Abstract Algebra

EUCLIDEAN RINGS OR EUCLIDEAN DOMAIN

Definition Let R be an integral domain. Then this integral domain R is said to be a Euclidean ring if for every non-zero element $a \in R$ there exists a non-negative integer $d(a)$ such that

(i) for all non-zero elements $a, b \in R$ $d(a) \leq d(ab)$ or $d(b) \leq d(ab)$

(ii) for each $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$.

Note:-

(i) The second property of above definition is known as divison algorithm

(ii) d is called the Euclidean valuation or Euclidean norm function.

(iii) we do not assign a value to $d(0)$.

(iv) The ring I of all integers is an Euclidean ring.

(v) The ring of Gaussian integers is a Euclidean ring.

(v) Every field is an Euclidean ring.

Property of Euclidean Rings

(i) Every Euclidean ring is a principal ideal ring.

(ii) A Euclidean ring possesses a unit element.

(iii) Let R be a Euclidean ring. Then any two non-zero elements a and b in R have a greatest Common divisor d. Moreover, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

(iv) The necessary and sufficient Condition that the non-zero element a in the Euclidean ring R is a unit is that $d(a) = d(1)$.

Unique Factorization Theorem

Let R be a Euclidean ring and $a \neq 0$ a non unit in R. Suppose

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

where each p_i and q_j are prime elements of R. Then $m = n$ and each p_i $(1 \leq i \leq m)$ is an associate of some q_j $(1 \leq j \leq n)$ and each q_j is an associate of some p_i.

Proof :- Since we have

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \quad \text{---} (1)$$

Also $p_1 \mid p_1 p_2 \cdots p_m \Rightarrow p_1 \mid q_1 q_2 \cdots q_n$ [from (1)]

$\Rightarrow p_1$ must divide at least one of $q_1, q_2, \ldots q_n$. Now R is a Commutative ring, without loss of generality we may assume that $p_1 \mid p_1 q_1$. But p_1 and q_1 are both prime elements of R, so p_1 and q_1 must be associates. Therefore, $q_1 = u_1 p_1$ where u_1 is a unit in R.

Thus we have

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

$$= (u_1 p_1) q_2 \cdots q_n = p_1 u_1 q_2 \cdots q_n$$

($\because R$ is Commutative)

Now by left Cancellation law, we have

$$p_1 p_2 \cdots p_m = u_1 q_2 q_3 \cdots q_n$$

Repeat the above argument on (2) with p_2, p_3 and so on

In Case $m < n$, after m steps the left side becomes 1 and the right side reduces to a product of some units in R and certain numbers of q_j's, but q_i's are not units in R, so that the product of some units are some q_j's Cannot be equal to 1. which shows that $m \nless n$.

Therefore, we obtain $m \geq n$ ——— (3)

Now interchanging the roles of p_i's and q_j's, we get

$n \geq m$ ——— (4)

From (3) and (4) we obtain $m = n$.

In above process, we have also showed that every p_i has some q_j as an associate and Conversely.