Q. Define Euclidean ring.

Ans. Let $(R,+,\cdot)$ be an integral domain then R is said to be Euclidean ring if for every $0 \neq a \in R$ we can assign a non-negative integer $d(a)$ such that

(1) For all $0 \neq a, 0 \neq b \in R$, $d(ab) \geq d(a)$.

(2) For any $a, b \in R$ where $0 \neq b$, there exist q and $r \in R$ such that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$.

Example. (1) Show the ring of integers is a Euclidean ring.

Solution. Let $(I,+,\cdot)$ be an integral domain

Define a function

$$d: I \longrightarrow I^+ \cup \{0\} \text{ such that}$$
$$d(a) = |a|, \ \forall a \in I.$$

Let $0 \neq a, 0 \neq b \in I \Rightarrow d(ab) = |ab|$

$\Rightarrow |ab| \geq |a|$ [$\because |b| \geq 1$ if $0 \neq b$]

$\Rightarrow d(ab) \geq d(a)$

so first property is satisfied

Again Let $a \in I, 0 \neq b \in I$ by division algorithm

$\exists q \in I, r \in I$ such that

$a = bq + r$ where $0 \leq r < b$.

or $0 \leq r < |b|$

$\Rightarrow r = 0$ or $1 \leq r < |b|$

$\Rightarrow$ Either $r = 0$ or $d(r) < d(b)$

ii $(I,+,\cdot)$ is a Euclidean ring.

(2) The ring of polynomials over a field is a Euclidean ring.

Sol. Let $\{F(x),+,\cdot\}$ be a polynomial domain over the field F.

Let $0 \neq f(x) \in F(x)$

Let $d[f(x)] = \deg f(x)$, [$\because \deg f(x) \geq 0$]

Let $0 \neq g(x) \in F(x)$ then

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$$

$$\Rightarrow \deg[f(x)g(x)] \geq \deg f(x) \quad [\because \deg g(x) \geq 0]$$

Finally $f(x) \in F(x)$, $0 \neq g(x) \in F(x)$ then by division algorithm $\exists\ q(x) \in F(x)$, $r(x) \in F(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

i.e $d(r(x)) < d(g(x))$

∴ the ring of polynomials over a field is a Euclidean ring.

(3) Every field is a Euclidean ring.

Sol Let $(F, +, \cdot)$ be a field

Let $0 \neq a \in F$ define $d(a) = 0$, $\forall\ 0 \neq a \in F$.

then $d(ab) \geq d(a)$ $\quad [\because 0 \neq a \in F \Rightarrow d(a) = 0$
$0 \neq b \in F \Rightarrow d(b) = 0$
$\therefore d(ab) = 0 = d(a)]$

Finally if $a \in F$, $0 \neq b \in F \Rightarrow$ by division algorithm $\exists\ q \in F$, $r \in F$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

In a field. Take $r = 0$

$$a = bq \Rightarrow q = b^{-1}a \text{ i.e } a = (b)(b^{-1}a) + 0$$

∴ Hence every field is a Euclidean ring.

Q. The ring of Gaussian integers is a Euclidean ring, prove it.

Ans. Let $(G,+,\cdot)$ be the ring of Gaussian integers

then $G = \{(a+ib) \mid a, b \in \text{Integers}\}$ — I

Define d function as

$$d(x+iy) = x^2+y^2, \quad \forall\ (0+i0) \neq (x+iy) \in G$$

Now

Let $0 \neq (x+iy),\ 0 \neq (m+in) \in G$

then $d[(x+iy)(m+in)] = d[(xm-yn)+i(my+nx)]$

$$= (xm-yn)^2+(my+nx)^2$$

$$= (x^2+y^2)(m^2+n^2)$$

$$\Rightarrow d[(x+iy)(m+in)] = (x^2+y^2)(m^2+n^2) > (x^2+y^2)$$

$$\geq d(x+iy)$$

so first condition is satisfied,

To prove second condition

Let $\alpha \in G,\ 0 \neq \beta \in G \Rightarrow \alpha = x+iy,\ \beta = m+in$

$$\lambda = \frac{\alpha}{\beta} = \frac{x+iy}{m+in} = \frac{(x+iy)(m-in)}{m^2+n^2} = \frac{(xm+yn)+i(ym-nx)}{m^2+n^2}$$

$$\lambda = \frac{\alpha}{\beta} = p+iq, \quad p = \frac{xm+yn}{m^2+n^2}, \quad q = \frac{ym-nx}{m^2+n^2}$$

Here p and q are rational no

so $\lambda \notin G$

Let p' and q' be the nearest integers to p and q respectively

then $|p-p'| \leq \frac{1}{2}$ and $|q-q'| \leq \frac{1}{2}$

Let $\lambda' = p'+iq'$ then $\lambda' \in G$

Now $\lambda = \frac{\alpha}{\beta} \Rightarrow \alpha = \lambda\beta + \lambda'\beta - \lambda'\beta$

Thus $\alpha = \lambda'\beta + (\lambda-\lambda')\beta$ ——— (1)

Since $\alpha \in I \Rightarrow \lambda'\beta \in I$, $(\lambda - \lambda')\beta \in I$

[$\because$ Integer = Integer + Integer]

Now We shall show

Either
(1) $(\lambda - \lambda')\beta = 0$ or (2) $d[(\lambda - \lambda')\beta] \leq d(\beta)$

(i) If p and $q \in I \Rightarrow p = p'$ and $q = q'$

$\because \lambda - \lambda' = (p + iq) - (p' + iq') = (p - p') + i(q - q') = 0 + i0 = 0$

so (1) is proved

(ii) If p and q are not both integers then

$$d[(\lambda - \lambda')\beta] = d[\{(p - p') + i(q - q')\}\{m + in\}]$$

$$= \{(p - p')^2 + (q - q')^2\}\{m^2 + n^2\}$$

$$\leq \left(\frac{1}{4} + \frac{1}{4}\right) \cdot d(\beta) \quad [d(\beta) = m^2 + n^2]$$

$$\leq \frac{1}{2} d(\beta) < d(\beta)$$

$$< d(\beta)$$

Thus $\alpha = \lambda'\beta + (\lambda - \lambda')\beta$ where $d[(\lambda - \lambda')\beta] < d(\beta)$.

Hence $(Q, +, \cdot)$ is a Euclidean ring.

Theorem. Every Euclidean ring is a principal ideal ring.

Proof. Let $(R,+,\cdot)$ be a Euclidean ring.

Let S be an ideal of R Then two cases arise

(1) $S=(0)$ (2) $S\neq(0)$

Case (1) if $S=(0) \Rightarrow$ S is a principal ideal

Case (2) if $S\neq(0] \Rightarrow \exists\ 0\neq b\in S$ such that $d(b)$ is minimum.

i.e. there exist no $c\in S$ such that $d(c) < d(b)$.

To show $S=(b)$ [S will be generated by b, $b\in S$]

Let $a\in S$, $0\neq b\in S$ Then by division algorithm $\exists\ q\in R, r\in R$ such that

$$a = bq + r \quad \text{where either } r=0 \text{ or } d(r)<d(b) \quad \text{--- (1)}$$

let $q\in R, b\in S \Rightarrow bq\in S$

$\Rightarrow -bq\in S$

Now $a\in S, -bq\in S \Rightarrow (a-bq)\in S$ [$\because$ S is a subgroup]

$\Rightarrow r\in S$ [$\because (a-bq)=r$]

Since $d(r) < d(b)$ & $d(b)$ is minimum

so r must be zero

So put $r=0$ in (1)

$a = bq$

$\Rightarrow a =$ multiple of b

i.e. $S = (b)$ [$\because a\in S$]

$\Rightarrow$ S is a principal ideal generated by 1 element

Also S was arbitrary so every ideal is principal ideal.

Hence $(R,+,\cdot)$ is a principal ideal ring.

Theorem. Every Euclidean ring possesses unity element.

Proof. Let $(R,+,\cdot)$ be a Euclidean ring

$\Rightarrow (R,+,\cdot)$ be Euclidean principal ideal ring generated by u_0 where $u_0\in R$

$\Rightarrow$ Elements of R will be multiple of u_0.

$R = \{ u_0, u_0 r_1, u_0 r_2, u_0 r_3, u_0 r_3 \cdots \}$

Since $u_0 \in R$, $u_0 r_i \in R$ for some i

$\Rightarrow u_0 = u_0 r_i \Rightarrow r_i$ is unity

ii R has unity element.

Theorem. Let R be a Euclidean ring and a and b be any two elements in R, not both of which are zero. Then a and b have a g.c.d. divisor d such that

$d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Proof. Let $(R, +, \cdot)$ be a Euclidean ring

Let $0 \neq a, 0 \neq b \in R$

Let us claim

$S = \{ sa + tb \mid s, t \in R \}$

Let $\alpha \in S \rightarrow \alpha = s_1 a + t_1 b$, $s_1, t_1 \in R$

$\beta \in S \Rightarrow \beta = s_2 a + t_2 b$, $s_2, t_2 \in R$

$\Rightarrow (\alpha - \beta) = [(s_1 - s_2) a + (t_1 - t_2) b]$

$\Rightarrow (\alpha - \beta) \in S$ as $(s_1 - s_2), (t_1 - t_2) \in R$

Again

Let $r \in R$, $\alpha \in S \Rightarrow \alpha = s_1 a + t_1 b$, $s_1, t_1 \in R$

$r\alpha = r[s_1 a + t_1 b]$

$r\alpha = (rs_1) a + (rt_1) b$

$\Rightarrow r\alpha \in S$ as $rs_1, rt_1 \in R$

ii $(S, +, \cdot)$ is an ideal in R

$\Rightarrow$ S is a principal ideal as $(R, +, \cdot)$ is principal ideal ring

$\Rightarrow \exists\ d \in S$ s.t.

$S = (d) \Rightarrow$ Elelements of S will be multiple of d

$\Rightarrow \exists\ \lambda, \mu \in R$ such that

$d = \lambda a + \mu b$ ——— (1)

~~Now put $s=1, t=0$ in~~

Let $sa+tb \in S$

put $s=1, t=0$

$\Rightarrow 1.a+0.b \in S \Rightarrow a \in S \Rightarrow a =$ multiple of d

$\Rightarrow d \mid a$ —— (2)

Again, take $s=0, t=1$

$0.a+1.b \in S \Rightarrow b \in S \Rightarrow b =$ multiple of d

$\Rightarrow d \mid b$ —— (3)

Let $c \mid a \Rightarrow c \mid \lambda a$ —— (4)

$c \mid b \Rightarrow c \mid \mu b$ —— (5)

(4) & (5) $\Rightarrow$

$c \mid (\lambda a + \mu b)$

$\Rightarrow c \mid d$ [$\because d = \lambda a + \mu b$]

$\therefore$ d is g.c.d of a & b such that $d = \lambda a + \mu b$, proved.

Theorem. Let $(R, +, \cdot)$ be a Euclidean ring

Let $a, b, c \in R$. Let g.c.d of a & b is one

Let $a \mid bc$ to prove $a \mid c$

Proof. Let $(R, +, \cdot)$ be a Euclidean ring

Let g.c.d of a & b is 1

$\Rightarrow 1 = \lambda a + \mu b$ —— (1)

Given $a \mid bc \Rightarrow \exists\, k_1 \in R$ such that

$bc = ak_1$ —— (2)

To prove $a \mid c$

multiplying (1) by c we have

$c = \lambda ac + \mu bc$

$c = \lambda ac + \mu [ak_1]$ from (2)

$\Rightarrow c = a[\lambda c + \mu k_1]$

$\Rightarrow a \mid c$, proved.

Corr. In a Euclidean ring R, if $p \in R$, is a prime & $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Algebra, CH-05 (08) Euclidean ring Dr Satish Kumar

Let R be a Euclidean ring. Let $0 \neq a, 0 \neq b \in R$ then

(i) if b is a unit in R then $d(ab) = d(a)$

(ii) if b is not a unit in R then $d(ab) > d(a)$.

Proof. Let $(R, +, \cdot)$ be a Euclidean ring

Let $0 \neq a, 0 \neq b \in R$

Suppose b is a unit in R

To prove $d(ab) = d(a)$

By definition of Euclidean ring

$$d(ab) \geq d(a) \quad \text{---(1)}$$

It is given b is a unit in $R \Rightarrow b$ is invertible $\Rightarrow b^{-1}$ exists

$\therefore$ we can write

$$a = (ab)b^{-1}$$

$\therefore d(a) = d[(ab)b^{-1}] \geq d(ab)$ [$\because d(ab, a) \geq d(a)$]

$\therefore d(a) \geq d(ab)$ ---(2)

From (1) & (2)

$$d(ab) = d(a)$$

$\Rightarrow$ (i) part is proved

(ii) Suppose b is not unit in R

Now $0 \neq a, 0 \neq b \in R \Rightarrow ab \neq 0$ & $ab \in R$

Now $a \in R, 0 \neq ab \in R \Rightarrow$ by division algorithm

$\exists\ q \in R, r \in R$ such that

$a = (ab)q + r$, Either $r = 0$ or $d(r) < d(ab)$

Case(i) if $r = 0$ then $a = (ab)q \Rightarrow a[1 - bq] = 0$

$\Rightarrow bq = 1 \Rightarrow b$ is unit in R

$\Rightarrow$ We get contradiction

Case (ii) if $d(r) < d(ab)$

i.e $d(ab) > d(r)$ ——— (3)

$a = (ab)q + r$

$\Rightarrow r = a - abq$

$r = a(1 - bq)$

$\Rightarrow d(r) = d[a(1-bq)] \geq d(a)$

$\Rightarrow d(r) \geq d(a)$. ——— (4)

(3) & (4) $\Rightarrow$

$d(a) \leq d(r) < d(ab)$

$\Rightarrow d(a) < d(ab)$, proved.

Theorem. State and prove Unique factrisation theorem for Euclidean ring.

Statement. Let $(R, +, \cdot)$ be a Euclidean ring

Let $0 \neq a \in R$ then either a is unit

or $a = p_1 p_2 p_3 \cdots p_m$, where each p_i is prime

and this representation is unique without its order.

Proof. Let $(R, +, \cdot)$ be a Euclidean ring.

Let $0 \neq a \in R$

if a is unit we are nothing to prove. [$d(a) = d(1)$]

Suppose a is not unit. We shall prove this theorem by mathematical induction. suppose the theorem is true for all non zero element of R whose d value is less than d value of a. then we shall prove that the theorem is true for a also.

CH-05, Algebra (10) Euclidean ring, Dr Satish Kr

Suppose a is unit.

% ~~We have~~

$a = ba$

$\Rightarrow d(a) = d(1 \cdot a) \geq d(1)$

~~SPACE~~

% a is prime we are nothing to prove

% a is not prime $\Rightarrow \exists$ $b, c \in R$ such that

$a = bc$ where neither b is unit nor c is Unit. —— (1)

(i) b is not unit in R, ~~$c \in R$~~ $c \in R$

$\Rightarrow$ ~~$d(ab) > d(a)$~~ $d(bc) > d(c)$ —— (2)

(ii) c is not unit in R, ~~$b \in R$~~

~~$d(bc) > d(b)$~~ $d(bc) > d(b)$ —— (3)

put ~~$bc = a$~~ $bc = a$ in (2) & (3), we have

$d(a) > d(c)$ —— (4)

and $d(a) > d(b)$ —— (5)

(4) $\Rightarrow d(c) < d(a)$

$\Rightarrow c = \alpha_1 \alpha_2 \cdots \alpha_s$ (by hypothesis) —— (6)

(5) $\Rightarrow d(b) \geq d(a)$

$\Rightarrow b = \beta_1 \beta_2 \cdots \beta_t$ (by hypothesis) —— (7)

(6) & (7) $\Rightarrow$

$bc = (\beta_1 \beta_2 \cdots \beta_t)(\alpha_1 \alpha_2 \cdots \alpha_s)$

$\Rightarrow a = \beta_1 \beta_2 \cdots \beta_t \alpha_1 \alpha_2 \cdots \alpha_s$

, proved.

Uniqueness Suppose a has two different representations

$a = p_1 p_2 \cdots p_m$, each p_i is prime, $1 \leq i \leq m$ —— (8)

$b = q_1 q_2 \cdots q_n$, each q_j is prime, $1 \leq j \leq n$ —— (9)

to prove $m = n$

(8) & (9) $\Rightarrow$

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

Let $p_1 \mid p_1 p_2 \cdots p_m$

$\Rightarrow p_1 \mid q_1 q_2 \cdots q_n$ [$\because p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$]

$\Rightarrow p_1$ will divide atleast one q_i's

Let $p_1 \mid q_1 \Rightarrow q_1 = u_1 p_1$, u_1 is unit

$\therefore p_1 p_2 \cdots p_m = u_1 p_1 q_2 \cdots q_n$ — (10)

$p_2 p_3 \cdots p_m = u_1 q_2 \cdots q_n$ — (11)

Again let

$p_2 \mid p_2 p_3 \cdots p_m$

$\Rightarrow p_2 \mid u_1 q_2 q_3 \cdots q_n$ [$\because p_2 p_3 \cdots p_m = u_1 q_2 \cdots q_n$]

Suppose $p_2 \mid q_2 \Rightarrow q_2 = u_2 p_2$, u_2 is unit

$\therefore$ (11) $\Rightarrow$

$p_3 \cdots p_m = u_1 u_2 q_3 q_4 \cdots q_n$

$p_3 p_4 \cdots p_m = u_1 u_2 q_3 q_4 \cdots q_n$

suppose $m < n$

then after m steps we have

$1 = u_1 u_2 \cdots u_{m-1} \cdot q_{m+1} q_{m+2} \cdots q_n$

which is impossible as product of prime no can be equal to 1 — (12)

$\Rightarrow m \nless n \Rightarrow n \leq m$

Interchanging the role of m & n, we get

$m \leq n$ — (13)

(12) & (13) $\Rightarrow m = n$

$\therefore$ the representation is unique, proved.

Content of a polynomial

Let $(R(x), +, \cdot)$ be a polynomial domain
*whose R is unique factorisation domain
Let $f(x) = (a_0 + a_1 x + \cdots + a_n x^n) \in R(x)$
then content of f we mean the g.c.d of $(a_0, a_1, \cdots a_n)$.

Note if $\left.\begin{matrix} cf = c_1 \\ cf = c_2 \end{matrix}\right\} \Rightarrow c_1 = u c_2$, u is unit

ex Let $f(x) = 3x^3 - 5x^2 + 7$
then cf = content of f = g.c.d of $(3, 5, 7)$
$= 1$.

~~Primitive polynomial~~ [UFD]

* Note. An integral domain R with unity element is called unique factorization domain if for $0 \neq a \in R$
(1) Either a is unit or
(2) $a = p_1 p_2 \cdots p_n$, each p_i is prime and this representation is unique except for the order in which p_i occur.

Primitive polynomial. Let R be a UFD then a polynomial $f(x) = \{a_0 + a_1 x + \cdots + a_n x^n\} \in R(x)$ is said to be primitive if g.c.d of $\{a_0, a_1, \cdots, a_n\}$ is a unit in R.

Example (1) Any monic polynomial over R is primitive.
(2) the polynomial $(3x^3 - 5x^2 + 7)$ is primitive as g.c.d of $(3, 5, 7) = 1$
(3) Every irreducible polynomial of positive degree is primitive but every primitive polynomial need not be irreducible. ex $(x^2 + 5x + 6) \in I(x)$ is primitive but not irreducible as $x^2 + 5x + 6 = (x+2)(x+3)$.
(4) An irreducible polynomial of zero degree may not be primitive.