Transactions of the Nigerian Association of Mathematical Physics
Volume 12, (July – Sept., 2020 Issue), pp41 – 44

BASICS PRIME SUBMODULES

Mengue Mengue David Joel

Department of Mathematic, University of Yaoundé 1, Cameroon,
P.O.Box:812 Yaoundé, Cameroon

Abstract

This article is devoted to point out some basic prime submodule and their properties. Using the fact that any ring is a module over itself, We investigate here some fairly new basics submodules called prime submodule and by AGUSTIN [**1**] ***definition we study some and use that notion to prove some well-known theorems firstly found inH. Matsumuru***[**2**]**.**
Mathematics Subject Classification: 20NO5

Keywords: Prime submodule, prime, maximal, radical, nil-radical, principal, primary ideal

INTRODUCTION

The quotient construction gives us a powerful way to build new modules and submodules. The properties of the modules we obtain as quotient depend on the properties of the submodule (ideals) we quotient by, and this lead us to the study of certain classes of submodulesBefore we state.Some results let us also introduce some notation and terminology. Throughout this note all rings are commutative with identity and all module are unital. Let R be a ring and let M be aR −module. A proper submodule K of M is said to be prime if for all $r$in R, the induced homothety $h_r: {}^{M}/_{K} \to {}^{M}/_{K}$, $h_r(\bar{n}) = r.\bar{n}$, is either injective or null. We may interpret the above as follows. The following definitions are also found in *P. Smith*[3].

Definition 1

Let R be a commutative ring, let M be a finitely generated R −submodule. A submodule K of M is prime if K is not equal to M and, for all r in R and all m in $M, r \cdot m$ is in K only if m is in K or rM is contained in K. In this chapter we are going to study tow important such classes.

Definition 2

Let R be a commutative ring and I an ideal of R. We said that I is a maximal ideal if it is not strictly contained in any proper ideal of R. We said that I is a prime ideal if $I \neq R$ and for all $a, b \in R$, whenever $a \cdot b \in I$ then either $a \in I$ or $b \in I$. If a prime I is principal any generator of I is said to be a prime element.

Theorem:1

a-) An ideal I in a ring R is prime if and only if ${}^{R}/_{I}$ is an integral domain.

b-) An ideal I of R is maximal if and only if R/I is a field.

c-) In particular a maximal ideal is prime.

Proof:

a-) Let R/I be an integral domain, suppose that $a, b \in R$. Note that $(a + I)(b + I) = 0 + I$ if and only if $ab \in I$. Thus R/I being an integral domain $(a + I)(b + I) = 0$ forces either $a + I = 0$ or $b + I$ is zero, that is, a or b lies in I, which shows that I is prime. The converse is similar.

b-) Suppose that I is maximal in R. We only have to show that every element of R/I has a multiplicative inverse. Let $r \in R$, $r \notin I$. The set $B = \{yr + a/a \in I, y \in R\}$ is an ideal of R which contains the element $r \notin I$ and so $B = R$. Therefore $1 = y_1 r + a_1$, say . So writing $\bar{x} = x + I$, we have, i.e., $\overline{1} = \overline{y_1} \cdot \bar{x}$ i.e;, $\overline{y_1}$ is the inverse of $\bar{x}$. Thus every nonzero element $\bar{x}$ has a multiplicative inverse. So R/I is a field.

Only if : Suppose that R/I is a field and I is not maximal. Then there exists an ideal B in Rsuch that $I \subseteq B \subseteq R$. Let r be any element of R, $b \in B, b \notin I$. Since R/I is a field, there exists $c + I \in R/I$ such that $r + I = (b + I)(c + I)$ i.e/, $r - bc \in I \subseteq B$. Therefore $r \in B$, since $b \in B$. So $B = R$. Hence I is maximal.

c-) The proof here is immediate from a-) and b-) since a field is an integral domain.

Remark:1

You can also give a direct prove that a maximal ideal is prime. Indeed if I is a maximal ideal and $a \cdot b \in I$, and suppose that $b \notin I$. Then the ideal $J = I + bR$ generated by I and b is strictly larger than I and so since I is maximal it must be all of R. But then $1 = i + b \cdot r$ for some $i \in I$and$r \in R$, and hence $a = a \cdot 1 = a \cdot i + (a \cdot b) \cdot r \in I$ since $i, a, b \in I$ as required.

Example:1

Let $R = \mathbb{Z}$, since an ideal I in $\mathbb{Z}$ is in particular a subgroup of the abelian group $\mathbb{Z}$, we know it must be cyclic, that is $I = d\mathbb{Z}$ for some integer d. Thus every ideal in $\mathbb{Z}$ is principal. An ideal $d\mathbb{Z}$ is prime exactly when d is prime, and since in that case $\mathbb{Z}/d\mathbb{Z}$ is a field provided $d \neq 0$ it follows the maximal ideals are exactly the nonzero prime ideals.

Correspondence Author: Mengue M.D.J., Email: mengueus@yahoo.com,

Theorem: 2
Let R be a ring with identity, $R \neq \{0\}$. Then R has at least one maximal ideal.
Proof:
We make use of the Zorn's lemma. Let $\Im$be the family of ideals of $R \neq \langle 1\rangle$ ordered by inclusion.$\Im$is non-empty since $\langle 0\rangle \in \Im$. Let $\{A_w\}_{w\in\Omega}$ be a chain of ideals in $\Im$ so that for each, $w, w' \in \Omega$ either $A_w \subseteq A_{w'}$or $A_{w'} \subseteq A_w$. Let $A = \cup A_w$. Then A is an ideal and $1 \notin A$since $1 \notin A_w$ for any w. So $\{A_w\}$ has an upper bound$A$and $A \in \Im$. Thus by Zorn's lemma,$\Im$ has a maximal element.
Corollary:1
Every proper ideal of a ring R with identity is contained in a maximal ideal.
Proof:
Let A be a proper ideal of R. Apply theorem 2 to R/A and the result follows.
Definition: 3
Let R be a commutative ring with identity. If R has a finite number maximal ideals, then R is said to be semi-local. If R has only one maximal ideal, then R is called a local ring.
Theorem:3
Let R be a commutative ring with identity.
(i) If I is an ideal of R such that every element of $R - I$ is a unit then R is a local ring and I is it unique maximal ideal.
(ii) If M is a maximal ideal of R such that every element of $1 + M$ is unit then R is a local ring.
Proof:
(i) Every ideal of R different from R cosists of non-units and so must be in I, so that I is the only maximal ideal of R.
(ii) Let $a \in R - M$, then $\langle a\rangle + M$ is an ideal of R and since M is maximal , $\langle a\rangle + M = R$. So there exists $b \in R, c \in M$, such that $ab + c = 1$ i;e., $ab = 1 - c \in 1 + M$ so that ab is a unit. Hence a is a unit. Thus R is local by (i).
Definition:4
Let R be a commutative ring with identity. The intersection of all the maximal ideals of R is called the Jacobson radical of R or just radical of R and denoted by $rad(R)$. An element a in a ring R is said to be nilpotent if $a^n = 0$ for some positive integer n. An ideal A in a ring R is said to be nilpotent if $A^n = AAA \ldots A$ (n times) $= \langle 0\rangle$, the zero ideal. Note that $A^n = \{\sum(a_1a_2a_3 \ldots a_n) \,/\, a_i \in A\}$ is an ideal . The ideal of nilpotent elements of R is called the nil radical and is denoted by $nil(R)$.
Theorem:4
Let R be a commutative ring with identity. Then ,$nil(R)$ is the intersection of all the prime ideals of R.
Proof:
From the definition of a prime ideal, it is clear that any $a \in nil(R)$ is an element of every prime ideal of R. So, we only have to show that given an element $s$of R, $s \in nil(R)$, there exists a prime ideal P such that $s \in P$. Let $S = \{s^n \,/\, n \not\geq 0\}$. Then S is a mulplicative subset of $R$and $S^{-1}R \neq \{0\}$. So, $S^{-1}R$ has at least one prime ideal Q say, (i.e., a maximal ideal by theorem). If $\varphi: R \to S^{-1}R$ is a map given by $(r) = r/1$, then $\varphi^{-1}(Q)$ is a prime ideal od R not containing s.
Definition:
Let I be an ideal in a commutative ring R with identity. The radical of I written $r(I) = \{x \in R/x^n \in I \; for\; some\; integer\; n > 0\}$
Theorem: 5
$r(I)$ is an ideal of R.
Proof:
Not that if $\varphi: R \to R/I$ denotes the canonical epimorphism. $\varphi(I) = \varphi^{-1}\big(nil(R/I)\big)$. So the radical of the ideal is also the an ideal. One can also use the definition of $r(I)$.
Theorem: 6
Suppose that I is an ideal in a commutative ring R with identity. Then $r(I)$ is the intersection of all the prime ideal of Rcontaining I.
Proof:
Immediate from theorem:4, since $r(I)$ is the inverse image of $r(0 + I)$ under the canonical map $R \to R/I$
We now define 'primary' ideals which correspond to the following properties of powers of a powers of a prime $p \in \mathbb{Z}$. Let a, b be two integers $n = p^m$ say, for some prime p. Suppose that n/ab and n/athen n/b^k, say. Conversely, any power of a prime has this property. This illustrate our next definition.
Definition:
An ideal Iin a commutative ring R with identity is said to be primary if whenever $a, b \in R, ab \in I$and $a \notin I$, then $b^k \in I$, for some integer k.
Example:
If $R = \mathbb{Z}$and p a prime, then $\langle p^k\rangle$is primary for any k.
The following theorem is immediate from the definition.
Theorem: 7
Suppose that I is a primary idealin a commutative ring with identity. Then the radical of I is a prime ideal.
Proof:
Let $ab \in r(I)$, $a \notin r(I)$, then $a^tb^t \in I$, say, for some $t \in \mathbb{Z}$. Since $a \notin I, a^t \notin I$ and since I is primary $(b^t)^s \in I$ for some integer s. So $b \in r(I)$.
Definition:
If I is a primary ideal in a commutative ring$R$, then the prime $P = r(I)$ is called the prime ideal belonging to I and I is called the $P - primary$ ideal of R.

Corollary: ([4] A. Marcelo and J. Munoz)
A prime ideal coincides with its radical.
We now consider a more substantial example, that of polynomials in one variable over a field. Although the case of field coefficients is the one we really need for the moment, the following lemma captures, for polynomials with coefficients in the general ring, when we can do "long division with remainders" in polynomial rings. For this we first need to recall the notion of the degree of a nonzero polynomial.

Definition: 3

If R is a ring and $f \in R[x]$ is nonzero, then we may write $f = \sum_{i=0}^{n} a_i x^i$, where $a_n \neq 0$. We set the degree $\deg(f)$ of f to be n, and said that a_n is a leading coefficient of f.If R is an integral domain, then for any $f, g \in R[x]$ you can check that $\deg(fg) = \deg(f) + \deg(g)$ (and so in particular this implies $R[x]$ is also an integral domain).

Theorem;2 (Division algorithm)

Let R be a ring and $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, where $a_n \in U(R) = R^{\times} = \{x \in R, \exists a \in R, x \cdot a = 1_R\}$. Then if $g \in R[x]$is any polynomial there are unique polynomials $q, r \in R[x]$ such that either $r = 0$ or $\deg(r) < \deg(f)$and $g = qf + r$.

Proof:

This is straight-forward to prove by induction on deg(g). Since $a_n \in R^{\times}$ if $h \in R[x] \setminus \{0\}$ by the fact that a unit is not a zero divisor it is easy to see that $\deg(fh) = \deg(f) + \text{def}(h)$. It follows that if $\deg(g) < \deg(f)$ we must take $q = 0$ and thus $r = g$. Now suppose that $g = \sum_{j=0}^{m} b_j x^j$ where $b_m \neq 0$and $m = \deg(g) \geq n = \deg(f)$. Then since $a_n^{-1} b_m x^{m-n} f$ has leading term $b_m x^m$ the polynomial $h = g - a_n^{-1} b_m x^{m-n} f$has $\deg(h) < \deg(g)$. It follows by induction that there are unique $q', r'$with $h = q'f + r'$. Setting $q = a_n^{-1} b_m x^{m-n} + q'$ and $r = r'$ it follows $g = qf + r$. Since q and r are clearly uniquely determined by q' and r' they are also unique as required.

It follows from the previous Theorem that if F is a field then we have the division algorithm for all non-zero polynomials. This allows us to prove that all ideals in $F[x]$ are principal.

Theoem: 3

Let I be a non-zero ideal in $F[x]$. Then there is a unique monic polynomial f such that $I = \langle f \rangle$. In particular all ideals in $F[x]$ are principal.

Proof:

Since I is nonzero we may pick an $f \in I$ of minimal degree, and rescale it if necessary to made it monic. We claim $I = \langle f \rangle$. Indeed if $g \in I$, then using the division algorithm, we may write $g = qf + r$ where either $r = 0$ or $\deg(r) < \deg(f)$. But then $r = g - qf \in I$, and thus by minimality of the degree of $f \in I$ we must have $r = 0$ and so $g = qf$ as required. The uniqueness follows from the fact that if $I = \langle f \rangle$ and $I = \langle f' \rangle$ then we would have $f = af'$and $f' = bf$, for some polynomials $a, b \in F[x]$. But then$f = af' = (ab)f$ so that a and b must have degree zero that is $a, b \in F$. Since we required f and f' to be monic, it follows that $a = b = 1$ and so $f = f'$ as required.

The division algorithm also allows to give a reasonably explicit description of the rings we obtain quotient of the polynomial ring $F[x]$. We have just seen that any non-zero ideal I is of the form $\langle f \rangle$ for a monic polynomial f. By the division algorithm, any polynomial g can be written uniquely as $g = qf + r$where $\deg(r) < \deg(f)$. Thus the polynomials of degree strictly less than $d = \deg(f)$ form a complete set of representatives for the $I-$cosets : every coset contains a unique representatives$r$ of degree lees than $\deg(f)$. Since the set $\{1, t, t^2, \dots, t^{\deg(f)-1}\}$ form a basis of the $F-$vector space of polynomials of degree less than $\deg(f)$ this means that if we let $q: F[x] \to F[x]/I$ be the quotient map, and $\alpha = q(x)$, then $\{1, \alpha, \dots, \alpha^{d-1}\}$ form a $F-$basis for $F[x]/I$, and we multiply in $F[x]/I$ using the rule $\alpha^d = -a_0 - a_1\alpha - \cdots - a_{d-1}\alpha^d$, where $f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$. In particular $F[x]/\langle f \rangle$ is a vector space of dimension $\deg(f)$. We can therefore interpret the quotient construction $F[x]/\langle f \rangle$ as a way of building a new ring out of F and an additional element α which satisfies the relation $f(\alpha) = 0$, or rather, the quotient construction gives us a rigorous way of doing this. The following example shows how one can use this to give a new construction of the complex numbers.

Example: 2

When $F = \mathbb{R}$ intuitively we build $\mathbb{C}$ out of $\mathbb{R}$ and an element "i" which satisfied $i^2 + 1 = 0$. The quotient construction lets us make this intuition rigorous: we simply define $\mathbb{C}$ to be the quotient ring $\mathbb{R}/(i^2 + 1)$. Indeed this is a field because $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. and if we let i denote the image of x under the quotient map from $\mathbb{R}[x]$ to $\mathbb{C}$, then $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$ is a two-dimensional $\mathbb{R}-$vector space with basis $\{1, i\}$ and i satisfies $i^2 + 1 = 0$.

Remark:2

In fact with a little more care it is straight-forward to check that if R is any ring and $f \in R[x]$ is a monic polynomial of degree d, and we let $Q = R[x]/\langle f \rangle$ and $\alpha = q(x)$ (where $q: R[x] \to R[x]/\langle f \rangle$ is the quotient maps as before) then any element of Qcan be written uniquely in the form $r_0 + r_1\alpha^1 + r_2\alpha^2 + \cdots + r_{d-1}\alpha^{d-1}$, where the multiplication in Q is given as above. Of course for a general ring not all ideal in $R[x]$ will necessarily be principal, and even if $I = \langle f \rangle$, if the leading coefficient of f is not a unit, we cannot apply the division algorithm.as in *T S Blyth*[5].

Notice that the argument we used in the proof of theorem 3, runs exactly the same way as the proof that every subgroup of $(\mathbb{Z}, +)$ is cyclic (or that any ideal in $\mathbb{Z}$ is principal). This suggests it might be useful to abstract the division algorithm for a general integral domain.

Definition:4

Let R be an integral domain and let $\mathcal{E}: R \setminus \{0\} \to \mathbb{N}$ be a function. We say that R is a Euclidean domain if given any $a, b \in R$ with $b \neq 0$there are $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varepsilon(a) < \varepsilon(b)$.

Remark:3
Some texts require that the norm ε satisfies additional proposition, and in practice these additional properties are often very useful. For example sometimes the norm satisfies $\varepsilon(ab) = \varepsilon(a) \cdot \varepsilon(b)$. (in which case the norm is said to be multiplicative) or $\varepsilon(ab) = \varepsilon(a) + \varepsilon(b)$. The most general additional property one often asks for is that $\varepsilon(a) \leq \varepsilon(ab)$ for all $a, b \in R \setminus \{0\}$. You can check that if R is a Euclidean domain satisfying this last property then the group of units $R^{\times}$ is respectively the set $\{a \in R, : \varepsilon(a) = \varepsilon(b)\}$. However, if one just wants to know the ring is a PID the only condition one needs is the division algorithm.. Both $\mathbb{Z}$and $F[x]$, for any field F, are Euclidean domains with the norm given by the absolute value and the degree function respectively. We now show that the Gaussian integers, $\mathbb{Z}[i]$ gives another example.

Theorem:4
Let $R = \mathbb{Z}[i]$ and let $\mathcal{E}: R \to \mathbb{N}$ be the function $\mathcal{E}(z) = a^2 + b^2$, where $z = a + ib \in \mathbb{Z}[i]$, $a, b \in \mathbb{Z}$. Then $(R, \mathcal{E})$ is an Euclidean Domain.

Proof:
Note that $\mathcal{E}$ is the restriction of the square of the modulus function on $\mathbb{C}$, so in particular $\mathcal{E}(zw) = \mathcal{E}(z).\mathcal{E}(w)$. We write $|z|^2$ instead $\mathcal{E}(z)$ when $z \in \mathbb{C} \setminus \mathbb{Z}[i]$. Suppose that $s, t \in \mathbb{Z}[i]$and $t \neq 0$. Then $s/t \in \mathbb{C}$, and writing $s/t \in u + iv$ where $u, v \in \mathbb{Q}$, we can clearly take $a, b \in \mathbb{Z}$ such that $|u - a|, |v - b| \leq 1/2$ and so $q = a + ib$ we have $|s/t - q|^2 \leq 1/4 + 1/4 = 1/2$, and so $\varepsilon(s - qt) \leq 1/2\,\varepsilon(t)$ (since $\varepsilon(z_1 z_2) = \varepsilon(z_1)\varepsilon(z_2)$) and hence if $r = s - qt \in \mathbb{Z}[i]$ we see that either $r = 0$ or $\mathcal{E}(r) \leq 1/2\,\varepsilon(t) < \varepsilon(t)$ as required. Note that r is not necessarily unique in this case.

Theorem:5
Let $(R, \mathcal{E})$ be an Euclidean domain; Then any ideal in R is principal.

Proof:
The proof that any ideal is principal is exactly the same as for $F[x]$. If I is a non-zero ideal, take $d \in I$ such that $\varepsilon(d)$ is minimal. Then if $m \in I$ we may write $m = qd + r$, where $r = 0$ or $\varepsilon(r) < \varepsilon(d)$. But $r = m - qd \in I$ so that the minimality of $\varepsilon(d)$ forces $r = 0$ and so $m = qd$. It follows that $I \subseteq Rd$, and since $d \in I$clearly $Rd \subseteq I$, hence $I = Rd$ as required.

Definition:5
An integral domain in which every ideal is principal, that is generated by a single element, is called a principal ideal domain. ThisIs usually abbreviated to PID. The previous theorem shows that any Euclidean domain is a principal ideal domain.

Remark:4
It is also possible to consider rings in which every ideal is principal but which are not necessarily integral domains. Such rings are called principal ideal rings. As we mostly focus on integral domains, we will not however use this term in this dissertation. We would like to calculate which ideals in a Euclidean domain are prime and which are maximal. In fact we can give an answer for any PID not just any Euclidean domain.

Definition:6
Let R be an integral domain. A nonzero element $r \in R$ is said to be irreducible if whenever $r = a \cdot b$ then exactly one of a or b is unit (so that in particular r is not a unit). We will say an element $r \in R \setminus (\{0\} \cup R^{\times})$ is reducible if it is not irreducible.

Theorem:6
Let R be a principal ideal domain and let $d \in R \setminus \{0\}$. Then the following are equivalent:
(1) $Rd = \langle d \rangle$ is a prime ideal
(2) d is irreducible in R
(3) Rd is a maximal ideal of R

Proof:
(We shall use the following method (1)$\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1)) .
For (1) $\Longrightarrow$ (2): If $d = ab$ then as $d \in Rd$ is prime we must have $a \in Rd$ or $b \in Rd$. By symmetry we may assume $a \in Rd$(and hence, since Rd is a proper ideal and $Ra \subseteq Rd$ we see that a is not a unit). But then there is some $r \in R$ with $a = rd$ and so $d = ab = (rb)d$ and hence $(1 - rb)d = 0$ and so since R is an integral domain and $d \neq 0$ we must have $rb = 1$, that is $b \in R^{\times}$.
For (2) implies (3): Suppose that d is irreducible and that $Rd \subseteq I \lhd R$. Since R is a PID we must have $I = Ra$ for some $a \in R$, and $Rd \subseteq Ra$ shows that $d = ab$ for some $b \in R$. But then as d is irreducible we must have one of a or b a unit. But if a is a unit, then $Ra = R$, while if b is a unit, d and a are associates and so generate the same ideal, that is $Rd = I$. It follows that $Rd$is a maximal ideal as claimed.
For (3) $\Longrightarrow$(1): We have already seen that in any ring a maximal ideal must be prime.

Remark:5
Note that the implication "(1) implies (2)" holds in any integral domain, while "(3) implies (1)" holds in any commutative ring. In a general ring $d \in R$ irreducible is equivalent to the ideal Rd being maximal amongst principal ideals in$R$.

THEOREM DEFINITION (MAIN RESULT):
Let R be a commutative ring and M a finitely generated $R-$submodule. A submodule K of M is prime if $K \neq M$ and $\forall r \in R, \forall m \in M,$ if $r \cdot m \in K$ then $m \in K$or $rM \subseteq K$. In case $M = R$ the prime submodules of M are precisely the prime ideals. For further study we shall consider the case $M \neq R$.

REFERENCES:

[1] Agustin, Felix *Marcelo* and Cesar Rodrigues '*Some reslts on Prime and Primary submodules'* Proyecciones Vol;22 No:3 pp 201-208 december 2002
[2] H. Matsumuru, "Commutative ring theory" Cambridge Univ Press (1986)
[3] P. Smith, "Primary Modules over Commutative rings" Preprint Univ. of Glasgow, (1999)
[4] A. Marcelo and J. Munoz "Prime submodules, the Descent Invariant, and Modules of finite length" J. alg. 189, pp 273-293, (1997)
[5] T S Blyth, 'Module Theory' Clarendon Press, OXFORD, (1977).