Lecture 13: ED, PID continued.

29 September 2020
17:42

Recall: 1) An int dom R is a **ED** if $\exists$ a norm $N: R^{\times} \to \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R^{\times}$ $\exists\, q, r \in R$ satisfying $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

2) An ID R is a **PID** if every R-ideal is principal (gen by 1 element)

- R ED $\Rightarrow$ R PID
- x **irred** if x nonzero nonunit & $x = yz \Rightarrow y$ is a unit or z is a unit
- x **prime** if " " " & $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.
- R an int dom. x prime $\Rightarrow$ x irred.
- R PID. x irred $\iff$ x prime.
- R a PID then every nonzero prime ideal is maximal.

Def^n: Let R be a comm ring with unity & $a, b \in R$ then $d \in R$ is said to be a **gcd** of a, b in R if $d \mid a$, $d \mid b$ and if $d' \in R$ is s.t. $d' \mid a$ & $d' \mid b \Rightarrow d' \mid d$. $d = \gcd(a, b)$ or $d = (a, b)$ (Caution: gcd is not unique!)

Eg: In $\gcd(4, 6) = 2$, $1, -1, -2 \leftarrow$ gcd

Prop: Let R be a ring & $a, b \in R$ s.t. $(a, b)R$ is a principal ideal dR, i.e. $(a, b) = (d)$ then d is the $\gcd(a, b)$. Moreover, $d = ax + by$ for some $x, y \in R$.

Pf: Since $a, b \in (d)$ $d \mid a$ & $d \mid b$. Let $d' \in R$ be s.t. $d' \mid a$ & $d' \mid b \Rightarrow a, b \in (d') \Rightarrow (d) = (a, b) \subseteq (d')$ $\Rightarrow d \in (d') \Rightarrow d' \mid d$. Moreover, follows since $d \in (a, b)$.

Cor: R a PID & $a, b \in R$ then $\gcd(a, b)$ exist. In fact $\gcd(a, b)$ is the generator d of the ideal (a, b) &

$$\boxed{d = ax + by \text{ for some } x, y \in R.}$$

- gcd may not be unique.
- gcd may exist even if (a, b) is not principal

Eg: In $\mathbb{Z}[X]$, $(X, 2)$. If $(f(X)) = (X, 2) \Rightarrow f(X) \mid X$ $\Rightarrow f(X) = \pm X$. But $2 \notin (f(X))$.

So $(X, 2)$ is not principal.
$\gcd(X, 2) = 1$

1) $\mathbb{Z}[X]$ is not a PID. (X) is prime ideal.

2) $\mathbb{Z}[\sqrt{-3}]$ is not a PID. $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Q}[\sqrt{-3}] \subseteq \mathbb{C}$

$\mathbb{Z}[\sqrt{-3}] \neq \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$

$I = (1+\sqrt{-3}, 2) \subseteq \mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$

$\mathbb{Z}[\sqrt{D}]$ is not a PID whenever D is squarefree & $D \equiv 1 \pmod 4$

claim: $I \cap \mathbb{Z} = 2\mathbb{Z}$

$x \in$ $\supseteq$ ✓

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4$

$x = \boxed{\alpha(1+\sqrt{-3})} + \beta 2 \in \mathbb{Z}$ $\quad \alpha \in \mathbb{Z}[\sqrt{-3}]$, $\beta \in \mathbb{Z}$

$\Rightarrow \alpha = a(1-\sqrt{-3})$ where $a \in \mathbb{Z}$

$x = 4a + 2\beta$

$\Rightarrow x \in 2\mathbb{Z}$

So $1 \notin I$. If $I = (a+b\sqrt{-3})$

Since $1+\sqrt{-3} \notin 2\mathbb{Z}[\sqrt{-3}] \Rightarrow I$ is not gen by integer.

So $b \neq 0$. $2 = (c+d\sqrt{-3})(a+b\sqrt{-3})$ ← (*)

$\Rightarrow c+d\sqrt{-3} = e(a-b\sqrt{-3})$

$N: \mathbb{Q}[\sqrt{-3}] \to \mathbb{Q}$

$a+b\sqrt{-3} \mapsto a^2+3b^2$

$4 = (c^2+3d^2)(a^2+3b^2)$

N satisfies

$N(\alpha\beta) = N(\alpha)N(\beta)$

$\forall \alpha, \beta \in \mathbb{Q}[\sqrt{-3}]$

If $\alpha \in \mathbb{Z}[\sqrt{-3}]$ then $N(\alpha) \in \mathbb{Z}$

$b \neq 0 \Rightarrow b = \pm 1,\ a = \pm 1$

$d = 0,\ c = 1$

i.e. $\pm 1 \pm \sqrt{-3}$

But $2 = (1+\sqrt{-3})\left(\frac{1-\sqrt{-3}}{2}\right)$ not in $\mathbb{Z}[\sqrt{-3}]$

$\Rightarrow 2 \notin (1+\sqrt{-3})$

In fact $\mathbb{Z}[\sqrt{d}]$ is not a PID

if $d \equiv 1 \pmod 4$

& d is squarefree

⊛ $\mathbb{Z}[i]$ is a Euclidean domain and hence a PID.

$i = \sqrt{-1}$
$\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}$

Pf: $N : \mathbb{Z}[i]^\times \longrightarrow \mathbb{Z}_{\geq 0}$
$a + bi \longmapsto a^2 + b^2$

Claim N is a Euclidean norm.

Let $\alpha, \beta \in \mathbb{Z}[i]^\times$, then
$\alpha = a+bi$ & $\beta = c+di$ for some $a, b, c, d \in \mathbb{Z}$

Want $\alpha = \beta q + r$ with $N(r) < N(\beta)$ or $r = 0$

$\frac{\alpha}{\beta} = \boxed{\frac{(a+bi)(c-di)}{c^2+d^2}} = u + vi \quad u, v \in \mathbb{Q}$

Let $p, q \in \mathbb{Z}$ be s.t. $|u-p| \leq \frac{1}{2}$ and $|v-q| \leq \frac{1}{2}$

$\alpha = \beta(p+qi) + \underbrace{\beta(u-p+(v-q)i)}_{\overset{\shortparallel}{r}}$ $\overset{?}{\in} \mathbb{Z}[i]$

$$N(r) = N(\beta)\left((u-p)^2 + (v-q)^2\right)$$
$$\leq \frac{1}{2} N(\beta) < N(\beta)$$

Hence the claim. i.e. $\mathbb{Z}[i]$ is ED.

Thm: R a comm ring with unity s.t. $R[X]$ is a PID then R is a field.

Pf: $R \subseteq R[X]$ is a subring and hence an int domain.

Let $\varphi : R[X] \longrightarrow R$ be the map
$f(X) \longmapsto f(0)$

Then φ is a surj ring homo.

& $\ker(\varphi) = (X)$
$\supseteq$ ✓

$\subseteq$: $\varphi(f(X)) = 0$ for $f(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$

then $a_0 = 0 \Rightarrow f(X) = X(a_{n-1}X^{n-1} + \dots + a_1)$
$\in (X)$

Hence $R[X]/(X) \cong R \Rightarrow (X)$ is a prime ideal in the PID $R[X]$.

Hence (X) is maximal ideal of $R[X]$.

$\Rightarrow R$ is a field.

Ex $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not ED.

R'' $\mathbb{Q}[\sqrt{-19}]$ $N\left(\frac{1+\sqrt{-19}}{2}\right) = \frac{1+19}{2} = 10 \in \mathbb{Z}$

Prop: (*) Let R be a ED but not a field then it contains a "universal side divisor", i.e. an element u which is non zero nonunit s.t. $\forall x \in R^\times$ $\exists q \in R$ satisfying $x - qu$ is either zero or a unit. $x = qu + r$

Pf: Let u be a nonzero nonunit in R with least Euclidean norm. Then u is a universal side divisor. ($x \in R^\times \Rightarrow \exists q, r \in R$ s.t. $x = uq + r$ with $N(r) < N(u)$ or $r = 0$ $\Rightarrow r = 0$ or r is a unit)

Units in $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

$N : R \longrightarrow \mathbb{Z}$ α is a unit iff $N(\alpha)$ is a unit. ($(\Rightarrow)$ $\alpha\alpha^{-1} = 1 \Rightarrow N(\alpha)N(\alpha^{-1}) = N(1) = 1$)

$\alpha\bar{\alpha} = \pm 1$

Let $\alpha = a + b\left(\frac{1+\sqrt{-19}}{2}\right)$ $N(\alpha) = \alpha\bar{\alpha} = \left(a + b\left(\frac{1+\sqrt{-19}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-19}}{2}\right)\right)$

$= a^2 + b^2\,\frac{1+19}{4} + ab$

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

α is a unit $\Leftrightarrow N(\alpha) = \pm 1$

$\Leftrightarrow a^2 + ab + 5b^2 = \pm 1$

$\left(a + \frac{1}{2}b\right)^2 + \frac{19}{4}b^2 = \pm 1$

$(2a + b)^2 + 19b^2 = 4$

$\Rightarrow b = 0$ & $a = \pm 1$

Units in $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is ± 1

Check $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ has no universal side divisor. u

$x = 2$ $2 = uq + r$, $r = \pm 1$ or 0

$u = \{\pm 2, \pm 3\}$

Prop (*) R is a PID iff R has Dedekind-Hasse norm.

where $N : R^\times \longrightarrow \mathbb{Z}_{>0}$ is a Dedekind-Hasse norm if $\forall a, b \in R^\times$ either $a \in (b)$, i.e. $b \mid a$ or $\exists r \in (a, b)$ s.t. $N(r) < N(b)$

$\exists x, y \in R$ $r = ax + by$ $N(ax + by) < N(b)$

Pf: $(\Leftarrow)$: $I \subseteq R$ a nonzero ideal

Let $b \in I$ be of least norm then $I = (b)$ (If $a \in I$ then $\exists r \in (a, b)$ with $\underbrace{N(r) < N(b)}_{\text{Not possible}}$ or $a \in (b)$)

$(\Rightarrow)$ Later.

$\exists q, r$ s.t. $a = bq + r$ $N(r) < N(b)$ or $r = 0$

$r = bq + a$

$\exists q', q$ s.t. $r = bq + aq'$ with $N(r) < N(b)$ or $r = 0$

Check that

$$N: \mathbb{Z}\Big[\underbrace{\tfrac{1+\sqrt{-19}}{2}}_{\omega}\Big]^{\times} \longrightarrow \mathbb{Z}_{>0}$$

$$a+b\omega \longmapsto a^2+ab+5b^2$$

is a Dedekind-Hasse norm.

Let D be squarefree integer.

$\mathbb{Q}(\sqrt{D})$ is a field

$$R=\begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Then R is called ring of integers in $\mathbb{Q}(\sqrt{D})$

$$N: \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$$

$$(a+b\sqrt{D}) \longmapsto a^2-Db^2$$

$$N|_R: R \longrightarrow \mathbb{Z}$$

$$N(\alpha\beta)=N(\alpha)N(\beta)$$

$N(\alpha)$ is a unit in $\mathbb{Z}$ $\Leftrightarrow$ α is unit in R.

α is unit $\Rightarrow$ $\alpha\alpha^{-1}=1$

$$1=N(1)=N(\alpha)N(\alpha^{-1})$$

$N(\alpha)$ is unit in $\mathbb{Z}$

$\pm 1 = N(\alpha)=\alpha\bar{\alpha} \Rightarrow \alpha$ is unit $\blacksquare$