ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 10 , October 2019

Review on Euclidean Domains, Principal Ideal Domains and Unique Factorisation Domains with its Applications

Jaspreet kaur

PG student, Assistant Professor, Department of Mathematics, Sri Guru Teg Bahadur Khalsa College,
Sri Anandpur Sahib,Punjab, India.

ABSTRACT: The aim of present paper is to review some results on ring theory. Throughout this paper we discuss R is commutative ring with unity. Particularly, we discuss the basic definitions of Rings, Ideals, Integral Domains, Principal Integral Domain (PID), Unique Factorization Domain(UFD) and Euclidean Domain(ED).We have presented some important application on Principal Ideal Domain (PID),Unique Factorization Domain(UFD) and Euclidean Domain(ED).

KEYWORDS: Binary operations, Commutative Ring, Integral Domains, Ideals, Ring of Integers, Polynomial Rings etc.

I.INTRODUCTION

Covers some very basic concepts of Ring Theory over some fields like Integers, Rationals, Real numbers,Complex numbers etc. We begin with some basic definitions of Ring theory. As we study that Group theory stands only on the study of only one Binary operation, While Ring theory involves two Binary operations with additional elementry properties. There are many mathematical structures of study having two binary operations ,one is addition and the other is multiplication on $\mathbb{Z}, \mathbb{Q}, R, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, n \times n\ matrices$ etc In Ring theory there is a very interested concept of “division”, ” division algorithm”, ” prime “, ”factorization” etc , from the ring of integers $\mathbb{Z}$ to an arbitrary commutative integral domain R with unity. Also we rephrase by definitions with innumerable examples ofIdeals, Divisors, Domains like Unique Factorization Domain,Principal Ideal Domain,Euclidean Domain along with their Applications including Euclidean Domain and the Gaussian Integers, Eisenstein integers, Polynomial rings, Smith Normal Form.

II.LITERATURE SURVEY

A) P.B.Bhattacharya, S.K. Jain, S.R.Nagpaul:- Outlined the expansion of ring theory with the concept of Ideals and homomorphism. In First edition he deals with rings and cover very basic concepts of rings, illustrated by numerous examples, including prime ideals, maximal ideals, UFD, PID and ED. Among these in second edition he represent the application division algorithm, Euclidean algorithm of Euclidean Domain(ED), Polynomial rings of Unique Factorization Domain(PID), Smith normal form of Principal ideal domain(PID).

B) C Musili:- In Second Revised edition covering the very basic aspects of Rings, Ideals, Factorisation in Commutative Integral Domain. He also extended the concepts of Division, Division algorithm, Gaussian integers, Prime, Factorization ,Polynomial rings over PID etc from the ring of integers $\mathbb{Z}$ to an arbitrary commutative integral domain R with unity.

C) David Joyce:-Expressed the ring theory its properties, Integral Domains, the Gaussian integers, Divisibility in Integral Domain, Euclidean Algorithm, Division for Polynomial that is Division Algorithm and also give very important Unique Factorization theorem proving result of Unique factorization domain.

D) Linda Gilbert/Jimmi Gilbert:-She has been writing text book since 1981 with her husband Jimmi Gilbert including ‘Elements of Modern Algebra’ and ‘Linear Algebra and Matrix theory’. As the earlier editions the author gradually introduce and develop concepts to help make the material more accessible. In 7th edition developed the concept that how ring of integers working in Integral Domains, how a Field and Integral domain(finite /infinite) working together.

E) Joseph J. Rotman:-The first edition is printed in 2002 and second in 2003.He study advanced algebra and its related topics .Introduces prime and maximal ideals in commutative rings, UFD etc.
F) E Weiss, MC Grawhill:-One can initiate the study of algebraic number theory either **globally and locally** i.e. either by considering ideals in the rings of integers of number fields or else by looking first at the behaviour of field extensions at a single prime divisor and investing relationship among different prime of same field and gives results on *Minkowski bound* .

III.RINGS

A nonempty set $Ɍ \neq \emptyset$ together with two binary operations '+','·'which are called as addition and multiplication (product) respectively, then it becomes a ring Ɍ if its satisfies following properties:

- $(Ɍ, +)$ is an abelian group.
- $(Ɍ,\cdot)$ is a semi group
- Distributive law hold for both left and right sides i.e.

$$p(q + r) = p.q + p.r \quad and \quad (p + q)r = p.r + q.r \qquad \forall p, q, r\epsilon Ɍ$$

A. Ring With Unity: A ring$(Ɍ, +,\cdot)$ in which multiplicative semi group has an identity element
i.e.$1 \in Ɍ$such that $p.1 = p = 1.p \qquad \forall p \in Ɍ$.

B. Commutative ring: A ring $(Ɍ, +,\cdot)$ in which multiplicative semi group satisfies commutative property
i.e. $p.q = q.p \qquad \forall p, q \in Ɍ$.

C. Examples(Trivial and Non trivial)

- The rings $\mathbb{Z}, \mathbb{Q}, Ɍ, \mathbb{C}$ are trivial examples of commutative ring with unity.
- An example of a non-trivial commutative ring in which every element is of square 0 (*C Musili)* different comparisons are:
- An example: $M_2(\mathbb{Z}/2\mathbb{Z})$ with usual addition but multiplication *defined as $P * Q = PQ + QP$, but associativity of * is failure here.
- If we tried $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with point wise addition and multiplication in vector calculus. But this process is also not associative.

IV. IDEAL

Let Ɍ be a ring, $Ƙ \subset R$ is a left ideal (right ideal) if it satisfies following two conditions:

- $a, b \in Ƙ \to a - b \in Ƙ$
- $a \in Ƙ\, and\, r \in R \to ra \in Ƙ\, \left(a \in Ƙ\, and\, r \in R \to ar \in Ƙ\right)$

Here a Left Ideal or Right Ideal is a subring of$(Ɍ, +, .)$. An Ideal is also called a two sided ideal if the subset Ƙ of Ɍ is both of left and right ideal.

A. Examples (Trivial and Non Trivial):

- $\{0\}$ and R are the trivial examples of ideals of Ɍ
- The sets $G_1 = \left\{\begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix} \mid p, q \in Ɍ\right\}$ and $G_2 = \left\{\begin{pmatrix} p & 0 \\ q & 0 \end{pmatrix} \mid p, q \in Ɍ\right\}$ are respectively right and left ideals of $M_2(R)$ for any ring Ɍ.

As we know that proper means "*not* Ɍ" and nonzero means "*not*$\{0\}$ and nontrivial means "*not*Ɍ *and not* $\{0\}$"
If $\xi: R \to S$ is ring homomorphism then its $kernalker\xi = \{r \in R: \xi(r) = 0\}$ is an ideal of Ɍ and must be proper ideal of Ɍbecause if $ker\xi = 0$then$\xi = identically\, 0$.

B. Prime Ideal:Let Ɍ be a commutative ring .An Ideal Ƙis said to be a Prime ideal of Ɍ if

1. $Ƙ \neq Ɍ$
2. $p, q \in Ɍ, pq \in Ƙ \to either\, p \in Ƙ\, or\, q \in Ƙ$

C. Maximal left Ideals*:* Let Ɍ be a commutative ring then aleft ideal is called maximal ideal of Ɍ if
1. $Ƙ \neq Ɍ$
2. For any ideal there is no Ideal strictly between Ƙ *and* Ɍ *i.e*
If any ideal $\mathcal{L}$ *of* Ɍ *such that* $Ƙ \subseteq \mathcal{L} \subseteq Ɍ \Rightarrow$ *either* $Ƙ = \mathcal{L}$ *or* $\mathcal{L} = Ɍ$ is hold

D.Minimal left Ideal:Let Ɍ be a commutative ring then aleft ideal is called minimal ideal of Ɍ if
1. $Ƙ \neq \{0\}$
2. For any ideal there is no ideal strictly between$\{0\}$ *and* Ƙ i.e.

$$\{0\} \subseteq \mathcal{L} \subseteq Ꝁ \Rightarrow \ \ either\ \mathcal{L} = \{0\}\ or\ Ꝁ = \boldsymbol{\mathcal{L}}$$

V. BASIC ALGEBRA OF THESE IDEALS

A. Addition of Ideals:If$Ꝁ$ *and* $\mathcal{L}$ are ideals in ring Ɍ ,then

$$Ꝁ + \mathcal{L} = \{x + y\ /\ x \in Ꝁ, y \in \mathcal{L}\} \subseteq Ɍ$$

B. Multiplication of Ideals:

IfꝀ , $\mathcal{L}$ are two ideals of the ringɌ, we define multiplication of two subsets $Ꝁ, \mathcal{L}\ of$ Ɍ as $Ꝁ\mathcal{L} = \{x_1y_1 + x_2y_2 + \cdots x_ny_n / x_i\epsilon Ꝁ, y_i \in \mathcal{L}, 1 \le i \le n, n \in N\}$i.e. finite sums of x.

VI. UNITS AND ZERO DIVISORS

A. Units: Let Ɍ be a ring with unity .An element $p \in$ Ɍ is said to be a unit or invertible if $\exists\ q \in$ Ɍ such that $pq = qp = 1$ the element q is called the multiplicative inverse of p and is denoted by p^{-1} .

B. Examples: The rings $\mathbb{Z}, \mathbb{Q}$, Ɍ, $\mathbb{C}$ are commutative ring with unity .Every non zero element of $\mathbb{Q}$, Ɍ, $\mathbb{C}$ is invertible and the inverse of p is p^{-1} . However the only units in is ± 1.

C. Zero Divisors*:* An element $p \in$ Ɍ is said to be a left zero divisor if $\exists q \neq 0$ suchthat $pq = 0$.Similarly p is right zero divisor if $\exists\ r \neq 0$ suchthat$rp = 0$. An element $p \in$ Ɍ is zero divisors, if it is both left and right zero divisor.

D. Example based on Units and Zero divisors:

- Find Zero divisors and Units of Ring $\mathbb{Z}_n \times \mathbb{Z}_m$.
- The units of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ are the different combinations of units of $\mathbb{Z}_n$and units of $\mathbb{Z}_m$
- If we take $\mathbb{Z}_6 \times \mathbb{Z}_2$ then units are different combinations of units of $\mathbb{Z}_6$ (units are 1 and 5) and units of $\mathbb{Z}_2$ (unit is 1).
- In a finite commutative ring,a non zero element is either a unit or a zero divisors .If we find all elements of $\mathbb{Z}_n \times \mathbb{Z}_m$ and find all units , then the zero divisors are left i.e. not exist.

VII. FIELDS

A field is also a special type of ring .Let F be a ring with some additional properties is become to form a field.
Conditions are:

- F is commutative ring.
- Identity element in F, i.e. e ≠ 0
- Multiplicative inverse exist for every non zero element

The Rationals, Reals, and Complex form field and also if any ring corresponding to any prime $\mathbb{Z}_p$ is a field.

VIII. INTEGRAL DOMAIN

Firstly we revise that there are many *ID* like every field is an Integral Domain that is ℝi.e Real no's field ,Rings of Polynomials, The ring of Integers but the ring of integers which is *ID*gives very usable properties for Domains. First is Euclidean domain that is basis on Division Algorithm Second is Principal Ideal and third is Unique Factorisation. Also every ring has not all these properties after defining all these nice properties we revise a special relationship between them that is every *ED⇒PID*, every *PID⇒UFD*, every *UFD⇒ID.*
i.e. IDs ⊃ UFDs ⊃ PIDs ⊃ EDs

A. Definition of Integral Domain:A ring Ɍ which is non zero is called an Integral Domain if there is no proper i.e. non trivial zero divisors in Ɍ.
An integral domain satisfies three main conditions:

- $If\ p^2 = 0 \Rightarrow p = 0$
- $If\ pq = pr \Rightarrow q = r$
- $If\ p \neq 0\ and\ q \neq 0 \Rightarrow pq \neq 0\ or\ pq = 0\ either\ p = 0\ or\ q = 0$

B.Examples (Trivial and Non Trivial respectively)

a)$\mathbb{Z}, \mathbb{Q}$, Ɍ, $\mathbb{C}, \mathbb{Z}_7, \mathbb{Z}_{19}$ are the trivial examples of Integral Domain.

b) We review that, if we understand then the ring of holomorphic functions(central object in Complex Analysis) on a domain such anontrivial example. It is an ID because zeros of holomorphic function are isolated and It has more units than the 1-function because every constant function is invertible.

C. Examples that not form ID:

a)$\mathbb{Z}_6$ Was not form anID as let 2,6∈ $\mathbb{Z}_6$ and 2.6≡0(mod6) but neither 2≠ 0 nor 6≠ 0

b)In $M_2(\mathrm{R})$ let $\begin{bmatrix} p & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & q \end{bmatrix}$ $\forall p, q \in \mathrm{R}$ and

$$\begin{bmatrix} p & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 \\ 0 & q \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

but neither $\begin{bmatrix} p & 0 \\ 0 & 0 \end{bmatrix} \neq 0 \quad nor \quad \begin{bmatrix} 0 & 0 \\ 0 & q \end{bmatrix} \neq 0$

so it does not form Integral Domain.

IX.PRIME AND IRREDUCIBLE ELEMENTS

Let R be a commutative Integral Domain with unity and $\mathrm{R}^* = \mathrm{R} - \{0\}$

A.Divisor: Let $p, q \in \mathrm{R}$ and $q \neq 0$. Then p divides q or p is divisor (or factor) of $q$and we are write it as

$$p/q \, \exists \, d \in R \; s.t. \; q = pd$$

B. Associates: Two elements $p, q \in \mathrm{R}^*$ are called associates if $\exists \; p \; unit \; v \in \mathrm{R} \; s.t. \; p = qv \;\; also \; q = pu \; where \; v^{-1} = u \; i.e. \; if \;\; p/q \; and \; q/p$

C. Irreducible element: Let p be non zero element of Integral Domain R with unity is called an irreducible element if:

1. p is non unit.

2. If$p = qd$ then either $q \; or \; d$ is must be unit i.e. in product both or atleast one is unit.

D. Prime element: An element $0 \neq \mathrm{R}$ of ID , R is called prime if

1. p is non unit in R 2. $p/lm \, ; l, m \in \mathrm{R} \; then \; either \;\; p/l \;\; or \;\; p/m$

E.Preposition:A prime is irrediucble element but not conversly.

Let p be a prime element in R. Take $p = lm$ .Then Obvious $p/l \;\; or \;\; p/m$. Take p/l .Then $l = pc$ for some $c \in \mathrm{R}$ .So $p = lm = pcm$, hence $1 = cm$ (by cancellation law hold as its ring).Thus either $c \; or \; m$ is unit .Take a unit in R .Hence p is irreducible element ,for the converse part we take an example $\mathbb{Z}[i\sqrt{3}]$ with the elements of the form $1 + i\sqrt{3}$.

X. EUCLIDEAN DOMAIN

In First property of *ID* a Division Algorithm is the basis of Euclidean algorithm We revise $\mathbb{Z}$ is *ED* but some other *ED* are Gaussian integers $\mathbb{Z}[i]$,the Eisentien integers $\mathbb{Z}[w]$ where w is primitive cube root of '*1*'and polynomial rings $P[x]$ over *P*. The Division Algorithm starts with an integer which is Dividend(a) non zero integer divisor(b),the quotient (q) and the remainder(r) such that

$$a = bq + r \;\; and \; 0 \leq r < b$$

By this equation we find GCD(greatest common divisor) as well as find that *GCD* is linear combination of them.

A. Definition of GCD: An element η in a commutative ring is a greatest common divisor of elements $\delta, \gamma \in \mathrm{R}$

η is common divisor ofδ, γ

If ρ is any other common divisor of δ, γ then ρ/η.

B. Definition of Euclidean Domain:A commutative Integral Domain with unity is called Euclidean Domains if there is a map defined by a function $\theta\colon \mathsf{S}^* \to \mathbb{Z}^+$ such that

- For every $a, b \in \mathsf{S}^* = \mathsf{S} - \{0\}, \;\; \theta(ab) \geq \theta(a)$
- For every $a \in \mathsf{S}^* = \mathsf{S} - \{0\} \Rightarrow \theta(a) \geq 0$
- For every $a \in \mathsf{S} \; and \; b \in \mathsf{S}^* \; and \; q, r \in \mathsf{S} \;\; s.t. \, a = bq + r \;\; with \; either \; r = 0 \; or \; \theta(a) < \theta(b)$

The map $\theta$is called the algorithm map and the second property is called Division Algorithm. The elements a, b, q, r Dividend , divisor, quotient and remainder respectively

C. Examples of Euclidean Domain:

- Any field F is ED. The algorithm map $\theta\colon \; F^* \to \mathbb{Z}^+$ i.e.$\theta(x) = 1 \; \forall x \in F^*$
- The ring of integers $\mathbb{Z}$ is Euclidean defined as$f(n) = |n|$.
- The ring of Gaussian integer$\mathbb{Z}[i]$ defined as$f(a + ib) = a^2 + b^2$.

D. The examples that not form ED

- The ring of integers of$\mathbb{Q}(\sqrt{-19})$, consisting of numbers of form $(a+b\sqrt{-19})/2$ where $a, b \in \mathbb{Z}$ (both even or odd).
- The ring $Ꞧ[xy]/\langle x^2+y^2+1\rangle$is not *ED*.

XI. PRINCIPAL IDEAL DOMAIN

Insecond property the ring of integers gives that every ideal in $\mathbb{Z}$ is generated by single elements i.e. all the non zero elements of ideal Ƙ is multiple of other element in Ƙ which is *GCD*. We revise every *PID* is *UFD* but converse is not possible i.e. $\mathbb{Z}[x]$(the ring of polynomial with integers coefficients)is *UFD* but generated by two elements 2 *and* x so not *PID*.

A. Definition of PID:-A commutative Integral Domain (i.e. Ring with unity also) Ꞧ is called *PID* if every element of Ꞧ is principal i.e. generated by one element.

B.Some Trivial and Non trivial examples are:

- The ring$2\mathbb{Z} = \langle 2\rangle$ is PID as its generated by single element
- First of all we discuss the definition of Class group and Minkowski bound for Non Trivial example of PID.

C. Class Group: Let I_F the ring of integers of a number field F . The class group$I_F\ of\ F$ which is the group of fractional ideals modulo the subgroup of principal fractional ideals$\langle x\rangle\ for\ x \in F$.

D. Finiteness of Class Group:Let F be a number field .There is constant $\mathcal{C}_{r,s}$ that depends only on the number r, s of real and pairs of complex conjugate embeddings of F such that every ideal of class of $I_F$constants an integral ideal of norm at most $\mathcal{C}_{r,s}\sqrt{|l_f}$ |,where l_f =Disc(I_F) .The class group $\mathcal{C}_F\ of\ F$ is finite .One can choosesuch that every ideal class is contains an integral ideal of norm at most$\sqrt{|l_f|}\left(\frac{4}{\pi}\right)\frac{t!}{t^t}$The explicit bound in the theorm is so called *Minkowski bound.*

E.Non Trivial Example of PID:

- Let here $F = \mathbb{Q}[i]$. $Then\ t = 2, s = 1$ and $|l_f| = 4$so the Minkowski bound is $\sqrt{|4|\left(\frac{4}{\pi}\right)^1\frac{2!}{2^2}} = \frac{4}{\pi} < 2$

Thus every fractional ideal is equivalent to an ideal of norm 1 since 1 isonly ideal of norm1 , every ideal is principal. So if ideal is principal so it is principal ideal domain.

Now In generally, $\mathrm{R}(-19) = \mathbb{Z}[1+\sqrt{-19}]/2$ is an example of a PID with unity which is not Euclidean domain.

But the interestedreader is referred to *J.C.Wilson* a PID that is not ED given a caution about this.

Perhaps confusing $\mathrm{R}(-19)\ with\ \mathbb{Z}[\sqrt{-19}]$ is taken PID but not ED.This is not correct since $\mathbb{Z}[\sqrt{-19}]$ is not PID because the ring $\mathbb{Z}[i\sqrt{3}]$ is not UFD so not PID since the element $1+i\sqrt{3}$ is irreducible but not a prime

In similar way $\mathbb{Z}[\sqrt{-19}]$ is not UFD since $1+i\sqrt{19}$ is irreudicible but not a prime so not PID .

XII.UNIQUE FACTORISATION DOMAIN

The ring of integers hold this property which gives every integer can be written uniquely in product of primes but not all rings hold that every element in any ring can be factorise into particles and cannot claim for uniqueness.

A. Definition of UFD: A commutative Integral Domain R with unity is said to be Unique Factorisation Domain if

If every non zero non unit element can be expressed as finite products of irreducible factors.

The factorization in irreducible elements is unique upto order and associates i.e. if $z \in Ꞧ^* = Ꞧ - \{0\}$ is as

$$z = rx_1x_2x_3\cdots x_i = sy_1y_2y_3\cdots y_m$$

Where $r, s$are units, all $x's$ *and* $y's$ are irreducible .Then$i = m$ and each $x's$are associate to $y's$.

B. Examples:

- The ring of Integers $\mathbb{Z}\ is\ UFD$.
- Each commutative principal ideal ring with identity is also an Integral Domain is a UFD.
- Consider $\mathbb{C}$ (set of complex numbers), it's a field hence it is UFD. But if we consider a subring $\mathbb{Z}\sqrt{-5}$ then its not UFD as $9 = 3.3$and also$9 = (2+\sqrt{5})(2-\sqrt{5})$.

Hence the Factorization is not unique.

XIII. THEOREM:EVERY IRREDUCIBLE ELEMENT IS PRIME IN Ɍ.

A.If Ɍ is PID. Let z be an irreducible element in Ɍ and Ɍ is PID. We want to show that the element $z \in$ Ɍ is prime element in Ɍ. Considerz/pq , $p, q \in$ Ɍ. Assume$\nmid p$. Since Ɍ is PID,there exist $d \in$ Ɍ and $\langle z \rangle$ and $\langle\ p \rangle$are ideals of Ɍ i.e is generated by single element are z and p respectively so by algebra of ideals $\langle z \rangle + \langle p \rangle = \langle d \rangle$ as Ɍ is PID such that zɌ $+ p$Ɍ $= d$Ɍ so$\langle z \rangle + \langle p \rangle = \langle d \rangle \Rightarrow \langle z \rangle \subseteq \langle d \rangle \Rightarrow z = cd, c \in$ Ɍ $i.e. z \in d$Ɍ.
As z is irreducible so either c or d must be unit .Suppose c is unit. Then$z$Ɍ $= d$Ɍ ;so we have zɌ $+ p$Ɍ $= z$Ɍ .So, we get $p \in zR$ which gives z/p but this is contradiction to our supposition .Hence d must be unit. Then dɌ = Ɍ , so zɌ $+ p$Ɍ = Ɍ then $\exists\, r, s \in$ Ɍ such that $zr + ps = 1$ .Thus we have $zqr + pqs = q$. Hence z/q because z/pq .We getresult.
B.If Ɍ is UFDLet$z$ be an irreducible element in Ɍ and Ɍ is UFD.Let $p, q \in R^*$ be such that z/pq. We have to show that either z/p orz/q Since z/pq , $\exists\, d \in R^*$ such that $zd = pq$. As Ɍ is UFD, There exist units r, s and irreducibles $x_i, y_j : 1 \leq i \leq l$ and $1 \leq j \leq m$, $p = rx_1x_2 \cdots x_l$ and $q = sy_1y_2 \cdots y_m$ now we have $zd = pq = rsx_1x_2 \cdots x_ly_1y_2 \cdots y_m$
Since irreducibility occur in only one factorization .Hence z is associate of some
$x_i : 1 \leq i \leq l$ .Take $z\alpha = x_i$ for some unit then get
$p = rx_1x_2 \cdots x_l = rx_1x_2 \cdots x_{i-1}z\alpha r_{i+1} \cdots r_l$ .Therefore we get p/a as we proved.

XIV. THEOREM: AN EUCLIDEAN DOMAIN IS A PRINCIPAL IDEAL DOMAIN.

Let Ꝁ be a non zero ideal of an Euclidean domain Ɍ. If it has only the element which is $\{0\}$, then there's nothing to prove.
In either way, if it has an element$k \neq 0$ and because$\forall k \in$ Ꝁ , $1/k$. Then $\theta(k) \geq \theta(1)$(by definition) .Then the set$\theta(k)$ is non empty set of integers .So by the principal of well ordering of integers there exist a element $l \in$ Ꝁ such that $\theta(l)$is least in this set.
We claim that Ꝁ $= \langle l \rangle$ if $l \in$ Ꝁ,for proving the theorem. If$k \in$ Ꝁthen$k = lq + r$, for some $q, r \in$ Ꝁ, with either $r = 0$ or $\theta(\mathrm{r}) < \theta(l)$. Since $k \in$ Ꝁso is $ql \in$ Ꝁ and $k \in$ Ꝁ also holds. So, by the definition of an ideal, $k - lq = r \in$ Ꝁ .But we take choice of $\theta(l)$ is least , $\theta(\mathrm{r}) < \theta(l)$is impossible.So,$r = 0$ so $k = lq \Rightarrow$ such that k $\in \langle l \rangle$. $i.e.$ Ꝁ $=$ $\langle l \rangle$. Proved
Note: Before proving the next theorem we will revise some lemmas that are based of next theorem.
Lemma:Let $\mathbb{D}$be a Domain in which every$d \in D$, neither 0 nor a unit element is a product of irreducibles .Then D is UFD if and only if (x) is prime ideal in $D$for every irreducible element $x \in D^3$
Lemma: If $C$is a commutative ring and $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n \subseteq K_{n+1\ldots}$ is an ascending chain of ideals in C, then $I = \bigcup_{n \geq 1} K_n$ is an ideal in C(i.e. union of ideals is again an ideal in C)
Lemma: If R is a PID,then it has no infinite strictly ascending chain of ideals.$K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq \cdots K_{n-1} \subsetneq K_{n+1} \subsetneq \cdots$
Lemma: if R is a PID,every element $r \in$ Ɍ is neither 0 nor a unit,then r has a factorisation into irreducibles elements.

XV.THEOREM: EVERY PID IS UFD.

First we show that if Ɍ is a principal ideal ring then Ɍ cannot have any infinite properly ascending chain on ideals. Therefore, let x_1Ɍ $\subset x_2$Ɍ $\subset x_3$Ɍ $\subset \cdots$
be chain of ideals in Ɍ.Let Ꝁ $= \cup\, x_i$Ɍ and $x, y \in$ Ꝁ, $r \in$ Ɍ .Then $x \in x_i$Ɍ, $y \in x_j$Ɍ for $some$ i, j. Because either x_iɌ $\subset x_j$Ɍ or x_jɌ $\subset x_i$Ɍ lie in one of the two ideals x_iɌ, x_jɌ, say in x_iɌ Then $x - y \in x_i$Ɍ $\subset$ Ꝁ $Also$ $ar \in$ x_iɌHence Ꝁ is an ideal in Ɍ because Ɍ is a principal ideal ring Ꝁ $= x$Ɍ for $some$ $x \in$ Ꝁ
Now $a \in$ Ɍ $\rightarrow a \in x_k$Ɍ for $some$ $k. Further,$
Ꝁ $= x$Ɍ $\subset x_k$Ɍ $\subset$ Ꝁ Hint that Ꝁ $= x$Ɍ $= x_k$Ɍ; Hence x_kɌ $= x_{k+1}$Ɍ $= \cdots$
Next, we show that each element $x \in$ Ɍ is a finite product of irreducible elements. If x is irreducible we are done. So let$x = bc$, where neither b nor c Is a unit? If both b and c are products of irreducible elements, we are done. So let b not be a product of irreducible elements, and write $b = rs$ $where$ r say, is not a products irreducible element this process leads to a properly ascending chain of ideals

$< x >\subset< b >\subset< r >\subset \cdots$That will continue indefinitely if x not a finite product of irreducible elements is. But since R cannot processes any infinite properly ascending chain of ideals we conclude that x must be a finite product of irreducible elements. To complete the proof that Ris a UFD we need to show that if p/xy where p is an irreducible element in R $and\ x, y \in$ R, $p/x\ or\ p/y$ which proves from the theorem that we are done previously that every irreducible element in PID is prime. Hence, the theorem is proved.

XVI.THE EUCLIDEAN ALGORITHM IN EUCLIDEAN DOMAINS

After proving that every$ED \Rightarrow PID$ and $\Rightarrow UFD$, therefore we find $ED \ \Rightarrow UFD$so we will revise at an example of Euclidean Algorithm in an ED other than $\mathbb{Z}$. The Euclidean Algorithm works as the same manner as that in integers. We will find the greatest common divisor and then extend this Euclidean Algorithm will construct the greatest common divisor as a linear combination of given original two elements.

To understand this there is an example from the polynomial ring $Q[y]$ .Let us find greatest common divisor of any two polynomials$p_1(y) = y^3 + y^2 + y + 1$and $p_2(y) = y^3 - y^2 + y - 1$.They have same degree so one of these is become to be a divisor , firstly we divide $p_1(y)$by$p_2(y)$,we can get the Quotient*1* and Remainder$p_3(y) = 2y^2 + 2$ and then divide $p_2(y)$ by $p_3(y)$ and this process is repeated until the remainder will become 0 which we get after some iterations

$$\begin{array}{cc} p_1(y) = y^3 + y^2 + y + 1 & p_1(y) = 1.p_2(y) + p_3(y) \\ p_2(y) = y^3 - y^2 + y - 1 & p_2(y) = \left({}^1\!/_2\, y\right)p_3(y) + p_4(y) \\ p_3(y) = 2y^2 + 2 & p_3(y) = 2p_4(y) + 0 \end{array}$$

$$p_4(y) = -y^2 - 1$$

Thus we get remainder 0 and then we find the greatest common divisor which is $p_4(y) = -y^2 - 1$ after that we can read these equations on the right in reverse order to find $p_4$as a linear combination of $p_1 \& p_2$.

$p_4(y) = p_2(y) - \left({}^1\!/_2\, y\right)p_3(y)$

$$p_4(y) = p_2(y) - \left({}^1\!/_2\, y\right)\left(p_1(y) - 1p_2(y)\right)$$

$$= -\left({}^1\!/_2\, y\right)p_1(y) + p_2(y)\left(1 - {}^1\!/_2\, y\right)$$

XVII.APPLICATION OF ED

A.Euclidean Domains and the **Gaussian Integers**: An Application

Some very important fact uses in Euclidean domains, in this we have look about the ring of Gaussian integers. This ring, is denoted by $\mathbb{Z}[i]$, which is defined as the set of all complex numbers $a + ib$ where both $a\ and\ b$ are integers as the field used in this ring is set of Integers. But before seen that any ring is an Euclidean domain, we must have to first define a $d-$function for this, Define a value for $d(a)$ satisfying the required properties. For the ring $Z[i]$, we seen that Given any $z \neq 0$ in $\mathbb{Z}[i]$, we define $d(z) to\ be\ |z|^2$, where by $|z|$, we mean the usual absolute value of the complex number z. So, if$a + ib \in \mathbb{Z}[i]$,we define $d(a + ib) = a^2 + b^2$. Clearly, for every non-zero element a of$\mathbb{Z}[i]$, $d(a)$ will be a non-negative integer.

We will find that this ring $\mathbb{Z}[i]$ is of *GAUSSIAN INTEGERS* become to be an Euclidean. It is an Application.

B.Euclidean Domain and the **Eisenstein integers**: An Application

As above we revise the basis for *Gaussian integers* is 1and i as similar the basis for *Eisenstein integers* consist of 1and ω where $\omega = \frac{(-1+i\sqrt{3})}{2}$ is a primitive cube root of unity .The equation $y^2 + y + 1$ has three roots $1, \omega\ and\ \omega^2$ .The *Eisenstein integers* is a triangular mesh which is $1 + \omega + \ \omega^2 = 0$ .The six sixth roots of unity in *Eisenstein integers 1* itself, primitive sixth roots $\omega - 1, -\omega$ .the primitive cube root is ω, primitive square root is *-1*.

As like Gaussian integers the *Eisenstein integers* are Euclidean.It is an Application.

XVIII.Application of UFD

A. Application: Polynomial rings

The application of Unique Factorization Domain will be a polynomial rings in one variable with coefficients in any field (or division ring more generally). Let ⍰ be a Division ring and let $\mathrm{R} = ⍰[x]$ denote the polynomial ring with coefficients in ⍰ . We review that since ⍰ is in particular an Integral ring, then $⍰[x]$ is also an integral ring and there is a degree map $d: \mathrm{R}^* \rightarrow \mathrm{N}$ which satisfies $d(pq) = d(p) + d(q)$for $p, q \in \mathrm{R}^*$. Herethis degree map is additive. Notice that any additive degree map satisfies first condition of a Euclidean ring as

$$d(pq) = d(p) + d(q) \leq min\big(d(p), d(q)\big)\ as\ d(p), d(q) \in \mathrm{N}$$

XIX.Application of PID

A. Application:Smith Normal form

The Smith Normal form is a normal form of Matrix with entries from Principal Ideal Domain with unity P.Two$r \times s$ matrices $\mathbb{M}\ and\ \mathbb{L}$ over Principal ideal domain P are in Smith Normal form if ∃two invertible matrices $Q \in P_r$ and $R \in P_s$ will be $\mathbb{L} = Q\mathbb{M}R$ is equivalent to a matrix in Diagonal form.

XX. CONCLUSION

It is concluded that in Ring theory the Rings, Ideals and Domains are very useful concepts for defining ED, PID and UFD. What is the relation in between them which is very useful to study the concept of all these. Euclidean Domain generalizes the concept of Gaussiansintegers, Eisenstein Integers. The Smith Normal form defined over PID that are very useful to find rank of Matrix and lastly UFD defined by Polynomial rings in one variable.

REFERENCES

[1]C Musili,*Introduction to Rings and Modules,* Second Revised Addition(1994),Narosa Publishing House Pvt.Ltd, India
[2]P.B.Bhattacharya SK .Jain, S.R.Nagpaul,*Basic Abstract Algebra*, Second Addition(1995),Cambridge University Press, United Kingdom .
[3]Gilbert/Gilbert,Elements of Modern Algebra,7th edition,2009,2005 Brooks/Cole, Cengage Learning, USA.
[4]Joseph J.Rotman ,Advanced Modern Algebra, Ist edition(2002),Second printing(2003);Prentice Hall, Handcover 1040 pages .
[5]David Joyce Referenced by J.C.Wilson Math.Mg,46,34-8(1973), Introduction to Modern Algebra, Clark University, Version 1.2.7,5Dec 2017
[6]Shreejit Bandyopadhyay ,Euclidean Domain and the Gaussian Integers: An Application,July 28,2013.
[7] E.Weiss,MC, Grawhill, Algebraic Number Theory, Second Addition(1976),New York: Chelsea Pub.Co