Corollary to Theorem 18.3

Let F be field. Then F[x] is U.F.D

Proof:- From theorem 16.3, We know that if F is field then F[x] is P.I.D
& From Theorem 18.3 (Prove it)
Every P.I.D is U.F.D
$\Rightarrow$ F[x] is U.F.D.

EUCLIDEAN DOMAINS (E.D)

An Integral Domain D is called Euclidean domain if $\exists$ a function d from non zero elements of D to non-negative Integers

i.e $\exists$ d : non zero elements $\longrightarrow$ non-ve integers of D

Such that:

(i) $d(a) \leq d(ab)$ $\forall$ non zero $a, b \in D$

(ii) If $a, b \in D$, $b \neq 0$ $\exists$ elements $q \& r$ in D such that

$a = bq + r$; $r = 0$ or $d(r) < d(b)$

Examples:- Prove that $\mathbb{Z}$ is E.D

Proof:- $\mathbb{Z}$ is Integral Domain

Define $d(a) = |a|$ $\forall a \in D$, $a \neq 0$

then $d(a) \geq 1$ $\forall a \in \mathbb{Z}$, $a \neq 0$

(1) $d(ab) = |ab| \geq |a| = d(a)$ $\forall a \neq 0, b \neq 0$ $a, b \in \mathbb{Z}$

(2) Let $a, b \in \mathbb{Z}$ & $b \neq 0$

Case-1 If $b > 0$, then by Division Algorithm $a = bq + r$ where $0 \leq r < b$ { $r \& b$ both are +ve }

So, if $r \neq 0$ then $d(r) = r < b = d(b)$

$\Rightarrow d(r) < d(b)$

Case-2 If $b<0$ then $-b>0$

$a=(-b)q+r$; $0\le r<-b$

$=(-q)b+r$; If $r\neq 0$ then

$d(r)=|r|<|b|=d(b)$

So $d(r)<d(b)$

So $\mathbb{Z}$ is E.D

Eg 2:- $\mathbb{Z}[i]$ is E.D

Proof:- $\mathbb{Z}[i]$ is Integral Domain

Define $d(a+ib)=a^2+b^2\ge 1$ $\forall\ a+ib\neq 0$.

① $d\big((a+ib)(c+id)\big)=d\big[(ac-bd)+i(bc+ad)\big]$

$=(ac-bd)^2+(bc+ad)^2$

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

$\ge (a^2+b^2)$

$=d(a+ib)$

Thus $d\big[(a+ib)(c+id)\big]\ge d(a+ib)$

Now let $x=a+ib$, $y=c+id\in\mathbb{Z}[i]$

We Want to find $q,r\in\mathbb{Z}[i]$

Such that

$x=qy+r$.

$\Rightarrow r=y\left(\frac{x}{y}-q\right)$

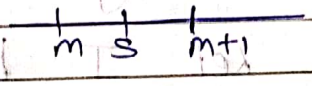
Where $\frac{x}{y}$ is Complex but not necessarily Gaussian.

So $xy^{-1} = (a+ib)\left(\frac{c-id}{c^2+d^2}\right) \in Q(i)$

$= \frac{ac+bd}{c^2+d^2} + i\left(\frac{bc-ad}{c^2+d^2}\right)$

$= s+it$ where $s, t \in \mathbb{Q}$.

Let m be the +ve integer nearest to s and n be +ve integer nearest to t, such integers are uniquely determined because every Rational no's lies between two integers



So that $|m-s| \leq \frac{1}{2}$

$|n-t| \leq \frac{1}{2}$

So $xy^{-1} = s+it = (m-m+s) + i(n-n+t)$

$\frac{a+ib}{c+id} = (m+in) + (s-m) + i(t-n)$

$a+ib = (c+id)(m+in) + \underbrace{(s-m)+i(t-n)}_{\gamma}(c+id)$ ★

$= (c+id)(m+in) + \gamma$ where $\gamma \in Z(i)$

$\Rightarrow \gamma = (a+ib) - (c+id)(m+in)$

& $d(\gamma) = d\left((s-m)+i(t-n)\right)^{(c+id)}$ (from ★)

$= \left[(s-m)^2 + (t-n)^2\right] d(c+id)$

$\leq \left(\frac{1}{4} + \frac{1}{4}\right) d(c+id)$

$< d(c+id)$

So $\gamma = 0$ or $d(\gamma) < d(c+id)$

$\because$ $d(xy) = d(x)d(y)$

Hence $Z[i]$ is E.D

Theorem 18.4:-
Every Euclidean Domain is Principal Ideal Domain.

Proof =
Given:- Let D be Euclidean Domain.
To prove:- D is Principal Ideal Domain
i.e P.I.D :- Every Ideal is principal Ideal.
Proof:-
Let I be an Ideal of D

Case-1 If $I = \{0\}$
then $I = \langle 0 \rangle$
nothing to prove then

So Let I be a nonzero Ideal of D
& Let a be any non zero element in I
i.e $a \in I$ s.t $d(a)$ is minimum.
Claim $I = \langle a \rangle$, We will Show that Every element of I is multiple of a.

Proof = Let $x \in I$
Since $a \neq 0$
$\therefore \exists\ q, r \in D$
Such that $x = aq + r$ where $r = 0$
or $d(r) < d(a)$
$\Rightarrow r = x - aq \in I$ as $a \in I$
& $x \in I$
$\therefore$
But if $d(r) < d(a)$
then r cannot belong to I
Thus $r = 0$
Hence $x = aq$
$\Rightarrow I = \langle a \rangle$
$\Rightarrow$ E.D $\Rightarrow$ P.I.D

Corollary :- Every Euclidean Domain is Unique Factorization Domain.

Ref E.D ⇒ P.I.D ⇒ U.F.D

From "Th^m" 18.4, we know that
E.D ⇒ P.I.D
2 From "Th^m" 18.3, we know that
P.I.D ⇒ U.F.D
Combining both the theorems
We can say
E.D ⇒ P.I.D ⇒ U.F.D

Remark :- U.F.D ⇏ P.I.D ⇏ E.D

Theorem 18.5
If D is Unique factorization Domain, then D[x] is U.F.D

Remark :- Z[x] is U.F.D but it is not P.I.D
It is not E.D

Q :- Prove that Z[√-5] is not U.F.D but an Integral Domain.

Proof :- First of all prove that Z[√-5] is an Integral Domain

Now, we will prove that Z[√-5] is not U.F.D.

Let a+b√-5 ∈ Z[√-5]
then N(a+b√-5) = a²+5b²
Units of Z[√-5] are ±1

Now Consider the following factorizations

$46 = 2 \times 23$

$46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$

We claim that all these four factors are irreducible over $Z[\sqrt{-5}]$.

Thus factorization is not unique

$\therefore Z[\sqrt{-5}]$ is not U.F.D.

Proof:- Let $2 = xy$; $x, y \in Z[\sqrt{-5}]$

& neither x nor y is unit

Now $N(2) = 4 = N(x)\,N(y)$

$\Rightarrow N(x) = N(y) = 2$

which is not possible.

$\therefore$ either x or y is a unit

Let $23 = xy$ where neither x nor y is unit

then $N(23) = N(x)\,N(y)$

$23 \times 23 = N(x)\,N(y)$

If $N(x) = 23 = N(y)$

Thus there must integers a & b such that

$a^2 + 5b^2 = 23$

which is not possible

$\therefore$ either x or y is unit

Now $1+3\sqrt{-5} = xy$ where neither x nor y is unit.

$N(1+3\sqrt{-5}) = N(xy) = N(x)\,N(y)$

$1+45 = N(x) \cdot N(y)$

$2 \times 23 = N(x)\,N(y)$

$\Rightarrow N(x) = 2$ & $N(y) = 23$

but $\nexists$ any integers a & b such that $a^2 + 5b^2 = 2$

& $a^2+5b^2 = 23$
So ± 1 means either x or y is unit

Hly we can prove that $1-3\sqrt{-5}$ is Irreducible Element.

Thus there are two representations for 46
Thus $Z[\sqrt{-5}]$ is not U.F.D

Q6:- Of Grallian :-

Let D be a Euclidean Domain & d be Associated function. Prove that U is a unit in D if and only if $d(U) = d(1)$

Proof:- Given :- Let D be E.D.
& Let U is a unit
To prove:- $d(U) = d(1)$
Proof:- Let U is a unit
$\therefore \exists\ V \in D$ s.t $UV = 1$
$\Rightarrow d(UV) = d(1)$
Now $d(UV) \geq d(U)$
$\Rightarrow d(1) \geq d(U)$ - (1)
Also $d(U) = d(U \cdot 1) \geq d(1)$ - (2)
from (1) & (2)
$d(U) = d(1)$

Conversely
Given:- $d(U) = d(1)$
To prove:- U is a unit
Proof:- Let $d(U) = d(1)$
Since $D = \langle 1 \rangle$
$\therefore d(x) = d(x \cdot 1) \geq d(1) = d(U)$

So $d(x) \geq d(U)$ $\forall x \in D$

Let $x = Uq + r$ where $r = U$ or $d(r) < d(U)$ -(1)

So $r = x - Uq \in D$

So $d(r) \geq d(U)$ -(2)

(1) & (2) are contradictory

$\therefore r = 0$, So $D = \langle U \rangle$

$\Rightarrow U$ is a unit

Q7: from Gallian

Let D be a Euclidean Domain & d is the Associated function. Show that if a & b are associates in D then $d(a) = d(b)$

Proof: Let $a, b \in D$ and a, b are Associates

$\Rightarrow \exists$ a unit U, s.t $a = bU$

$\Rightarrow b = U^{-1}a$

So $d(a) = d(bU) \geq d(b)$ -(1)

$d(b) = d(U^{-1}a) \geq d(a)$ -(2)

(1) & (2) $\Rightarrow$

$d(a) = d(b)$ if a & b are Associates

Q33 from Gallian

Show that for any non-trivial Ideal I of $Z[i]$, $Z[i]/I$ is finite

Proof: Since $Z[i]$ is E.D

$\Rightarrow Z[i]$ is P.I.D

I is non trivial Ideal of $Z[i]$

$\Rightarrow$ I is principal Ideal

Let $I = \langle a+ib \rangle$, $a+ib \neq 0$

$a^2+b^2 \neq 0$

$$\mathbb{Z}[i]/_I = \{x+iy \mid \langle a+ib \rangle \; ; \; x, y \in \mathbb{Z}\}$$

We note that $(a+ib)(a-ib) \in I$.

$\Rightarrow a^2+b^2 \in I$

Let $x = (a^2+b^2)q_1 + r_1$ & $y = (a^2+b^2)q_2 + r_2$

$0 \leq r_1, r_2 < a^2+b^2$

So $\mathbb{Z}[i]/_I = \{x+iy+I\} = \{(a^2+b^2)q_1 + r_1 + (a^2+b^2)q_2 + r_2 + I$

$0 \leq r_1, r_2 < a^2+b^2\}$

$= \{r_1+r_2+I, \; 0 \leq r_1, r_2 < a^2+b^2\}$

$\Rightarrow \mathbb{Z}[i]/_I$ is finite