Algebra Lec 13. ED. PID UFD

Euclidean domain (ED)

principle entire ring, principle ideal domain (PID)

factorical ring. unique factorization domain (UFD)

def. (norm). A: entire ring (domain)

$$N: A \to \mathbb{Z}^+ \cup \{0\}, \quad N(0)=0$$
$$\begin{matrix} \not\ni \\ 0 \end{matrix} \mapsto \begin{matrix} \not\ni \\ 0 \end{matrix}$$

def The entire ring A is called a Euclidean domain

if $\exists$ a norm N on A

s.t. $\forall a, b \in A$. $b \neq 0$. $\exists q, r \in A$

s.t. $a = qb + r$

w. $N(r) < N(b)$. or $r = 0$.

then we can do

$$\left.\begin{aligned} & a, b \in A \\ & a = qb + r_0 \\ & b = q_1 r_0 + r_1 \\ & r_0 = q_2 r_1 + r_2 \\ & \quad \vdots \\ & r_{n-1} = q_{n+1} r_n + 0 \end{aligned}\right\} \quad N(b) > N(r_0) > N(r_1) > \cdots > 0$$

eg. $\mathbb{Z}$. entire ring

$a \in \mathbb{Z}$. $N(a) = |a|$ $\Rightarrow$ ED.

eg. F: field $F[x]$: ED

$p(x) \in F[x]$ $N(p(x)) \triangleq \deg p(x)$

eg. $\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \}$

$\alpha = a+bi$

$\beta = c+di$

$$\Rightarrow \frac{\alpha}{\beta} = r+si = \frac{(ac+bc)+i(bc-ad)}{c^2+d^2}$$

closest to p

$$= \underset{\mathbb{Z}}{\underset{\cap}{p}} + \underset{\mathbb{Z}}{\underset{\cap}{q}} i + \theta$$

$$\alpha = (p+qi)\beta + \underset{\mathbb{Z}}{\underset{\cap}{\theta\beta}}.$$

$$\Rightarrow N(\theta\beta) = N(\theta)N(\beta) \le \left(\left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2\right) N(\beta)$$

def. A principle entire ring (PID)

is an entire ring, in which every ideal is principle.

Rmk. ED $\Rightarrow$ PID

Pf A: ED $\underset{\text{(ideal)}}{I \subseteq A}$

let $d \in I$ be a nonzero elem of I. which has min. norm.

claim. $\underline{I = (d)}$

<u>pf of claim:</u> $\forall a \in I.$ $a = qd + r$ if $r \neq 0$ $N(r) < N(d)$. $\times$

<u>def</u> A: entire ring

$\underset{\neq 0}{a} \in A$ is called <u>irreducible</u>.

if a is not unit and if $a = bc$. $b, c \in A$

then b is a unit or c is a unit

<u>Rmk</u>. A entire ring. $a \in A$

(a) : prime $\Rightarrow$ a: irreducible

<u>pf</u>. if $a = bc$, $\because$ (a) is prime

$b \in (a)$. or $c \in (a)$

say $b \in (a)$. $\therefore$ $b = ad$ for some $d \in A$

$\therefore$ $a = bc = adc$ $\Rightarrow$ $cd = 1$ $\therefore$ c unit. $\Rightarrow$ irreducible

Summary

$\mathbb{Z}[(1+\sqrt{-19})/2]$. not ED
(p277. p282. D-F).

field $\subset$ Euclidean domain $\subset$ PID $\subset$ UFD $\subset$ entire ring domain.

$\mathbb{Z}$ not a field. $\mathbb{Z}[x]$ not PID $\mathbb{Z}[\sqrt{-5}]$ not UFD

(prime $\Leftrightarrow$ irred $\Leftrightarrow$ max) (prime $\Leftrightarrow$ irred) (prime $\Rightarrow$ irred)

HW. Lang Chap II ex 1. 9. 10

Unique factorization of an elem $a \in A$

$$\underset{\neq 0}{a} \in A \qquad a = u \prod_{i=1}^{r} p_i = v \prod_{i=1}^{s} q_i$$

u : unit $\quad v$: unit

p_i : irred $\quad q_i$: irred

$\Rightarrow r = s$, $p_i = u_i q_i$. u_i : unit

$\Rightarrow$ We say $\underset{A}{\underset{\cap}{a}}$ has a unique factorization into irreducibles

def. A is called a factorial ring, UFD

if A is entire, and $\forall \underset{\neq 0}{a} \in A$, a has a unique factorization into irreducibles

def A. entire ring

$a, b \in A$. $ab \neq 0$

$a | b \Leftrightarrow \exists c \in A$. s.t. $ac = b$

$d = \gcd(a,b) \iff \begin{cases} \cdot\ d|a,\ d|b \\ \cdot\ \text{if } e|a,\ e|b \Rightarrow e|d \end{cases}$

Prop of PID

A: PID

$a,b \in A.\ ab \neq 0$

$(a)+(b) = (c) \Rightarrow c = \gcd(a,b)$

pf. $(a)+(b) = (c)$

$\Rightarrow b \in (c) \Rightarrow b = cx$. for some $x \in A$

$\therefore c|b$. Similarly $c|a$

if $d|a.\ d|b.$ $\quad a = dy$

$b = dz$

$c \in (a)+(b) = (a,b) = (c)$

$c = wa + tb = wdy + tdz \Rightarrow d|c \Rightarrow c$ is gcd.

Thm. A: principle entire ring (PID) $\Rightarrow$ A: factorial ring (UFD).

pf. $\forall a \in A$ a. not unit

$\begin{cases} a: \text{irred. done} \\ a: \text{not irred} \quad a = a_1 a_2,\ a_1. a_2 \text{ not unit} \end{cases}$

If a_1, a_2 unit done.

If not ......

If the process terminates at finite steps. done ✓

If not. we have.

$$\left.\begin{aligned} a &= a_1 a_2 \\ a_1 &= a_{11} a_{12} \\ a_{11} &= a_{111} a_{112} \\ &\vdots \end{aligned}\right) \text{all. not unit}$$

$$\therefore \underset{I_1}{(a)} \subsetneq \underset{I_2}{(a_1)} \subsetneq \underset{I_3}{(a_{11})} \subsetneq \underset{I_4}{(a_{111})} \cdots \subset A. \quad \text{infinite chain.}$$

let $I = \bigcup_i I_i$: ideal of A and proper.

$\Rightarrow I = \bigcup_i I_i = (b)$. $b \in I_j$ for some j

$\Rightarrow I_{j+1}\ I_{j+2} \cdots = I_j$ $\quad$ ~~—~~ $\times$

uniqueness

(exercise). A: PID. $f \in A$ not unit $\neq 0$

(f) : prime $\Leftrightarrow$ (f) : max $\Leftrightarrow$ f : irred.

$a \in A$.

if $\quad a = p_1 \cdots p_n = q_1 \cdots q_m.\quad m \geq n$

$p_1 \mid q_1 \cdots q_m.$

irred $\Leftrightarrow$ prime $\quad \Rightarrow \quad p_1 \mid q_j$ for some j

$\Downarrow$ renumber

$p_1 \mid q_1 \quad \therefore q_1 = u_1 p_1$. u_1 must be unit

Continue this process $\quad$ done. $\quad \square$

Thm. A: UFD $\Rightarrow A[x]$: UFD $\quad$ (not now!)

Rmk. $\mathbb{Z}$: UFD $\Rightarrow \mathbb{Z}[x]$: UFD

Rmk. $\mathbb{Z}[x]$: UFD

$\mathbb{Z}[x]$: not PID

$(2, x)$: ideal in $\mathbb{Z}[x]$

$\parallel$

$\{2P(x) + xQ(x) \mid P, Q \in \mathbb{Z}[x]\}$.

$2 \in (2, x)$ $\quad$ if $\mathbb{Z}[x]$ is a PID $\quad$ then $(2, x) = (a(x)) \ni 2$

$2 = a(x)\, b(x)$ for some $b(x) \in \mathbb{Z}[x]$

$\Rightarrow a(x) = \pm 1, \pm 2 \quad \Rightarrow \quad a(x) = \pm 2 \quad \divideontimes$