STUDY MATERIALS

(RING THEORY-II)

TOPIC: EUCLIDEAN DOMAIN

Mathematics Honours
Semester – 6

Paper – C14T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

Euclidean Domains:-

Any field F can be considered as a Euclidean domain with $v(a) = I$, $\forall a \neq 0$.

Because, $a = (ab^{-1})b + 0$. where $bb^{-1} = I$.

i.e., $a = q \cdot b + r$, where $q = ab^{-1} \in F$ and $r = 0$.

Also $v(a) \leq v(ab)$, $\forall a(\neq 0), b(\neq 0) \in F$.

Let R be a commutative ring with unity I. The following conditions are equivalent:-

(i) R is a field

(ii) $R[x]$ is a Euclidean domain

(iii) $R[x]$ is a PID.

PROOF: We have proved: If R is a field, then $R[x]$ is a Euclidean domain. $\therefore$ (i) $\Rightarrow$ (ii).

Also every Euclidean domain is a PID.

$\therefore$ (ii) $\Rightarrow$ (iii).

Now to prove: (iii) $\Rightarrow$ (i), i.e., if $R[x]$ is a PID then R is a field

For, let $a \in R$, $a \neq 0$, and I be the unity in R. Let us consider $U = \langle a, x \rangle$, the ideal of $R[x]$ generated by a and x.

Since $R[x]$ is a PID, $\exists f(x) \in R[x]$ s.t. $U = \langle f(x) \rangle$. So $a \in \langle f(x) \rangle$; $x \in \langle f(x) \rangle$

$\Rightarrow a = f(x) \cdot g(x)$; $x = f(x) \cdot h(x)$, for some $g(x), h(x) \in R[x]$.

$\therefore \deg(f(x)) = 0 \Rightarrow f(x) \in R$ and let $f(x) = b$.

Now $b \cdot h(x) = x \Rightarrow bc = I$ for some $c \in R$.

$\Rightarrow b$ is a unit in R and so $U = \langle b \rangle = R[x]$

We have $I \in U \Rightarrow I = af_1(x) + xf_2(x)$, for $f_1(x), f_2(x) \in R[x]$

$\Rightarrow I = d \cdot a$ for $d \in R \Rightarrow a$ is a unit in $R \Rightarrow R$ is a field.

Corollary :- $Z[x]$ is NOT a PID.

Since Z is a commutative ring with unity I, and Z is NOT a field, hence $Z[x]$ is NOT a PID.

Th. Let D be a E.D. with a Euclidean valuation v. Then (i) $v(I)$ is minimal among all $v(a)$, $\forall a(\neq 0)$ in D; (ii) an element $u \in D$ is a unit iff $v(u) = v(I)$.

Proof: (i) Let $a \in D$ and $a \neq 0$.

$\therefore v(a) = v(a.I) \geq v(I) \Rightarrow v(I)$ is minimal

(ii) Let u be a unit in D. Then $u^{-1} \in D$ and

$u.u^{-1} = I \Rightarrow v(I) = v(u.u^{-1}) \geq v(u)$.

Also we have from (i) $v(u) \geq v(I)$

$\therefore v(u) = v(I)$.

Conversely, let $v(u) = v(I)$, for $u \in D$, $I \in D$.

Then $\exists\, q, r \in D$ s.t. $I = u.q + r$; where either $r = 0$ or $v(r) < v(u)$.

Since $v(I) = v(u)$ is minimal, $\therefore v(r) \nless v(u)$.

$\therefore r = 0 \Rightarrow I = u.q \Rightarrow u$ is a unit in D.

Th. Let D be a E.D. and v be its Euclidean valuation. For $a \neq 0$, $b \neq 0$ in D, $v(a) < v(a.b)$ iff b is a non-unit in D.

We have $v(a.b) \geq v(a)$, $\forall a \neq 0, b \neq 0$ in D.

Let b be a unit in D. Then $b^{-1} \in D$ and

$v(a) = v(abb^{-1}) \geq v(ab) \geq v(a)$

$\Rightarrow v(a) = v(a.b)$

So contrapositively, $v(a) < v(ab) \Rightarrow b$ is non-unit.

Conversely, let b be a non-unit in D s.t. $a.b \neq 0$ in D. Then $\exists\, q$ and r in D s.t.

$a = (ab)q + r$ where either $r = 0$ or $v(r) < v(ab)$

$r = 0 \Rightarrow a - abq = 0 \Rightarrow I - bq = 0$ (Since $a \neq 0$) $\Rightarrow b.q = I$

$\Rightarrow b$ is a unit, a contradiction. So $r \neq 0$. And

$v(r) < v(a.b)$. $v(r) = v(a(1-bq)) \geq v(a) \Rightarrow v(a) < v(a.b)$.

(5) If d be a gcd of three elements a, b, c in a PID D, show that d can be expressed as $d = au + bv + cw$ for some u, v, w in D.

Let us consider the principal ideals $\langle a \rangle, \langle b \rangle$ and $\langle c \rangle$ in D.

$\langle a \rangle + \langle b \rangle + \langle c \rangle$ is also an ideal in D.

Since D is a PID, $\langle a \rangle + \langle b \rangle + \langle c \rangle = \langle d \rangle$ for some $d \in D$.

$\Rightarrow \langle a \rangle \subset \langle d \rangle, \langle b \rangle \subset \langle d \rangle, \langle c \rangle \subset \langle d \rangle$.

$\Rightarrow d | a$, $d | b$ and $d | c$

$\Rightarrow d$ is a common divisor of a, b, c.

Let q be another common divisor of a, b, c.

$\therefore q | a$, $q | b$ and $q | c$

$\Rightarrow \langle a \rangle \subset \langle q \rangle, \langle b \rangle \subset \langle q \rangle, \langle c \rangle \subset \langle q \rangle$

$\Rightarrow \langle a \rangle + \langle b \rangle + \langle c \rangle \subset \langle q \rangle$; Since $\langle a \rangle + \langle b \rangle + \langle c \rangle$ is the smallest ideal containing $\langle a \rangle, \langle b \rangle$ and $\langle c \rangle$.

i.e., $\langle d \rangle \subset \langle c \rangle \Rightarrow c | d$

$\therefore d$ is a gcd of a, b and c.

Now $\langle d \rangle = \langle a \rangle + \langle b \rangle + \langle c \rangle \Rightarrow d | a$, $d | b$ and $d | c$

$\Rightarrow d = au + bv + cw$ for some $u, v, w \in D$.

(6) Let D be a Euclidean domain with Euclidean valuation v. If b is a unit in D, prove that $v(ab) = v(a)$ for all non-zero $a \in D$.

By the property of v in the Euclidean domain D, we have $v(a) \leq v(ab)$ for all non-zero $a, b \in D$.

Since b is a unit, $b \neq 0$, and $b^{-1} \in D$ s.t. $bb^{-1} = 1$.

Hence $v(a) = v(abb^{-1}) = v((ab)b^{-1}) \geq v(ab)$

$\therefore v(a) \leq v(ab)$ & $v(a) \geq v(ab)$

$\Rightarrow v(ab) = v(a) \;\forall\; a (\neq 0) \in D$.

(8) Let D be a Euclidean domain with v. Prove that $v(1) < v(a)$ for all non-zero non units $a \in D$.

Let $a \in D$ be a non-zero & non-unit element.

$\therefore 1a \neq 0$ in D, as D contains no divisor of zero.

By Euclidean domain property, $\exists$ elements q & r in D s.t. $1 = (1a)q + r$, either $r = 0$ or $v(r) < v(1a)$.

$r = 0 \Rightarrow 1 - (1a)q = 0 \Rightarrow 1(1 - aq) = 0 \Rightarrow 1 - aq = 0$ in D, $(1 \neq 0)$

$\Rightarrow a$ is a unit, a contradiction.

Therefore, $r=0$ does not hold.

So $v(r) < v(1a)$.

But $v(r) = v[1(1-aq)] \geq v(1)$

$\therefore$ $v(1) < v(1a)$.

$\Rightarrow$ $\underline{v(1) < v(a)}$, $\forall$ non-zero non-units $a \in D$.

---

(11) (iii) Use Euclidean algorithm to find a gcd of the elements $a = 7+4i$, $b = 4+3i$ in $\mathbb{Z}[i]$ with a Euclidean valuation v defined by $v(m+ni) = m^2+n^2$. If d be a gcd, express d as $d = au+bv$ for some $u, v \in \mathbb{Z}[i]$.

$$\frac{7+4i}{4+3i} = \frac{(7+4i)(4-3i)}{(4+3i)(4-3i)} = \frac{40-5i}{25} = \frac{8-i}{5}$$

$$= (2+0i) - \left(\frac{2}{5}+\frac{1}{5}i\right)$$

a, $7+4i = 2(4+3i) - (4+3i)\left(\frac{2}{5}+\frac{1}{5}i\right)$

$= 2(4+3i) - (1+2i) = q(4+3i) + r$;

where $q = 2 \in \mathbb{Z}[i]$, $r = -1-2i \in \mathbb{Z}[i]$

and $v(r) = 5 < v(4+3i)$

Now $\frac{4+3i}{-1-2i} = \frac{(4+3i)(-1+2i)}{5} = \frac{-10+5i}{5} = -2+i$.

a, $4+3i = (-1-2i)(-2+i) = q_1(-1-2i) + r_1$;

where $q_1 = -2+i \in \mathbb{Z}[i]$, $r_1 = 0$.

The process terminates and $\underline{-1-2i \text{ is a gcd}}$.

We have, $7+4i = (4+3i)\cdot 2 + (-1-2i)$

a, $-1-2i = (7+4i)\cdot 1 + (4+3i)\cdot(-2)$.

$d = -1-2i = au + bv$, where $u=1$, $v=-2 \in \mathbb{Z}[i]$

Th: Let E be a E.D. and $a, b \in E$. If $a|b$, $b \neq 0$, and a is neither a unit nor an associate of b, then $v(a) < v(b)$.

Since a is not an associate of b, and $a|b$, then $b \nmid a$. Hence $a = b \cdot q + r$, for $q, r \in E$ and $r = 0$ or $v(r) < v(b)$.

Now $a|b \Rightarrow b = a \cdot c$ for some $c \in E$.

$\Rightarrow r = a - b \cdot q = a - ac \cdot q = a \cdot (1 - c \cdot q)$

If $r = 0$ and $1 - c \cdot q = 0 \Rightarrow c$ is a unit $\Rightarrow b$ is an associate of a [$\because b = a \cdot c$], which is a contradiction.

$\therefore 1 - c \cdot q \neq 0$ [$\because a \neq 0$] $\Rightarrow r \neq 0$, $\therefore v(r) = v(a(1 - c \cdot q)) \geq v(a)$

$\therefore v(b) > v(a)$. [$\because v(r) < v(b)$].