Pf WLOG, $d, d' \neq 0$. $d \in (d') \Rightarrow \exists x \in R.\ d = xd'$

$d' \in (d) \Rightarrow \exists y \in R.\ d' = yd$

Thus $d = xyd \Rightarrow d(1-xy) = 0$.

Since $d \neq 0$, $xy = 1$. □

Thm R a ED, $a, b \in R \setminus \{0\}$. Let $d = r_n$ be the last nonzero remainder in the EA for a, b. Then

① d is a gcd of a, b

② $(d) = (a, b)$, so $d = ax + by$ for some $x, y \in R$.

Pf Suffices to show (i) $d \mid a$ & $d \mid b$ $\Rightarrow (d) \subseteq (a, b)$

($a = dr$ $b = ds$)

(ii) $d = ax + by$ $\Rightarrow (a, b) \subseteq (d)$

(i) $r_n \mid r_{n-1}$ & $r_n \mid r_n$. $r_{k-1} = q_{k+1} r_k + r_{k+1} \Longrightarrow$ if $r_n \mid r_k$ & $r_n \mid r_{k+1}$, then $r_n \mid r_{k-1}$. By downward induction, $r_n \mid a, b$.

(ii)

$$\begin{aligned}
r_0 &= a - q_0 b \\
r_1 &= b - q_1 r_0 \\
r_2 &= r_0 - q_2 r_1 \\
&\ \vdots \\
r_n &= r_{n-2} - q_n r_{n-1}
\end{aligned}$$

□

Lecture 33

Sunday, March 29, 2015 2:01 PM

Principal Ideal Domains

Recall In a PID R, if $(d) = (a,b)$ then

① d is a gcd of a,b

② $d = ax + by$ for some $x,y \in R$

③ d is unique up to mult by a unit of R.

Prop Every nonzero prime ideal in a PID is max'l.

Pf $(p) \neq 0 \trianglelefteq R$ a PID. Let $I = (m)$ be an ideal containing (p). Claim $I = (p)$ or $I = R$.

$p \in (m) \Rightarrow p = rm$ for some $r \in R$. $rm \in (p)$ prime $\Rightarrow r \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(m) \subseteq (p) \Rightarrow (m) = (p)$.

If $r \in (p)$, $r = ps \Rightarrow p = rm = psm \Rightarrow sm = 1 \Rightarrow m \in R^\times$

$\Rightarrow (m) = R$. $\square$

Cor If R is a comm ring such that $R[x]$ is a PID, then R is a field.

Pf $(x) \in \operatorname{Spec} R[x]$ b/c $R[x]/(x) \cong R$ an int domain.

By the prop, (x) is max'l, so R is a field! $\square$

Q Are there PID's which are not ED's?

Defn N is a Dedekind-Hasse norm if N is a positive norm and $\forall\, a,b \in R$ either $a \in (b)$ or $\exists\, s,t \in R$ w/ $0 < N(sa - tb) < N(b)$.

$s = 1$ makes R a ED

Sunday, March 29, 2015 2:14 PM

<u>Prop</u> An int dom R is a PID $\Leftrightarrow$ R has a D-H norm.

<u>Pf</u> $0 \neq I \trianglelefteq R$, $0 \neq b \in I$, $N(b)$ minimal. For $0 \neq a \in I$, $(a,b) \subseteq I$. If $a \notin (b)$, then $\exists s,t \in R$ w/ $0 < N(\underbrace{sa-tb}_{\in I}) < N(b)$, contradicting min'y of $N(b)$. Thus $a \in (b) \Rightarrow I = (b)$.

Converse: next time. $\square$

<u>e.g.</u> $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ has D-H norm

$N(a + b(1+\sqrt{-19})/2) = a^2 + ab + 5b^2$ } see book

so R is a PID.

<u>Fact</u> R is not a ED:

$u \in R \setminus (R^\times \cup 0)$ is a <u>universal</u> <u>side</u> <u>divisor</u> if $\forall x \in R$ $\exists z \in R^\times \cup 0$ s.t. $x = qu + z$

<u>Prop</u> R an int dom which is not a field. If R is a ED, then $\exists$ univ side divisors in R.

<u>Pf</u> $u \in R \setminus (R^\times \cup 0)$ of minimal norm.

$x = qu + r$ w/ $r = 0$ or $N(r) < N(u)$ $\Rightarrow$ $r \in R^\times \cup 0$ by min of u

Hence u is a univ side div. $\square$

<u>Fact</u> $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ has no univ side divs.