“Introduction of Euclidean Domain”

Dr. Amrish Kumar Srivastav
Assistant Professor
Department of Mathematics
Araria College, Araria
Bihar, India
Email – amrish112233@gmail.com

Abstract

Euclidean domain is also known as Euclidean ring. It is an integral domain which is associated with at least one Euclidean function [1]. A non zero commutative ring in which of product two non zero element is non zero is known as integral domain. Integral domain is generalization of ring of integers [2]. In Euclidean domain we use Euclidean algorithm for calculating greatest common divisors of two elements. Greatest common divisors of two elements always exist and this can be represented in linear combination of these elements. Euclidean domain has ideals and every ideal of Euclidean domain is principal ideal [3]. Euclidean domain has property of unique factorization domain and every Euclidean domain is a unique factorization domain it means every non zero non unit element can be written as product of prime elements.

Key words: algorithm, ideal, trichotomy, polynomials

Introduction

In 1817, Rechard Dedekind defined the concept of the ring of integers of a number. He introduced the term “ideal” but did not use the term “ring” and concept of ring in general. Rechard Dedekind was a German mathematician who made important contribution to number theory and abstract algebra particularly in ring theory. The concept of group has its origin in set of mapping or permutations. On the other hand ring has its origin with set of integers. Ring is different from groups because it has two binary operations; these operation are normally known as addition and multiplication. Ring closely follows the pattern of groups. In ring theory, we especially study the structure of rings, their representation, modules and different special classes of rings such as integral domain, division ring, skew field, Euclidean domain, finite integral domain etc.

Concept

Let R be an integral domain.

A function d: $R \setminus \{0\} \to N$ □□$\{0\}$ is a Euclidean valuation of R if the following conditions are satisfied:

1- d (a) □ d(a b), □ a, b ∈ $R \setminus \{0\}$, and

2- For any a, b ∈R a, b □□□□∃□q, r ∈ R

Such that $a = b\,q + r$, where $r = 0$ or $d(r) < d(b)$

An integral domain with a Euclidean valuation is called a Euclidean domain.

Euclidean domains are so called because of the essential property of the division algorithm. This is the basis for the Euclidean algorithm for finding the greatest common divisors of any two non-zero elements in the domain. Now let us consider an example of such a domain.

Example: Show that Z is a Euclidean domain.

Solution: Define d: Z→ N □□$\{0\}$,such that

$d(n) = |n|$

Then, for any a, b ∈ $Z \setminus \{0\}$,

$d(a\,b) = |a\,b|$

$= |a|.|b|$

$d(a\,b) \geq |a|$ (since$|b|$ □1 for b □ 0)

$= d(a)$,

i.e., d (a) □ d(a b)

Further, the division algorithm in Z says that if a, b $\in$ Z, b □□0, then
$\exists$ q, r $\in$ Z such that
a = b q + r, where r = 0 or 0 < |r| < | b|,
i.e., a = b q + r, where r = 0 or d(r) < d(b)
Hence, d is a Euclidean valuation on Z, making Z a Euclidean domain.

Theorem: If R be a Euclidean domain with Euclidean valuation d. Then prove that, for any a $\in$R \{0},

$$d\,(a) = d(1)$$

iff a is a unit in R.

Proof: Let us first assume that a $\in$R \ {0} with d(a) = d(1)
By the division algorithm in R, $\exists$ q, r $\in$ R having condition
1 = a q + r, where the value of r = 0, if not, then
d(r) < d(a) = d(1)
Now, if r □ 0, d(r) = d (r.1) $\geq$ d (1)
Thus, d(r) < d (1), it is not possible.
Thus, the only possibility for r is r = 0
Therefore, 1 = a q, so that a is a unit.
Conversely, assume that a is a unit in R. Let b $\in$R such that
a b =1
Then d (a) □ d (a b) = d(1)
But we know that d(a) = d(a.1) $\geq$ d(1)
So, we must have, d(a) = d(1)

Theorem: Let R be a Euclidean domain, with Euclidean valuation d. Then every ideal I of R is a principal ideal, i.e., I = R a, for some a $\in$R

Proof: If I = {0}, then I = R a, where a = 0
So let us assume that I □□{0}. Then I \{0} is non-empty.
Consider the set {d (a): a $\in$ I \ {0}}
It has a minimal element, d (b), where b $\in$ I \ {0}
We will show that I = R b
Since b $\in$ I and I is an ideal of R,
R b $\subseteq$ I ………… (1)
Now take any a $\in$ I. Since I $\subseteq$ R and R is a Euclidean domain,
We can find q, r $\in$R with property,
a = b q + r, where the value of r = 0, if not, then or d(r) < d(b).
Now, b $\in$ I and b q $\in$ I, also a $\in$ I,
Therefore, r = a – b q $\in$ I
The way we have chosen d (b),
Where d(r) < d(b), which is not possible.
Therefore, r = 0, and hence, a = b q $\in$ R b
Thus, I $\subseteq$ R b …………. (2)
From (1) and (2), we get I = R b
Thus, every ideal I of a Euclidean domain R with Euclidean valuation d is principal, and is generated by a $\in$ I, where d(a) is a minimal element of the set {d(x) | x $\in$ I \ {0}}

Comment: Every Euclidean domain is a Principal integral domain, but the converse is not true. Thus, Z, F and F[x] are Principal integral main, for any field F.

Example: Show that C, with the Euclidean valuation d defined by d(a) = 1, □ a $\in$C \{0}, is a Euclidean domain.
Solution: It is given that d(a) = 1 □ a $\in$C \{0},
d(x) =1, For any a, b $\in$C \ {0},

d(a b) =1 = d(a)
Hence d(a) = d(a b), □ a, b ∈C \ {0}
Also, for any a, b ∈ C, b □ 0,
a = (a b^{-1}) b + 0
So, d trivially satisfies the second condition for a function to be a Euclidean valuation. Thus, C is a Euclidean domain.

Example: If we define the function
d: R[x] \{0}→ N □□{0} such that d(f (x)) = deg f (x)
Then we have to show that d is a Euclidean valuation on R[x], and hence, R[x] is a Euclidean domain. Is d, restricted to Z[x] \{0}, a Euclidean valuation? Why, or why not?
Solution: We know that,
deg (f (x) g(x)) = deg f (x) + deg g(x) □ f (x), g(x) ∈R [x] \{0}
We know that given f (x), g(x) ∈ R[x], g(x) □ 0, ∃ q (x) and r(x)
Such that f (x) = q(x) g(x) + r(x), with deg r(x) < deg g(x)
Hence d is a Euclidean valuation on R[x], and R[x] is a Euclidean domain.
d: Z[x] \ {0}→N□{0}: d(f (x)) = deg f (x) is not a Euclidean valuation, Since the division algorithm is not true within Z[x]. For example, given 3x and 2x in Z[x], there are no q(x) and r(x) such that 3x = 2x q(x) + r(x)

Example: Show that $< Z, +, .>$, the ring of integers is a Euclidean domain.
Solution: For any $0 \neq a \in \mathbb{Z}$, we define $d\ (a\ )= |a\ |$(the absolute value of a).
Then $d(a) > 0$.
Let a, $b \in \mathbb{Z}$ such that $a \neq 0$, $b \neq 0$
Then $d(\ a\ )= |a|$, $d\ (a\ b\ )= |a\ b|= |a|\ \ |b|$
As $|a| \leq |a|\ |b\ |= |ab|$
$\Rightarrow d\ (a) \leq d\ (ab)$, for every $0 \neq a$, $0 \neq b$, a, $b \in \mathbb{Z}$
Again, let a, $b \in \mathbb{Z}$ such that $b \neq 0$
Case1: Suppose if $b > 0$
By division algorithm in $\mathbb{Z}$, there exists t, $r \in \mathbb{Z}$ such that
$a = b\ t + r$ where $0 \leq r < b$
If $r = 0$, then we get result.
If $r \neq 0$, then as $0 < r < b$
$\Rightarrow |r| < |b\ |$
$\Rightarrow d(r) < d(b)$
Case2: Suppose if $b < 0$, then $-b > 0$.
Applying division algorithm to a and $-b$, we obtain
$a = -b\ t + r$, where $0 \leq r < (-b)$ and r, $t \in \mathbb{Z}$.
$\Rightarrow a = -t\ b + r, -t, r \in \mathbb{Z}$.
If $r = 0$, then get result.
If $r \neq 0$, as $0 < r < (-b)$.
$\Rightarrow |r| < |-b|= |b|$.
$\Rightarrow d(r) < d(b)$.
Hence, $< Z, +, . >$ is a Euclidean domain.

Example: The ring of Gaussian integers given by

$$\mathbb{Z}\ i = a + ib : a,\ b \in \mathbb{Z}$$

is an Euclidean domain[4].

Solution: We know that $\mathbb{Z}\ i$ is an integral domain.
For $0 \neq a + ib \in \mathbb{Z}\ i$, we define $d\ a + ib = a^2 + b^2$.
Then $d(a + ib)$ is a non-negative integer because
If $0 \neq a + ib \in \mathbb{Z}\ i$, then either $0 \neq a$ or $0 \neq b$

In any case $a^2 + b^2 > 0$

(i) -Let $0 \neq x = a + ib$, $0 \neq y = c + id \in \mathbb{Z}\, i$ be arbitrary.

Then $d\ xy = d(\ a + ib\ c + id\ )$

$= d(\ (ac - bd\ ) + i\ (ad + bc\ ))$

$= (ac – bd)^{\ 2} + (ad + bc)^{\ 2}$

$= (a^2 + b^2)\ (c^2 + d^2)$

$= d\ (x)\ d(\ y\ )$ …………(1)

As $y \neq 0 \Rightarrow d\ (y) > 0$

$\Rightarrow d\ (y) \geq 1$ (as $d(y)$ is an integer.)

$\Rightarrow d\ (x)\ d(y) \geq d(x)$.

Therefore, $d\ (x) \leq d\ (x)\ d(\ y\ )= d(xy)$

(ii) - Step1: Let $x \in \mathbb{Z}\, i$ be a positive integer.

Then $x = n + i0$, where $n \in \mathbb{Z}_+$

Let $0 \neq y = a + ib \in \mathbb{Z}\, i$ be arbitrary.

Now we show that there exists $t, r \in \mathbb{Z}\, i$ such that $y = nt + r$ where $r = 0$ or $d(r) < d(x)$.

Applying Division algorithm to integers a, n and b, n.

We obtain,

$a = un + r_1$, $0 \leq r_1 < n$, where $r_1 \in \mathbb{Z}$ and

$b = vn + r_2$, $0 \leq\ r_2 < n$, where $r_2 \in \mathbb{Z}$

As r_1 and $n/2$ are two real numbers, therefore by law of trichotomy either $r_1 \leq n/2$ or $r_1 > n/2$

If $r_1 > n/2$, then $-r_1 < -n/2$

$\Rightarrow n - r_1 < n - n/2$

$\Rightarrow n - r_1 < n/2$

As $a = un + r_1$

$\Rightarrow a = un + n - n + a + r_1$

$= n\ u + 1 - (n - r_1)$

$= nq + k_1$, where $q = n\ (u + 1)$ and $k_1 = -(n - r_1\ )$

We know that $r_1 < n$ which implies that $n - r_1 > 0$

$\Rightarrow -\ (n - r_1) = n - r_1 < n/2$

If $r_1 \leq n/2$

Then, $a = un + r_1$ where $r_1 \leq n/2$

Thus in either case, we have $a = un + k_1$, where $k_1 < n/2$

Similarly, for $b = vn + r_{2,}$ we can find an integer k_2 such that

$b = vn + k_2$, where $k_2 < n/2$

Therefore, $y = a + ib$

$= un + k_1 + i(vn + k_2)$.

$= tn + r$,

Where $t = u + iv$ and $r = k_1 + i\ k_2 \in \mathbb{Z}_{[i]}$

As k_1 and k_2 can be zero also. It follows that either $r = 0$ or

$d\ r = d\ k_1 + i\ k_2$

$= {k_1}^2 + {k_2}^2$

$\leq \mathrm{n}^2/4 + \mathrm{n}^2/4 = n^2/2$

$< n^2 + 0^2$

$d\ r = d(n + i0)$

$= d(x)$

Thus, we obtain that $y = nt + r$, where either $r = 0$ or $d(r) < d(x)$

Step2: Let $0 \neq x, y \in \mathbb{Z}_{[i]}$

Let x' denotes the conjugate of x, then $x'x$ is a positive integer.

Let $x' = n$, $n \in \mathbb{Z}_+$

As $yx \in \mathbb{Z}_{[i]}$ and n is a positive integer. Applying step1 to yx' and n, there exists $t, r \in \mathbb{Z}_{[i]}$
$yx' = tn + r$ where either $r = 0$ or $d(r) < d(n)$ …….. (2)
If $r = 0$, then $yx = tn = txx$
$\Rightarrow y = tx + 0$ (as $x \neq 0 \Rightarrow x' \neq 0$ and cancellation law holds in an integral domain).
If $d(r) < d(n)$
From (2), we have $r = yx' - tn$.
$\Rightarrow d(\ yx - tn\ )< d\ (xx')$.
$\Rightarrow d\ (yx' - txx') < d\ x\ d(x'\ )$ (using (1))
$\Rightarrow d(x'\ (y - tx)) < d\ x\ d(x'\ )$
$\Rightarrow d\ (x'\ )d(y - tx) < d\ x\ d(x'\ )$
$\Rightarrow d(y - tx) < d\ x$
Let $-tx = r_0$, then $d(\ r_0) < d(x)$
Thus, $y = tx + r_0$, where either $r_0 = 0$ or $d(\ r_0) < d(x)$
Hence, $\mathbb{Z}_{[i]}$ is a Euclidean Domain.

Theorem: Prove that if F is a field, then polynomial function $F[x]$ will be an Euclidean domain.
Proof: Let F be a field.
For $0 \neq f(x) \in F[x]$, define $d(\ f\ (x)) = \deg f(x)$
Then $d(f\ (x\ ))$ is a non-negative integer.
As F is a field, therefore $F[x]$ is an integral domain with unity.
(i)- For $0 \neq f(x)$, $0 \neq g(x) \in F[x]$ be arbitrary.
$\deg (f\ (x)\ g\ (x)) = \deg f(\ x\ )+ \deg g(x)$
$\Rightarrow \deg f(x) < \deg (f\ (x)\ g\ (x)) - \deg g(x) \leq \deg (f\ (x)\ g\ (x))$
$\Rightarrow d(f\ x\ ) \leq d(f\ x\ g\ x\ )$
(ii)- Let $f(x)$, $g(x) \in F[x]$ and $g(x) \neq 0$
Applying Division algorithm to $f\ (x)$, $g(x)$ in $F[x]$, there exists unique polynomials $q(x)$, $r(x) \in F[x]$ such that,
$f(\ x) = g(\ x\ )q(\ x\ )+ r(x)$, where either $r\ x = 0$ or
$\deg r\ (x\ ) < \deg g(x)$
$\Rightarrow f(\ x\ )= g\ (x\ )q\ (x\ )+ r(x)$, where either $r\ x = 0$ or
$d(\ f\ (x\ ))< d(g\ (x\ ))$
Hence, $F[x]$ is a Euclidean domain.

Conclusion

For being Euclidean domains, it is the essential property to hold the division algorithm. This is the basis for the Euclidean algorithm for finding the greatest common divisors of any two non-zero elements in the domain. Every Euclidean domain is a Principal integral domain, but the converse is not true [5]. Thus, Z, F and F[x] are Principal integral domain, for any field F. if F is a field, then polynomial function $F[x]$ will be an Euclidean domain. The ring of Gaussian integers is a Euclidean domain.

REFERENCES

1- ROGERS, KENNETH (1971),"*THE AXIOMS FOR EUCLIDEAN DOMAINS*",
AMERICAN MATHEMATICAL MONTHLY, JSTOR 2316324.

2- SAMUEL, PIERRE (1 OCTOBER 1971)."*ABOUT EUCLIDEAN RING"* JOURNAL OF ALGEBRA. DOI:
10.1016/0021-8693(71)90110-4.
ISSN 0021-8693

3- Motzkin, T., *The Euclidean algorithm*, Bull. Amer. Math. Soc. 55 (1949) pp. 1142–1146.

4- Harper, Malcolm; Murty, M. Ram (2004), "*Euclidean rings of algebraic integers*" (PDF), Canadian Journal of Mathematics,
doi:10.4153/CJM-2004-004-5

5- Campoli, Oscar A., *A principal ideal domain that is not a Euclidean domain*, Amer. Math. Monthly 95 (1988) pp. 868–871