime ideal of R.*

Proof. Let $ab \in (K : M)$. Then $(ab)m \in K$ for every $m \in M$. Suppose that $am \notin K$. We have that $b(am) \in K$, since K is prime, then $b \in (K : M)$ or $am \in K$. Since $am \notin K$, then we must have $b \in (K : M)$, completing the proof. □

Consider the R as $R-$module. Then every $S-$prime ideal is an $S-$prime submodule of R. Similarly, every prime ideal is a prime submodule of R. This is a particular example for $S-$prime submodules.

After all these, one may wonder if Lemma 3 is valid for $S-$prime submodules. Take $ab \in (K : M)$. Then $(ab)m \in K$ for every $m \in M$. Since $sm \in M$ for an $s \in S$, we can say that $s(ab)m = (ab)(sm) \in M$. Suppose that $sa \notin (K : M)$. Since K is $S-$prime, then $sb \in (K : M)$ or $sam \in K$. Since $sam \notin K$, $sb \in (K : M)$. This proves that $(K : M)$ is an $S-$prime ideal of R.

Corollary: If K is an $S-$prime submodule of M, then $(K : M)$ is an $S-$prime ideal of R.

Lemma 4. *Let $S_1 \subseteq S_2$ multiplicative sets and K be a S_1-prime submodule of M. If $(K : M) \cap S_2 = \emptyset$, then K is also S_2-prime submodule.*

Proof. This is obvious since if $rm \in K$, then $sr \in (K : M)$ or $sm \in K$ for some $s \in S_1 \subseteq S_2$. $\square$

Definition. *The set*

$$S^* = \{x \in R : \frac{x}{1} \text{ is a unit of } S^{-1}R\}$$

is called saturation of S.

We will use the fact that $S \subseteq S^*$ which is a clear conclusion since $\frac{s}{s}$ is a unit of $S^{-1}R$ for every $s \in S$.

Lemma 5. *P is an $S-$prime submodule of M if and only if P is an S^*-prime submodule.*

Proof. ($\Rightarrow$) Firstly, we shall see that $(P : M) \cap S = \emptyset$ if and only if $(P : M) \cap S^* = \emptyset$. If $rm \in P$ for some $r \in S^*$, then $(\frac{s}{r}r)m \in M$ for some $s \in S$. Then, $sm \in P$ which asserts

$$(P : M) \cap S = \emptyset \Rightarrow (P : M) \cap S^* = \emptyset$$

by contraction. Converse is obvious. Now, by Lemma 4, half of the proof is done.

($\Leftarrow$) Take $rm \in P$. Since P is S^*-prime, we have $pr \in (P : M)$ or $pm \in P$ for some $p \in S^*$. If $pr \in (P : M)$, since p is a unit in $S^{-1}R$, $pa = s$ for some $s \in S$ and $a \in R$. Recall that $\frac{p}{1}\frac{a}{s} = 1$. Now, $sr \in (P : M)$ since $(P : M)$ is an ideal of R and $sr = par \in (P : M)$. If $pm \in P$, then again $sm \in P$ since $sm = par \in P$ and P is a submodule. $\square$

Lemma 6. *If P is a $S-$prime submodule of M, then $S^{-1}P$ is a prime submodule of $S^{-1}M$.*

Proof. Take $\frac{p}{s}m \in S^{-1}P$ for some $s \in S$ and $p \in R$. This yields to that $pm \in P$ since $pm = \frac{p}{s}\frac{s}{1}m \in S^{-1}P$. Since P is $S-$prime, $s'p \in (P : M)$ or $s'm \in P$ for some $s' \in S$. Thus, $\frac{s'p}{1} \in (S^{-1}P : S^{-1}M)$ or $\frac{s'}{1}m \in S^{-1}P$. Since $(S^{-1}P : S^{-1}M)$ is an ideal of $S^{-1}R$ and $S^{-1}P$ is a submodule of $S^{-1}M$, we have $\frac{s'}{ss'}p = \frac{p}{s} \in (S^{-1}P : S^{-1}M)$ or $\frac{s'}{ss'}pm = \frac{p}{s}m \in S^{-1}P$. Hence, we are done. $\square$

Lemma 7. *P is an $S-$prime submodule of M if and only if there is an $s \in S$ and $IN \subseteq P$ implies $sI \subseteq (P : M)$ or $sN \subseteq P$ for each ideal I of R and submodule N of M.*

Proof. ($\Rightarrow$) Let $IN \subseteq P$. Take any $jm \in IN$ where $j \in I$ and $m \in N$. Since P is S-prime and $jm \in P$, then $sj \in (P : M)$ or $sm \in P$ for some $s \in S$. This implies that $sI \subseteq (P : M)$ since j is arbitrary and $sN \subseteq P$ since m is arbitrary.

($\Leftarrow$) Let $rm \in P$. Take $r \in \langle r \rangle = I$ and $m \in \langle m \rangle = N$. If $r' \in I$ and $m' \in N$, then $r'm' = (ra)(bm) = (ab)(rm) \in P$ for some $a, b \in R$. Thus, $IN \subseteq P$. By assumption, $sI \in (P : M)$ or $sN \subseteq P$ for some $s \in S$. It yields to that $sr \in (P : M)$ or $sm \in P$. □

Corollary: Take R as an $R-$module where the scalar multiplication is the ring multiplication itself. Then P is an $S-$prime ideal of R if and only if $IJ \subseteq P$ implies $sI \subseteq P$ or $sJ \subseteq P$ for each ideal I, J of R.

Lemma 8. *Let M, M' be $R-$modules, and let $f : M \to M'$ be a module homomorphism. Then:*

1. *If P is an $S-$prime submodule of M' with $(f^{-1}(P) : M) \cap S = \emptyset$, then $f^{-1}(P)$ is an $S-$prime submodule of M.*
2. *If f is onto and P is an $S-$prime submodule of M with $ker(f) \subseteq P$ then $f(P)$ is an $S-$prime submodule of M'.*

Proof.

1. Let P be an $S-$prime submodule of M' with $(f^{-1}(P) : M) \cap S = \emptyset$. Take $rm \in f^{-1}(P)$. Then $rf(m) \in P$. Since P is $S-$prime, we have $sr \in (P : M')$ or $sf(m) \in P$. If $sf(m) \in P$ then $f(sm) \in P$, so $sm \in f^{-1}(P)$ and we are done. If not, we need to show that $sr \in (f^{-1}(P) : M)$. Take any $m \in M$. Then we have $(sr)f(m) \in P$, so $f(srm) \in P$ and $srm \in f^{-1}(P)$, thus $sr \in (f^{-1}(P) : M)$. This is not only showing us that $sr \in (f^{-1}(P) : M)$, it also proves that $(P : M') \subseteq (f^{-1}(P) : M)$.
2. Let f be onto and P is an $S-$prime submodule of M with $ker(f) \subseteq P$. Suppose that $rm' \in f(P)$. Then there is an $m \in M$ such that $f(m) = m'$ since f is onto. So, $rf(m) \in f(P)$ which results by $rm \in P$. Since P is $S-$prime, $sr \in (P : M)$ or $sm \in P$. If $sm \in P$, then $sf(m) =$

$sm' \in P$ and we are done. If not, take any $n \in M'$ and suppose that $(sr)n \in f(P)$. By the first isomorphism theorem, $M/ker(f) \cong M'$. Thus, there is an isomorphism ϕ such that $\phi(P + ker(f)) = \phi(P) = f(P)$. Thus, $(sr)\phi(f^{-1}(n) + ker(f)) = \phi(f^{-1}(srn) + ker(f)) \subseteq f(P)$. Since n is arbitrary, we are done by Lemma 7. This does not only show that $sr \in (f(P) : M')$, it also shows that $(P : M) \subseteq (f(P) : M')$ so that $(P : M) = (f(P) : M')$ by the previous part of proof, hence $(f(P) : M') \cap S = (P : M) \cap S = \emptyset$ in this case.

□

Corollary: Let P be a submodule of M with $L \subseteq P$ where L is also a submodule of M. P is $S-$prime submodule of M if and only if P/L is an $S-$prime submodule of M/L.

One may wonder whether the converse of the corollary of Lemma 3 is true. The next lemma asserts a condition for this. Before that, we need a definition.

Definition. *A multiplication module is a module M, for every submodule N of M there is an ideal I of R such that $N = IM$.*

Lemma 9. *If M is a multiplication module and the ideal $(P : M)$ is $S-$prime, then P is an $S-$prime submodule of M.*

Proof. Let N be a submodule of M and I be an ideal of R such that $IN \subseteq P$. Then we conclude that $J(N : M) \subseteq (JN : M) \subseteq (P : M)$. Since $(P : M)$ is $S-$prime, there is an $s \in S$ so that $sJ \subseteq (P : M)$ or $s(N : M) \subseteq (P : M)$. Hence, $sJ \subseteq (P : M)$ or $sN \subseteq s(N : M)M \subseteq s(P : M)M = P$. We are done by Lemma 7. □

In the proof, the existence of $IN \subseteq P$ comes from the fact that M is a multiplication module. By Lemma 3 and Lemma 9, we conclude that P is $S-$prime submodule of M if and only if $(P : M)$ is an $S-$prime ideal of R whenever M is a multiplication module.

Theorem 2. *Let M be a finitely generated multiplication R-module and P a submodule of M. Let S be a multiplicative set with $(P : M) \cap S = \emptyset$. The following statements are equivalent:*

1. *P is an $S-$prime submodule of M*

2. $(P : M)$ *is an* $S-$*prime ideal of* R

3. $P = IM$ *for some ideal* I *with* $ann(M) \subseteq I$.

Proof. $(1 \Rightarrow 2)$ is proven in Lemma 9.

$(2 \Rightarrow 3)$ Take $f = Id_M$ in Lemma 8. Then $f(P) = f(IM) = If(M) = IM = P$ is an $S-$prime submodule of M, clearly.

$(3 \Rightarrow 1)$ Let $P = IM$ for some ideal I with $ann(M) \subseteq I$. Assume that $JN \subseteq P$ for some ideal J and submodule N. Then $J(N : M)M \subseteq IM$. We need another theorem at this point.

Theorem 3. *Let* A, B *ideals of* R. $AM \subseteq BM$ *is valid if and only if* $A \subseteq B + ann(M)$ *or* $M = ((B + ann(M)) : A)M$.

Proof. For the main theorem, it is sufficient to prove it one way. Suppose $AM \subseteq BM$. If $ann(M) = 0$ and $A \subsetneq B$, note that

$$(B : A) = \bigcap_{a \in A-B} (B : Ra)$$

Then, $(B : A)M = \bigcap_{a \in A-B}(B : Ra)M$. Let $a \in A-B$ and let $C = (B : Ra)$. Let S be the intersection of all prime ideals that is containing C. Suppose that $M \neq PM$ for such a P. Then there is an $x \in M - PM$. $Rx = DM$ for some ideal D since M is a multiplication module. We know $x \notin P$, so $D \subsetneq P$. Then $cM \subseteq Rx$ for some $c \in R$ with $c \notin P$. Now,

$$caM \subseteq cAM \subseteq cBM = BcM \subseteq Bx$$

implies that $cax = bx$ for some $b \in B$. It follows that $(ca-b)x = 0$ and hence $c(ca - b)M = 0$. But, $ann(M) = 0$, so that $c^2a = cb \in B$. So, $c^2 \in C \subseteq P$ but since P is prime, $c \in P$ and this is a contradiction. Thus, $M = PM$ for each prime ideal such that $C \subseteq P$. Now, $M = \bigcap PM = (\bigcap P)M = SM$ Let $m \in M$. There exists an ideal I of R such that $Rm = IM$ and hence $Rm = Sm$. Then there exists some $s \in S$ such that $m = sm = s^n m$ for every positive integer n and hence $m \in CM$. It follows that $M = CM$. Now, let $ann(M)$ to be any ring. Let $R' = R/ann(M)$. Now, M has an annihilator 0 as an $R'-$module. So the theorem follows from the result above. □

Here, since M is finitely generated, we have $J(N : M) \subseteq I + ann(M) = I$. As I is $S-$prime, there is an $s \in S$ such that $sJ \subseteq I \subseteq (P : M)$ or $s(N : M) \subseteq I \subseteq (P : M)$ and hence $sJ \subseteq (P : M)$ or $sN \subseteq P$. □

Lemma 10. *Let* $R = R_1 \times R_2$ *where* R_1, R_2 *are commutative rings with identity and* $S = S_1 \times S_2$ *where* S_1, S_2 *are multiplicatively closed subsets of* R_1 *and* R_2*, respectively. The ideal* $P = P_1 \times P_2$ *is* $S-$*prime if and only if* P_1 *is* S_1-*prime ideal of* R_1 *and* $P_2 \cap S_2 \neq \emptyset$ *or* P_2 *is* S_2-*prime ideal of* R_2 *with* $P_1 \cap S_1 \neq \emptyset$.

Proof. Suppose P is $S-$prime. Since $(0, 0) = (1, 0)(0, 1)$ in P, there exists (s_1, s_2) such that $(s_1, 0) \in P$ or $(0, s_2) \in P$. Let $(0, s_2) \in P$. So, $P_2 \cap S_2 \neq \emptyset$. Let $ab \in P_1$ and take $(ab, 0) \in P_1 \times P_2$. Then there is an $s = (s_1, s_2) \in S$ such that $s(a, 0) \in P_1 \times P_2$ or $s(b, 0) \in P_1 \times P_2$. This yields to that $s_1a \in P_1$ or $s_1b \in P_1$. This proves that P_1 is $S-$prime. The proof for P_2 is the same.

Conversely, suppose that P_1 is S_1-prime and $P_2 \cap S_2 \neq \emptyset$. Take $(a, b)(c, d) \in P_1 \times P_2$ and $s_2 \in S_2 \cap P$. This yields to $ac \in P$ Then there is an $s_1 \in S_1$ such that $as_1 \in P_1$ or $cs_1 \in P_1$. Now take $s = (s_1, s_2)$ and this proves the lemma. □

The proof of Lemma 10 is similar for modules. So, we can conclude that a module $P_1 \times P_2$ is a $S-$prime submodule of $M_1 \times M_2$ if and only if P_1 is S_1-prime and $(P_2 : M_2) \cap S_2 \neq \emptyset$ or the converse. By induction, we can generalize this corollary for n cases: $P_1 \times ... \times P_n$ is $S_1 \times ... \times S_n$ prime ideals of $R_1 \times ... \times R_n-$module $M_1 \times ... \times M_n$ if and only if there is an integer i such that P_i is S_i-prime and $(P_j : M_j) \cap S_j \neq \emptyset$ for $j \in \{1, ..., n\} - \{i\}$.

Lemma 11. *Let* P *be an* $S-$*prime submodule of* M*. Then the following statements hold for some* $s \in S$*:*

1. $(P : s') \subseteq (P : s)$ *for every* $s' \in S$
2. $((P : M) : s') \subseteq ((P : M) : s)$ *for all* $s' \in S$.

Proof.

1. Suppose P is $S-$prime. Take $x \in (P : s')$. Then $xs' \in P$. This implies $ss' \in (P : M)$ or $sx \in P$. $ss' \notin (P : M)$ since $S \cap (P : M) = \emptyset$, so $x \in (P : s)$.
2. This is the direct corollary of 1.

□

Next theorem gives the converse statement to Lemma 6.

Lemma 12. *Let M be a finitely generated $R-$module and P be a submodule of M with $(P:M)\cap S=\emptyset$ for a multiplicative set S of R. P is $S-$prime if and only if $S^{-1}P$ is a prime submodule of $S^{-1}M$ and there is an $s\in S$ such that $(P:s')\subseteq (P:s)$ for all $s'\in S$.*

Proof. $(\Rightarrow)$ This way is proven in Lemma 6. So we need to prove $(\Leftarrow)$ way. Take $rm\in P$. So $\frac{r}{1}\frac{m}{1}\in S^{-1}P$. Since $S^{-1}P$ is prime, we have $\frac{r}{1}\in (S^{-1}P:S^{-1}M)=S^{-1}(P:M)$ or $m\in S^{-1}P$. Then there are $a,b\in S$ so that $ar\in (P:M)$ or $bm\in P$. By assumption there is an $s\in S$ such that $rM\in (P:a)\subseteq (P:s)$, so $sr\in (P:M)$ or $bm\in (P:b)\subseteq (P:s)$ thus $sm\in P$. $\square$

Theorem 4. *Suppose that P is a submodule of M with $(P:M)\cap S=\emptyset$. P is $S-$prime if and only if $(P:s)$ is a prime submodule of M for some $s\in S$.*

Proof. Assume that $(P:s)$ is prime for some $s\in S$. Let $rm\in P$. Then $rm\in (P:s)$, clearly. Thus, $r\in ((P:s):M)=((P:M):s)$ or $m\in (P:s)$. Thus, $sm\in P$ or $rs\in (P:M)$.

Conversely, suppose that P is $S-$prime. Then there is an $s\in S$ so that $rm\in P$ implies $sr\in (P:M)$ or $sm\in P$. Take $pm\in (P:s)$. Then $spm\in P$. Therefore, we can say that $s^2p\in (P:M)$ or $sm\in P$. If $sm\in P$, then $m\in (P:s)$ so we are done. If not, suppose $s^2p\in (P:M)$. So $p\in ((P:M):s^2)\subseteq ((P:M):s)$ by the second case of Lemma 11. Hence, $p\in ((P:s):M)$ and we are done. $\square$

From now on, $J(R)$ will denote the Jacobson Ideal, which is the intersection of every maximal ideal of R. $Max(R)$ will be the set consists of maximal ideals of R. In a way, $J(R)=\bigcap_{I\in Max(R)} I$. There is a quick observation; take any $I\in Max(R)$. Then $R-I$ is a multiplicative set. $1\notin I$ since I is maximal, so it must be $1\in R-I$. Let $a,b\in R-I$. Then $ab\notin I$ since $ab\in I$ implies $a\in I$ or $b\in I$. We used the fact that every maximal ideal is a prime ideal in a commutative ring with identity. Lastly, we have $0\notin R-I$ since $0\in I$. Therefore, $R-I$ is a multiplicative set. So, we can put $S=R-I$ and examine whether a submodule P is $S-$prime or not. Here is the lemma.

Lemma 13. *Let P be a submodule of M and $I\in Max(R)$. Let $S=R-I$ and suppose that $(P:M)\subseteq J(R)$. P is a prime submodule if and only if*

$(P : M)$ is a prime ideal of R and P is an $S-$prime submodule of M for every such $I \in Max(R)$ and corresponding S.

Proof. ($\Rightarrow$) If P is prime, then $(P : M)$ is a prime ideal by Lemma 3. Now, since $(P : M) \subseteq J(R) \subseteq I$ for every $I \in Max(R)$, we conclude that $(P : M) \cap (R - I) = \emptyset$. Hence, we are done for this way.

($\Leftarrow$) Suppose that $(P : M)$ is prime and P is $(R - I)-$prime for every maximal ideal I. Let $rm \in P$ with $r \notin (P : M)$. There is an $s \in R - I$ so that $sr \in (P : M)$ or $sm \in P$ by assumption. Since $(P : M)$ is a prime ideal of R, we get that $s \in (P : M)$ or $r \in (P : M)$. Both cases lead to a contradiction. So we must have $sm \in P$. Consider the set $X = \{s \in R : \exists I \in Max(R),\ s \notin I\ sm \in P\}$. Let $\langle X \rangle \subseteq K$ be a maximal ideal. There exists $s' \in X$ such that $s' \notin K$. This is a clear contradiction. Thus, $\langle X \rangle$ cannot be contained in a maximal ideal or be a maximal ideal itself. Thus, $\langle X \rangle = R$. This yields $1 \in \langle X \rangle$, so we have

$$1 = \sum_{s_i \in S} r_i s_i$$

for some $r_i \in R$ and $s_i \in S$ with $s_i \notin M_i \in Max(R)$ and $s_i m \in P$. Therefore,

$$m = \sum_{s_i \in S} m r_i s_i \in P.$$

Therefore, P is prime. $\square$

If R is a quasilocal ring, then there is only one maximal ideal; name it I. Then we can rewrite Lemma 13 as P is prime if and only if $(P : M)$ is prime and P is $(R - I)$-prime.

Definition. *The idealization $R(+)M = R \times M$ where the multiplication is defined as $(r, m)(p, n) = (rp, rn + pm)$ and the addition as $(r, m) + (p, n) = (r + p, m + n)$.*

$R(+)M$ is a commutative ring with the identity $(1_R, 0_M)$. If $S \subseteq R$ is a multiplicative set and P is a submodule of M, then $S(+)P$ is a multiplicative set.

Lemma 14. *Let S be a multiplicative set of R and P be an ideal of R with $P \cap S = \emptyset$. The following are equivalent:*

1. *P is an $S-$prime ideal of R*

2. *$P(+)M$ is an $S(+)0-$prime ideal of $R(+)M$*

3. *$P(+)M$ is an $S(+)M-$prime ideal of $R(+)M$.*

Proof. (1⇒2) Let P be $S-$prime and suppose that $(a,0)(b,0) \in P(+)0$. This yields $(ab,0) \in P(+)0$, thus it must be $ab \in P$. For an $s \in S$, we have $sa \in P$ or $sb \in P$, therefore we conclude that $(s,0)(a,0) \in P(+)M$ or $(s,0)(b,0) \in P(+)M$.

(2⇒3) Follows from Lemma 4.

(3⇒1) Suppose that $P(+)M$ is $S(+)M-$prime and let $ab \in P$. Then $(a,0)(b,0) \in P(+)M$. By assumption, there is an (s,m) so that $(s,m)(a,0) \in P(+)M$ or $(s,m)(b,0) \in P(+)M$. Thus, we have $(sa,ma) \in P(+)M$ or $(sb,bm) \in P(+)M$. Hence, $sa \in P$ or $sb \in P$. □

4 Noetherian and $S-$Noetherian Modules

A Noetherian ring is a ring where the ascending chain condition holds. So we call R Noetherian if $I_1 \subseteq I_2 \subseteq ...$ is a chain of ideals; then there is a maximal ideal of this chain. Here is a useful theorem to identify Noetherian rings.

Theorem 5. *R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. Let R be Noetherian. Let $I = \{a_1, a_2, ...\}$ be an ideal. Then $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq ...$ is a chain of ideals. By assumption, this chain stops at some point. In other words, there is $n \in N$ so that $\langle a_1, a_2, ..., a_n \rangle$ is the maximal element of the chain. However, let $b \in I - \langle a_1, a_2, ..., a_n \rangle$. If such b existed, then $\langle a_1, a_2, ..., a_n, b \rangle$ would be larger in the chain, so that would be a contradiction with maximality. So $I = \langle a_1, a_2, ..., a_n \rangle$. Thus, I is finitely generated.

Conversely, suppose that there is an ideal J is infinitely generated. Let $J = \langle a_1, a_2, ... \rangle$. Then $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle ...$ is an infinite chain with no maximal element so R is not Noetherian. Proof is done by contraction. $\square$

In Noetherian rings, every ideal is contained in a finitely generated set by Theorem 4. We can generalize this definition by $S-$finiteness. We call an ideal is $S-$finite if there is a finitely generated ideal J of R and an $s \in S$ such that $sI \subseteq J \subseteq I$. We call R is $S-$Noetherian if every ideal of R is $S-$finite. As modules, we call a module is $S-$Noetherian if every submodule is $S-$finite, so if P is a submodule of M, then there is $s \in S$ and finitely generated submodule K so that $sP \subseteq K \subseteq P$.

Lemma 15. *Let M be an $S-$finite $R-$module. Then M is $S-$Noetherian if and only if the submodules of the form PM are $S-$finite for each prime ideal P of R with $P \cap S = \emptyset$.*

Proof. ($\Rightarrow$) This way comes from the definition. We shall prove ($\Leftarrow$) this way. Let PM be $S-$finite for each prime ideal P of R with $P \cap S = \emptyset$. As M is $S-$finite, $sM \subseteq L$ for some finitely generated submodule L. Suppose that M is not $S-$Noetherian. Consider non-$S-$finite submodules of M. For every chain of non-$S-$finite submodules, the union of the chain is also non-$S-$finite. So every chain has a supremum under inclusion; thus, there is a maximal non-$S-$finite ideal N of M by Zorn's Lemma. Put $P = (N : M)$.

This is a prime ideal by Lemma 3 of [2]. If $P \cap S$ had at least one element u, then we would have $usN \subseteq uL \subseteq N$ which is a contradiction by non-$S-$-finiteness. Therefore, $P \cap S = \emptyset$. Then $P = (N : M) \subseteq (N : L) \subseteq (N : sM) = (P : s) = P$, hence $P = (N : L)$. Let $L = \langle m_1, ...m_k \rangle$. Then $P = (N : m_1) \cap ... \cap (N : m_k)$. $P = (N : m_i)$ for some i since P is prime. $m_i \notin N$ since $P = (N : m_i) \neq N$. By maximality of N, $N + Rm_i$ is $S-$finite. So, $t(N + Rm_i) \subseteq \langle n_1 + a_1 m_i, ..., n_l + a_l m_i \rangle$ for some $t \in S$, $n_1, ..., n_l \in N$ and $a_1, ...a_l \in R$. It follows that $tN \subseteq K + Pm_i \subseteq K + PM$ where $K = \langle n_1, ..., n_l \rangle$. As PM is $S-$finite, so $vtN \subseteq K + vPM \subseteq N$ for some $v \in S$. This is a contradiction of non-$S-$finiteness of N. $\square$

5 Torsion-Free and $S-$Torsion-Free Modules

Definitions are given in Section 2. Remind that a canonical homomorphism is a homomorphism $\pi : R \longrightarrow R/I$ by the rule $\pi(a) = a + I$ for an ideal I of R. Multiplication and addition are well-defined in quotient rings, so one may put $a + I = \overline{a}$. We will use the fact that $a - b \in I$ if and only if $a + I = b + I$, or equivalently, $\overline{a} = \overline{b}$ if and only if $a - b \in I$. In the following proof, we will take $b = 0$ without noticing.

Lemma 16. *Let P be a submodule of M and S be a multiplicative set. Then P is $S-$prime if and only if the quotient module M/P is a $\pi(S)-$torsion-free $R/(P : M)-$module.*

Remember that R/I is an integral domain if and only if I is a prime ideal of R. This can be seen as a generalized statement.

Proof. ($\Rightarrow$) Let $\overline{rm} = \overline{0}$. Thus, we must have $rm - 0 = rm \in P$. Then there is an $s \in S$ so that $rs \in (P : M)$ or $sm \in P$. If $sm \in P$, this yields to that $\overline{sm} = \overline{0}$. Suppose that $sm \notin P$. Then we must have $rs \in (P : M)$, so $\overline{rs} = \overline{0}$ in $R/(P : M)$. Therefore, M/P is $\pi(S)-$torsion-free.

Conversely, suppose that M/P is $\pi(S)-$torsion-free. Let $rm \in P$. Then we must have $rm - 0 \in P$ so that $\overline{rm} = \overline{0}$. Since M/P is $\pi(S)-$torsion-free, then there is an $s \in S$ such that $\overline{sr} = \overline{0}$ in $R/(P : M)$ or $\overline{sm} = \overline{0}$ in M/P. This yields to that $sr \in (P : M)$ or $sm \in P$. □

Corollary: Take $R = M$ and S be set of all units of R. We conclude that I is prime if and only if R/I is an integral domain.

Theorem 6. *Let R be an integral domain and M be an $R-$module. The following are equivalent:*

1. *M is a torsion-free module.*
2. *M is an $(R - P)$-torsion-free module for each prime ideal P.*
3. *M is an $(R - L)$-torsion-free module for each maximal ideal L.*

Proof. ($1 \Rightarrow 2$) This is clear; just choose $s = 1$.

($2 \Rightarrow 3$) This is also clear since every maximal ideal is a prime ideal.

($3 \Rightarrow 1$) Let $rm = 0_M$ for some $r \neq 0_R$. Take any maximal ideal J of R. Then there exists $s \in R - J$ such that $sr = 0_R$ or $sm = 0_M$. Note that $s \notin J$. Put $X = \{s_m \in R : \exists I \in Max(I),\ s_m \notin I,\ s_m m = 0\}$. As we did in Lemma 13, $\langle X \rangle = R$. So, we have $s_{m_1}, ..., s_{m_k}$ such that $r_1 s_{m_1} + ... + r_k s_{m_k} = 1_R$ for some $r_1, ..., r_k \in R$. We conclude that $m = r_1 m s_{m_1} + ... + r_k m s_{m_k} = 0_M$. This means that M is torsion-free. □

We call M is simple if only submodules of M are M and 0. Here is the next theorem of characterization of simple modules in terms of $S-$prime submodules.

Theorem 7. *Let M be a finitely generated $R-$module and $S \subseteq R$ be a multiplicative set with $ann(M) \cap S = \emptyset$. Then each proper submodule is $S-$prime if and only if M is a simple module.*

Proof. ($\Rightarrow$) Suppose each proper submodule is $S-$prime. Let a be a zero-divisor of M. So there is $0_M \neq b \in M$ such that $ab = 0$. Since 0 submodule is $S-$prime by assumption, then there is $s \in S$ such that $sa \in ann(M)$ or $sb = 0$. If $sb = 0$, then $s \in ann(b)$. Put $P = ann(b)M$. See that $S \cap (P : M) \neq \emptyset$, because s in the intersection. So we must have $P = ann(b)M = M$ otherwise, P wouldn't be $S-$prime which contradicts our assumption. By Corollary 2.5 of [3], there is an $x \in ann(b)$ such that $1 - x \in ann(M) \subseteq ann(b)$. This yields that $1 \in ann(b) = R$, so $b = 0$. This is a clear contradiction. We have $sa \in ann(M)$. So, $s \in (ann(a) : M)$ and hence by assumption $ann(a) = M$. Thus we get $a \in ann(M)$. Therefore, $ann(M)$ is the set of all zero divisors. Let a not to be a zero-divisor. If $a^2M = M$, then $aM = M$. Suppose $a^2M \neq M$. Since a^2M is $S-$prime, and $\langle a \rangle aM \subseteq a^2M$, by Lemma 7, there is an $s \in S$ such that $saM \subseteq a^2M$. Then $sam = a^2n$ for all $m \in M$ and some $n \in M$. Since a is not a zero-divisor, $sm - an \in ann(a) = 0$, and hence $sm = an$. This yields to that $sM \subseteq aM$ and therefore, $s \in (aM : M)$. By assumption, we have $aM = M$. Now take a submodule P of M. If $(P : M) = ann(M)$, then $P = ann(M)M = 0$. If not, take $a \in (P : M) - ann(M)$. Since $ann(M)$ is the set of zero-divisors, $a \notin ann(M)$ so $aM = M$. Then we get $M = aM = (P : M)M = P$. Therefore, M is a simple module.

($\Leftarrow$) This way is easy. Since the only proper submodule is 0 and $ann(M) \cap S = \emptyset$, we are done as 0 is a prime submodule.[4] □

6 References

[1] Ahmed Hamed, Achraf Malek. *S-prime ideals of a commutative ring.* Department of Mathematics, Faculty of Sciences, Monastir, Tunisia, 2019.

[2] Anderson DD, Dumitrescu T. *S-Noetherian rings.* Communications In Algebra, 2002.

[3] Atiyah M. *Introduction to Commutative Algebra.* Boca Raton, FL, USA: CRC Press, 2018.

[4] Esra Şengelen Sevim, Tarık Arabacı, Ünsal Tekir, Suat Koç. *On* $S-$*prime Submodules.* Turkish Journal of Mathematics, 2019.