Th^m 13.5

Every PID is a UFD

Proof

Need to show a PID D satisfies (i) and (ii) of 13.4.

First (ii) Assume $d \in D$ ~~is~~ is irreducible & $d \mid ab$ ($d \neq 0$, d not a unit).

Consider $\langle d \rangle + \langle a \rangle$ an ideal. D is a PID so $\exists c \in D$ s.t.

$$\langle d \rangle + \langle a \rangle = \langle c \rangle.$$

$\therefore \quad d, a \in \langle c \rangle$

$\therefore \quad c \mid d \;\; \& \;\; c \mid a.$

So $d = ce$ But d is irreducible

so either ① c is a unit ~~or~~

② e is a unit.

If ② $c = de^{-1}$ $\therefore d \mid c$ & $c \mid a$ $\therefore d \mid a$.

If ① c is a unit $\langle c \rangle = D$ (TE).

$\therefore \quad 1 = ds + at$ for $s, t \in D$

$\therefore \quad b = bds + bat = \cancel{bds + \ldots}$

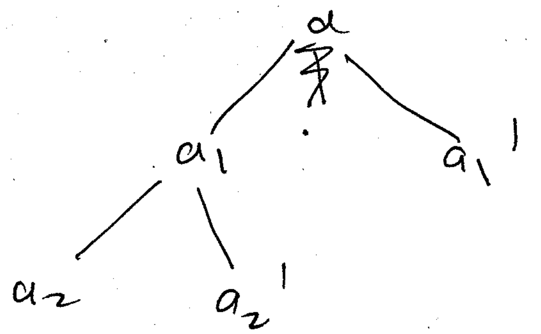
$d \mid ba \quad \therefore \quad d \mid b.$

$\therefore$ d is prime.

Second (i)

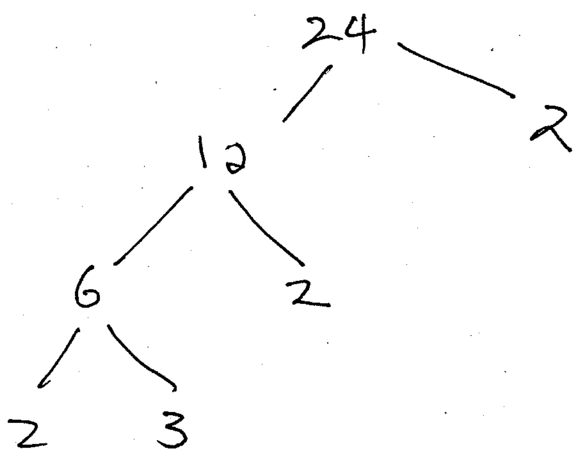
Let $a \in D$. If a is irreducible we are done. If not $a = a_1 a_1'$ neither a unit. If a_1, a_1' are irreducible we are done. If not say $a_1 = a_2 a_2'$ neither a unit & ~~$a_1' = b_2 b_2'$ etc~~.

We form a tree



etc

eg



If ~~a~~ the tree stops then all ends are irreducible & a is their product.
If it goes on forever we get a sequence $a_1, a_2, a_3, \ldots\ldots$
s.t $a_2 | a_1,\ a_3 | a_2, \ldots$

We prove a Lemma ~~next &~~ below showing that in a PID

then imple $\exists N$ s.. a_n is associate to a_N
$\forall n \geq N$

Then $\quad a_N = a_{N+1}\, a'_{N+1}$

& $\quad a_{N+1} = a_N u \quad \therefore\ a'_{N+1}$ is a unit.

This is a contradiction so we are done. //

<u>Lemma 13.6</u>

If $a_1, a_2, \ldots \in D$ a PID &
$a_2 | a_1,\ a_3 | a_2$ etc $\exists N$ s.t. $\forall n \geq N$
a_n & a_N are associate.

<u>Proof</u> $\quad a_{i+1} | a_i \iff \langle a_{i+1} \rangle \supseteq \langle a_i \rangle$ (TE6)

$\therefore\ \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots \subseteq$

Let $\quad J = \bigcup_{i=1}^{\infty} \langle a_i \rangle \qquad$ <u>Ex</u> J is an ideal

D is a PID $\therefore \quad J = \langle a \rangle$

also $\quad a \in \langle a_N \rangle$ for some N

$\therefore \quad \langle a \rangle \subseteq \langle a_N \rangle$

$\therefore$ ~~∃~~ If $n \geq N$ then

$J \subseteq \langle a_N \rangle \subseteq \langle a_n \rangle \subseteq J$

$\therefore\ \langle a_N \rangle = \langle a_n \rangle \ \therefore$ ~~$\langle a_N \rangle$~~ a_N, a_n
associate. //
(TE6)

Final result

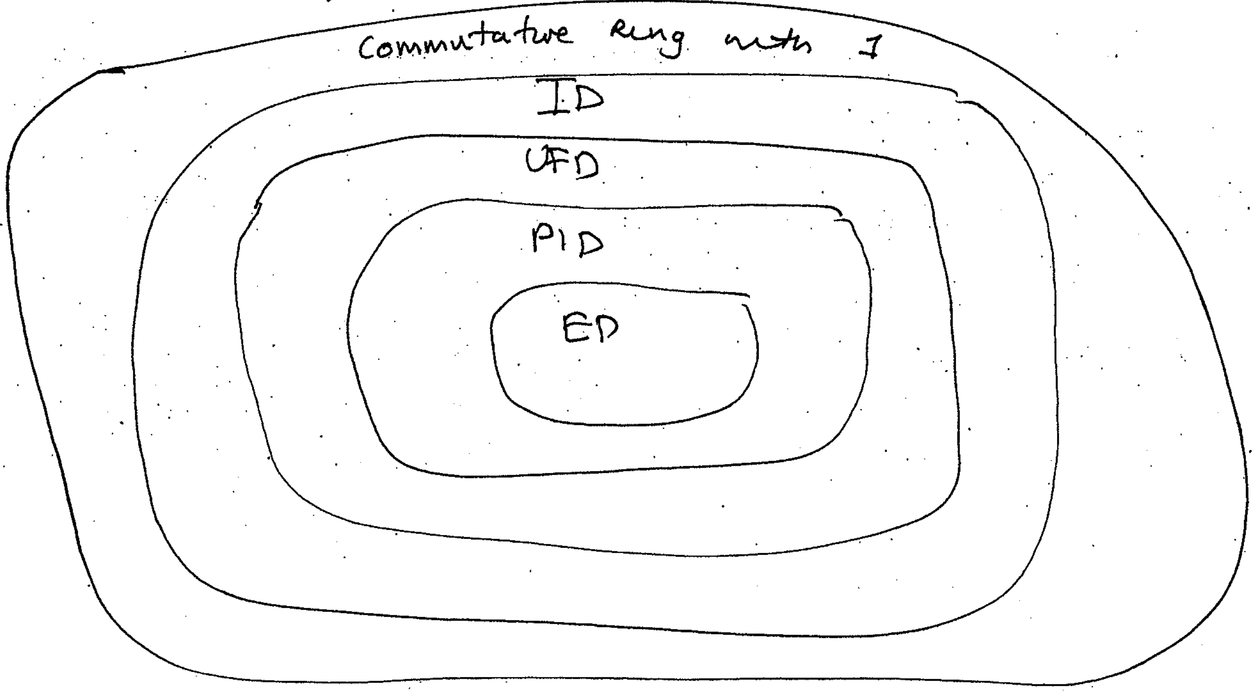
13.4 Polynomial rings as UFD's

If F is a field we know $F[x]$ is a Euclidean domain so that $F[x]$ is a UFD. More generally we have

Thm 13.9 If D is a UFD so also is $D[x]$.

Proof (omitted) (interesting but not enough time)

Corollary 13.10 If D is a UFD so also is $D[x_1, \ldots, x_n]$.



Final Examples

ED's $\mathbb{Z}$, $F[x]$, F a field, $\mathbb{Z}(i)$, $\mathbb{Z}(\sqrt{2})$

we didn't prove this

PID's not ED's $\left\{ \frac{m}{2} + \frac{n}{2}\sqrt{-19} \mid m, n \in \mathbb{Z} \right\}$

we didn't do this. See wikipedia article on PID's.

UFD not PID's $\mathbb{Z}[x]$

Also $\mathbb{Z}[x,y]$, $F[x,y]$

$I = \{ f(x,y) \mid f(0,0) = 0 \}$

ID's not UFD's $\mathbb{Z}(\sqrt{-5})$ $\mathbb{Z}(\sqrt{10})$

$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$ $(4+\sqrt{10})(4-\sqrt{10}) = 6 = 2 \cdot 3$

Commutative rings with 1 not ID'

$\mathbb{Z}_6$, $\mathbb{Z}_m$ m composite