IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 15, Issue 2 Ser. III (Mar – Apr 2019), PP 40-43
www.iosrjournals.org

Some Paradigms on Principal Ideal Domain

Dr. Rehana Parvin[1], Dr. Rashida Pervin[2]

[1] *(Department of Quantitative Sciences, IUBAT-International University of Business Agriculture and Technology, Bangladesh)*

[2] *(Department of Quantitative Sciences, IUBAT-International University of Business Agriculture and Technology, Bangladesh)*

Abstract: *A direct sum of simple modules is being splited by every module. There are different kind of rings but special case has been raised in Principal Ideal Domain(PID). PID is considered like as semisimple rings that is splited a direct sum. In fact while the integer Z and the ring of polynomial $k[x]$ may look like as different rings initially but these are very analogous for being both PIDs.*

Keywords: *Semisimple Ring ,Principal Ideal Domain, Principal Ideal, Integral Domain, Direct Sum.*

Date of Submission: 07-04-2019 Date of acceptance: 23-04-2019

I. Introduction

In this paper, we have tried to focus on few illustrations on commutative rings that will escort up to the perception of PID .Besides these, it has been tried to draw on PID namely the integer Z for which modules are just abelian groups. If we follow another type of significant example that will be the ring of polynomials denoted by $k[x]$ in one variable over a field k .

1.1 Integral Domain:

If a ring follow the condition i.e. $0 \neq 1$, here 0 is an additive identity and 1 is a multiplicative identity and whenever $a,b \in R$ and $ab = 0$ either $a = 0$ or $b = 0$ is known as an Integral domain (or in short domain).
A ring is a field when $0 \neq 1$ and every nonzero element is a unit, i.e. has a multiplicative inverse.

1.2 Principal Ideal Domain:

A principal ideal domain is an integral domain in which every ideal is principal i.e. can be generated by a single element. More generally, a principal ideal ring is a nonzero commutative ring whose ideals are principal, although some author (e.g., Bourbaki) refers to a PIDs as principal rings.

1.3 Semi-simple Ring:

A ring R with 1 is Semi-simple, or left semi-simple to be precise, if the free left $R-\text{mod}ule$ underlying R is a sum of simple $R-\text{mod}ule$.

1.4 Direct Sum:

The direct sum is an operation from abstract algebra, a branch of mathematics. For example, the direct sum $R \oplus R$, where R is real coordinate space, is the Cartesian plane R^2.To see how direct sum is used in abstract algebra, consider a more elementary structure in abstract algebra, the abelian group. The direct sum of two abelian groups A and B is another abelian group $A \oplus B$ consisting of the ordered pairs (a,b) where $a \in A$ and $b \in B$. To add ordered pairs, we define the sum $(a,b)+(c,d)$ to be $(a+c, b+d)$; in other words addition is defined coordinate wise. A similar process can be used to form the direct sum of any two algebraic structure such as rings, modules and vector spaces.

II. Paradigms

2.1: A ring has no zero-divisor <= > it is a domain. If $ab = 0$ and $a,b \neq 0$, it would be said that a and b are zero-divisors. Consider a unit denoted by u which is never a zero-divisor.

Since $ub = 0$ => $b = u^{-1}ub = u^{-1}0 = 0$.Hence every field represents a domain. Fields will usually be denoted by k instead of R^2.

Remark: Multiplication lets cancellation in a domain. If $ac = bc$ and $c \neq 0$ then $a = b$. In fact we have $(a-b)c = 0$ since $c \neq 0$, $a - b = 0$.

2.2: The complex C, the real R and the rational numbers Q are fields.

2.3:The integers Z are not a field but domain.

2.4: Assume the linear mapping $f : R \to R$ (with point wise multiplication and addition). So $C(R)$ be the ring of continuous function. Then R is not a domain.

To make it clear, it could be constructed continuous function f and g such that $f(x) = 0$ for $x \notin [0,1]$ and $g(x) = 0$ for $x \notin [2,3]$ but $f(\frac{1}{2}) = g(\frac{5}{2}) = 1$. Then $fg = 0$ but $f, g \neq 0$.

2.5: From the number theory it is standard fact that for y any prime p, the integers $\text{mod}\ p$ denoted by $Z/(p)$, can divided(except by 0) $\text{mod}ulo$ a prime.

2.6: In fact express $n = ab$ where $a, b \neq \pm 1$ when n is not prime, $Z/(n)$ is not a domain. Then $\text{mod}ulo$ n, a and b are nonzero but $ab \equiv 0$.

III. Necessary and sufficient condition of an ideal to be maximal

3.1 Prime: An ideal I in a ring R is prime if the quotient of R and I i.e. R/I is a domain and maximal if R/I is a field.

3.2: Proposition: Consider an ideal and larger ideal are denoted by I and J respectively. Assume that $I \subset J \subset R$.Then no strictly larger ideal J will occur if and only if an ideal I which is also belong to a ring R, is maximal.

Proof: Ideals $J \subset R$ containing I are equivalent to ideals of R/I .Let $r : R \to R/I$ and $s : R \to R/J$ be the canonical maps.If $I \subseteq J$, then $s(I) = 0$ we can factor s uniquely as tr for some $t : R/I \to R/J$, which is surjective since s is unique. Then we gain an ideal $j' = \ker(t)$ in R/I.

On the contrary if we start with $J' \subset R/I$, it would be defined an ideal $J \supseteq I$ as the kernel of the composition $R \to R/I \to (R/I)/J'$.These are inverse to each other[1,page-3].

Thus a proper ideal is 0 if and only if $k = R/I$ is a field. If k is a field and $I \subset k$ is an ideal and $a \in I$ is nonzero, then $1 = a^{-1}a \in I$, from which it follows that $I = k$, a contradiction. Conversely, if k is not a field and $a \in k$ is non zero and not a unit, then $1 \notin (a)$ so (a) is a nonzero proper ideal.

IV.PIDs and prime factorization

4.1: Definition:

An ideal I in a ring R is principal if it is equal to (a) **for** some $a \in R$ **.**A principal ideal domain is a domain in which every ideal is principal.

4.2: Proposition: PID is belonged in integers.

Proof:

Assume an ideal denoted by I which is also belonged to integers i.e. $I \subset Z$ .It is necessary to prove that I is principal. If $I = 0$, this is trivial. If $I \neq 0$, let n be the smallest positive integer in I (if $m \in I$, then $-m \in I$, so some positive integer is in I). We claim that $I = (n)$. Now $m \in I$, we can divide m by n with remainder to write $m = qn + r$ where the remainder r satisfies $0 \leq r < n$. But then $r = m - qn \in I$, so minimality of n forces r to be 0. Hence $m = qn \in (n)$. Since $m \in I$ was arbitrary $I = n$.

4.3: Let R be a domain and $m,n \in R$. Then m divides n or $m|n$ if there exists $l \in R$ such that $n = ml$. Equivalently, $m|n$ if $(n) \subseteq (m)$. We say $m \in R$ is irreducible if m is not a unit and whenever $m' = mn$ either $m'|m$ or $m'|n$. We say m' is prime if the ideal (m) is a prime ideal.

4.4: Theorem: Assume a Principal Ideal Domain is R and m is a nonzero element in R i.e. $m \in R$. Then from the theorem of fundamental arithmetic equation expounds that
(1) m' is prime
(2) m' is irreducible
(3)the ideal (m') is maximal.

Proof: (2=>3): Let m' is irreducible. Then whenever $m|m'$, n is either a unit or an associate of m'. Since $(m') \subseteq (m)$ if and only if $m|m'$. It is obtained that $(m') \subseteq (m)$ only holds for $(m) = (m')$ or $(m) = R$. Since a Principal Ideal Domain is R, every ideal is (m) for some m, so this represents that exactly (m') is maximal according the proposition of 3.2.
(3=>1): To be prime, ideal must be maximal ideal individually.
(1=>2): Consider m' be prime and let $m' = mn$. Then modulo (m'), $mn \equiv 0$.Since the quotient of ring and nonzero element i.e. $R/(m')$ is a domain, it follows that either $m \equiv 0$ or $n \equiv 0$ i.e. $m \in (m')$ or $m \in (m')$ .This is equivalent to either $m'|m$ or $m'|n$ as required[1, theorem;2.5,page:6].

4.5: Corollary: Consider a PID R whose every non zero element of R can be factorized as $up_i^{d_i}$ where u is a unit and p_i are primes, $(i > 0, d_i > 0)$ .Then $up_i^{d_i}$ is unique up to permuting the p_i.

Proof: To prove the above corollary we need to prove first the existence of the factorization. If a is a unit, this is zero. Otherwise, let P be any maximal ideal containing (a). Then $P = (p_1)$ for some chosen prime p_1, and $p_1|a$ since $(a) \subseteq (p_1)$ .Write $a = p_1 a_1$. The argument is repeated with a_1 in place of a to write $a_1 = p_2 a_2$ if a_1 is not a unit. Continue by induction. If we ever get $a_n = u$ to be a unit, we are done, since $a = p_1 a_1 = p_1 p_2 a_2 = ... = p_1 p_2 .... p_n u$. If we never get a unit, we get an infinite ascending chain of ideals $(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset ......$ Let $I = \bigcup (a_n)$; then I is an ideal. But then $I = (b)$ since R is a PID, and $b \in (a_n)$ for some n. But then $I = (a_n) \supseteq (a_{n+1})$, so $(a_n) = (a_{n+1})$, a contradiction. Hence the process must eventually stop with a_n a unit, and we get the desired factorization.
Now to prove uniqueness by induction on $\sum d_i$. If $\sum d_i = 0$ (i.e., $n = 0$), then $a = u$ is just a unit, and uniqueness is obvious. Now suppose $\sum d_i > 0$ and $a = up_1^{d_1} p_2^{d_2} ... p_n^{d_n} = vq_1^{e_1} q_2^{e_2} ... q_m^{e_m}$ are two different factorizations. Then p_1 divides the product on the right-hand side and is prime, so p_1 must divide one of the factors. Since no two chosen primes are associate, this implies that $p_1 = q_i$ for some i. Cancelling these common factors, we get $b = up_1^{d_1 - 1} p_2^{d_2} ..... p_n^{d_n} = vq_1^{e_1} q_2^{e_2} q_3^{e_3} q_4^{e_4} ...... q_i^{e_i - 1} .... q_m^{e_m}$ .We have decreased $\sum d_i$ by one, so by induction the factorization of b is unique, so these two factorizations are the same up to permutation. It follows that the two original factorization of a were the same up to permutation.

V. Conclusion

In fact this paper highlights on the Principal Ideal Domains paradigms .To focus on those property it forces that 4.1 gives the concept of ideal i.e. PID.
4.2 elaborates between PID and Integers and 4.4 represents when the PID is prime, irreducible and maximal ideal. Hence finally 4.5 says that PID can be factorized and it is unique up to permuting.

References

[1]. Waffle, Principal Ideal Domain, Mathcamp 2009, P: 1-9.
[2]. A.W Chatters "Rings which are nearly principal Ideal Domain." Glasgow Math. J.40(1998):343-351.
[3]. From Google Wikipedia.
[4]. Thomas William Hungerford, "On the structure of Principal Ideal Rings." PJ of Mathematics, vol25, No.3,1968.

Rehana Parvin. "Some Paradigms on Principal Ideal Domain." IOSR Journal of Mathematics (IOSR-JM) 15.2 (2019): 40-43.