Ring

D. Hilbert → German word.

$4 = 2 \times 2$
$(1+\sqrt{5})(-1+\sqrt{5})$ } Not unique.

Ring → A nonempty set $R \neq \Phi$ with two binary operations $(+, \cdot)$, satisfying the following is called a ring. $((1) \to (7))$

(1) $a+b \in R \quad \forall a, b \in R$
(2) $a+(b+c) = (a+b)+c \quad \forall a, b, c \in R$.
(3) $\exists\ 0 \in R$ s.t. $a+0 = 0+a = a \quad \forall a \in R$
(4) for every $a \in R$ $\exists\ b \in R$ s.t. $a+b = b+a = 0$

} Additive gp.

(5) $a+b = b+a \quad \forall a, b \in R$

Also $a.b \in R$ $\forall a, b \in R$

(6) $a.(b.c) = (a.b).c \quad \forall a, b, c \in R$
(7) $a.(b+c) = a.b + a.c$
$(a+b).c = a.c + b.c \quad \forall a, b, c \in R$.

- We say R is commutative if $a.b = b.a \ \forall a, b \in R$.
- We say R has a unity
  ↓
  Multiplicative Identity if $\exists\ 1 \in R$ s.t. $a.1 = 1.a = a \ \forall a \in R$
- We say $a \in R$ is a unit if $\exists\ b \in R$ s.t.
  invertible
  $a.b = b.a = 1$.

(8) $a.b = b.a \quad \forall a, b \in R$

(9) $\exists 1 \in R$ s.t. $a.1 = 1.a = a \quad \forall a \in R$ (Unity)

(10) For each $0 \neq a \in R$ $\exists b \in R$ s.t. $a.b = b.a = 1$

unit.

Defⁿ – R is a field if it satisfies [(1) → (10)].

Ex → → $(\mathbb{Z}, +, \times)$ → ring of integers.

commutative ring with unity.

→ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ → fields.

→ $(\mathbb{Z}_n, \oplus, \otimes)$ → comm. ring with unity.
→ field if n → prime.

→ $M_n(R)$ → generally non commutative
↳ any ring need not have unity.
will have unity if R has unity.

Polynomial ring → $R[x_1, x_2, \ldots, x_n]$ → commutative if R is comm.
unity if R has unity.

→ $f: X \to \mathbb{R}$ Comm. ring ✓ as $\mathbb{R}$ is comm.

$(f+g)(x) = f(x) + g(x)$

$(f.g)(x) = f(x).g(x)$

Laurent Polynomials → $\mathbb{R}[x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_n, x_n^{-1}]$

non square integer $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ → Ring. $\mathbb{Q}[\sqrt{d}]$ → field.

$\mathbb{Z}[i]$ — Ring of Gaussian integers.

Power Series Ring → $\mathbb{R}[[x]]$ $\sum_{i=1}^{\infty} a_i x^i$

- R be a commutative ring. We say $a^{\neq 0} \in R$ is a <u>zero divisor</u> if $\exists\, b \neq 0$ s.t. $a.b = 0$.

If R is a field, $a.b = 0 \rightarrow a = 0$ or $b = 0$
(Multiply by a^{-1} or b^{-1})

- Let R be a ring with unity. We say R is a <u>division ring</u>, if every non-zero element is a <u>unit</u>.

<u>Division Ring</u> <u>Field</u>
need not be commutative ↓ commutative ✓

$$Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$$

Hamiltonian Quaternion or Quaternion Ring.

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Division Ring ✓ (not a field)

Inverse → $\frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$

<u>Defⁿ</u> Let R be a ring. The smallest +ve integer k s.t. $k.a = 0$ $\forall a \in R$ is called the <u>characteristic</u> of the ring R.

$$\underbrace{a + a + \dots + a}_{k \text{ times}}$$

We say <u>char(R) = 0</u> if there is no such 'k'.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\text{char}(\mathbb{Z}_n) = n$

$\text{char}(\mathbb{Z}_p) = p$ (field ✓)

Defⁿ → R be a ring. A subset I of R is called an ideal of I if it is an additive subgp. (①)

② → $r.a \in I \quad \forall\ r \in R, a \in I$ ← Left sided ideal

$a.r \in I \quad \forall\ r \in R, a \in R$ ← Right sided ideal

Ex → $R = \mathbb{Z}$ $I = 2\mathbb{Z}$ is an ideal.

$I = k\mathbb{Z}$ —— " ——

Trivial ideals → (0), R

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ → only trivial ideals.

(field) ↓

(True for all fields)

Pf $a \neq 0 \in I$

$\Rightarrow 1 = a^{-1}a \in I$

↓

generate the whole R.

We will mostly focus on commutative rings in this course.

- Subring → Similar defⁿ as subgp.
  ↳ Nonempty subset of R with binary operations $(+, \cdot)$ which is itself a ring.

- Ideal → Let R be a ring. An additive subgp I of R is called an ideal of
  $r.a \in I \quad \forall\ r \in R, a \in I$.

Similar to normal subgps

Ex → $\mathbb{Z}$ (0), $2\mathbb{Z}$, $k\mathbb{Z}$

Any field → $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\quad I \neq 0 \Rightarrow a \neq 0 \in I$, $1 = a^{-1} a \in I$

→ only ideals are trivial ideals.

$\mathbb{R}[x]$ $\quad f(x)$: the constant terms of $f(x)$ is zero.

$g(x) f(x) \longrightarrow$ constant term zero ✓.

Let R be a ring. Let S be a subset of R.
The ideal generated by S

$$(S) = \left\{ \sum_{i=1}^{n} r_i s_i : r_i \in R, s_i \in S \right\}.$$

$\mathbb{Z}[x]$ $\quad (2, x) \rightarrow$ set of all polynomials with even constant term.

$(3, x) \rightarrow$ ——— " ——— with constant term divisible by 3.

R → Ring, I → Ideal.

$\frac{R}{I}$ → ring → Quotient Ring

$= \{a + I : a \in R\}$

Quotient map.

$R \longrightarrow \frac{R}{I}$

$(a+I) + (b+I) = (a+b) + I$

$(a+I)\cdot(b+I) = ab + I$

$f: R \to S$ homomorphism

(1) $f(a+b) = f(a) + f(b)$
(2) $f(a \cdot b) = f(a) \cdot f(b)$
(3) $f(1_R) = 1_S$

} preserves both binary operations

$1 \mapsto 1 \leftarrow \mathbb{Z} \to \mathbb{Z}$ only trivial homomorphism
$f(2) = f(1)+f(1) = 2$ $\mathbb{Q} \to \mathbb{Q}$ —"—
$f(n) = n$. $\mathbb{R} \to \mathbb{R}$ —"—

$f: R \to S$

Do image of ideal need to be an ideal?

NO.

$f: \mathbb{Z} \to \mathbb{Q}$
↳ ideal (0) & $\mathbb{Q}$

Take f to be identity map. $f(\mathbb{Z}) = \mathbb{Z}$ ↳ not ideal in $\mathbb{Q}$.

But $f^{-1}(I)$ is an ideal of J is an ideal of S.

$I + J = \{a+b : a \in I, b \in J\}$
is an ideal.

X $IJ = \{a \cdot b : a \in I, b \in J\}$ need not be an ideal.

$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}$

Suppose $f: R \to S$ is a ring homomorphism.

$\ker f = \{x \in R : f(x) = 0\}$

↳ ideal of R.

$$f(x+y) = f(x) + f(y) = 0$$
$$f(x \cdot x) = f(x) \cdot f(x) = 0.$$

1st isomorphism thm. $\frac{R}{I} \cong f(R)$ $\qquad \phi : \frac{R}{I} \to f(R)$

2nd isomorphism thm. $I \subset J \subset R$ $\qquad \frac{IJ}{J} \cong \frac{I}{I \cap J}$ ← What does it mean?

$I \subset J \subset R$

$\frac{R}{I} \quad \frac{R}{J} \qquad \frac{R}{I} \to \frac{R}{J}$

Defn → A ring (nonzero commutative ring with unity.) without zero divisors is called an integral domain. (ID)

Ex → $\mathbb{Z}$, any field F.

Claim → R is an ID. Then $\text{char}(R) = 0$ or p → prime.

Pf → Suppose not ($\text{char}(R) \neq 0$), To show that $\text{char}(R) = p$.

n – char of R, $n = pq$.

$$n \cdot a = 0 \quad \forall a \in R$$

$\Rightarrow$

$pq \cdot 1 = 0 \Rightarrow (p \cdot 1)(q \cdot 1) = 0$

$\Downarrow$

$(p \cdot 1) = 0$

$\Rightarrow (p \cdot 1) a = 0$

$\Rightarrow p \cdot a = 0.$

$\Rightarrow\Leftarrow$

$\frac{R}{I} = \{a + I : a \in R\}$ ⟶ Quotient Ring

$\oplus, \odot$

$(a+I) \oplus (b+I) = (a+b) + I$

$(a+I) \odot (b+I) = (ab) + I$

$\mathbb{Z}$, $I = 2\mathbb{Z}$

$\frac{\mathbb{Z}}{I} \cong \mathbb{Z}_2$ } $\mathbb{Z} \to \mathbb{Z}_2$, $x \mapsto x \bmod 2$, 1st isomorphism thm ✓✓.

Isomorphism Theorems –

(1) $f : R \to S$. Then

$\frac{R}{\ker f} \cong f(R)$

$\ker(f) = \{x \in R : f(x) = 0\}$

(2) $I \subset J \subset R$.

$I + J = \{a + b : a \in I, b \in J\}$.

R has a unity.

$\frac{I+J}{J} \cong \frac{I}{I \cap J}$

(3) $I \subset$

$\frac{R}{I}$

$IJ =$

Defⁿ → Prim

Ex →

→

$S \subset R$ $\quad I \to$ ideal.

↳ subring.

$S+I$ is a subring of R.

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

$S \to \frac{S+I}{I}$

$s \mapsto s+I$.

(3) $I \subset J \subset R$.

$$\frac{R}{I} \to \frac{R}{J} \qquad \frac{\frac{R}{I}}{\frac{J}{I}} \cong \frac{R}{J}$$

\# $IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}$

↳ ideal.

$I \not\subset IJ$

$I \supset IJ$ ✓

Similarly $J \supset IJ$ ✓ $\Big\}$ $IJ \subset I \cap J$

Where as $IJ = I \cap J$ (or $I \cap J \subset IJ$)?

Def^n → Prime ideals :- An ideal $I \overset{*}{\subset} R$ of R is called a prime ideal of for $a.b \in I \Rightarrow$ either $a \in I$ or $b \in I$.

Ex → $a.b \in (P) \Rightarrow a \in (P)$ or $b \in (P)$.

→ $\mathbb{Z}$ $\quad P\mathbb{Z}$ is prime ideal, (0) is prime ideal.

Thm – Let $I \neq R$ be an ideal of a ring R. Then $\exists$ a maximal ideal M of R s.t. $M \supseteq I$.

Corollary – A ring with identity contains a maximal ideal.

→ $\mathbb{R}[x]$ (x) is prime ideal.

- R is an ID iff (0) is a prime ideal.
- R ring and I is ~~a~~ an ideal. Then I is a prime ideal iff $\frac{R}{I}$ is an ID.

$$\frac{R}{I} = \{a+I : a \in R\}$$

$$(a+I)(b+I) = I \iff ab + I = I \iff ab \in I$$

$$\Updownarrow$$

$$a \in I \text{ or } b \in I$$

$$\Updownarrow$$

$$a+I = I \text{ or } b+I = I$$

$$\checkmark$$

Def^n – **Maximal Ideal** – An ideal M of R is maximal if there is no ideal of R strictly containing M.

$$M \subsetneq R$$

Why such M exist?

$I \rightarrow$ ideal

Every ring with unity has a maximal ideal.

$$J = \{M \subsetneq R \text{ ideal} : I \subseteq M\}$$

Top

POSET

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n \subseteq \ldots$$

$$M_i \subseteq \bigcup_{i=1}^{\infty} M_i \text{ ideal} \checkmark$$

Use Zorn's Lemma.

Every

$$\bigcup_{i=1}^{\infty}$$

- M C

$$\frac{R}{M}$$

Thm – There

Pf → Same

Pf → (⇐)

(⇒) $\frac{R}{M}$

Every maximal ideal is a prime ideal.
(Not converse).

$\bigcup_{i=1}^{\infty} M_i \neq R$

↳ contains 1.

- $M \subset R$ ideal.

$\frac{R}{M}$ is a field iff M is a maximal ideal.

Thm → There is a one-to-one correspondence between ~~subrings~~ subrings of R containing I and subrings of $\frac{R}{I}$.

Pf → Same as group.

$(a+M)\cdot(b+M) = 1+M$

Pf → ($\Leftarrow$) $(a) + M = R$

$ra + b = 1$

$ra + \underline{b + M} = 1 + M \Rightarrow ra + M = 1 + M$

$\rightarrow (r+M)(a+M) = 1+M$

✓

($\Rightarrow$) $\frac{R}{M}$ is a field

$M \subset N \subset R$

$\frac{N}{M} = \frac{R}{M}$ or $\frac{N}{M} = M$.

Chinese Remainder Thm

$\longrightarrow$ $n_1, n_2, \ldots, n_k$ are pairwise coprime integers.

$a_1, a_2, \ldots, a_k \in \mathbb{Z}$

$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$
$\vdots$
$x \equiv a_k \bmod n_k$

$\Big\downarrow$ has a solution.

a, b are 2 solutions, then

$$a - b \equiv 0 \bmod (\Pi n_i)$$

$$\mathbb{Z} \longrightarrow \overbrace{\frac{\mathbb{Z}}{n_1\mathbb{Z}}}^{a_1} \times \overbrace{\frac{\mathbb{Z}}{n_2\mathbb{Z}}}^{a_2} \times \cdots \times \overbrace{\frac{\mathbb{Z}}{n_k\mathbb{Z}}}^{a_k}$$

$$a \longmapsto (a_1 + n_1\mathbb{Z}, a_2 + n_2\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$$

$\ker f = \bigcap n_i\mathbb{Z} = (\Pi n_i)\mathbb{Z}$ (as pairwise coprime)

1st isomorphism thm $\Rightarrow$ $\dfrac{\mathbb{Z}}{(\Pi n_i)\mathbb{Z}} \cong \dfrac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n_2\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{n_k\mathbb{Z}}$

$I \subseteq R$

$a, b \in R$

We say $a \equiv b \bmod I$ if $a - b \in I$

$\Longrightarrow$

If $(m,n)=1$

$(m)+(n)=\mathbb{Z}$

as $\exists\ r,s$ s.t. $rm+sn=1 \rightsquigarrow$ construct $\mathbb{Z}$.

(Bezout's identity)

PAGE NO.:
DATE: / /

Def^n – I and J are 2 ideals (coprime)(comaximal)

iff $I+J=R$.

Thm – Let $I_1, I_2, \ldots, I_n$ be pairwise coprime (co-maximal) ideals of R. Then

$$\frac{R}{\bigcap_{j=1}^{n} I_j} \cong \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n}$$

$\not\Longleftarrow$ $I+J=R \Longrightarrow IJ=I\cap J$

Proof ↓

$$I\cap J \supset IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}$$

$I_1, I_2, \ldots, I_n$ $\quad I_i+I_j=R \quad i\neq j$

Then $\rightarrow$ $\boxed{\bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j}$

For 2 elements

Pf → $\varphi : R \longrightarrow \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n}$

$a \longmapsto (a+I_1, a+I_2, \ldots, a+I_n)$

$\ker \varphi = \{a : a \in \bigcap_{i=1}^{n} I_i\}$

$= \prod_{i=1}^{n} I_i$

If by 1st iso. Thm ✓

General

$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ example of a ring with no maximal ideal.

PAGE NO.
DATE

For 2 elements

$I_1 + I_2 = R$

$a + b = 1$

$b \equiv 1 \bmod I_1 \qquad b \equiv 0 \bmod I_2$

$a \equiv 1 \bmod I_2 \qquad a \equiv 0 \bmod I_1$

$\frac{R}{I_1 \cap I_2} \cong \frac{R}{I_1} \times \frac{R}{I_2}$

$a \longmapsto (a + I_1, a + I_2)$

$\therefore c_1 = (a_1 + I_1, a_2 + I_2)$ To Prove surjective

$c = a_2 a + a_1 b$

$c \equiv a_2 \bmod I_2 \qquad c \equiv a_1 \bmod I_1$

$c \longmapsto a_2 a + a_1 b$

Generalization $I_1 + I_j = R \quad j \neq 1$

$a_j + b_j = 1 \quad \forall j \neq 1$

$\prod_{j=2}^{n} (a_j + b_j) = 1$

$= \left(\frac{\sum a_i b_j}{\in I_1} \right) + \prod_{j=2}^{n} b_j = 1$ ($\prod_{j=2}^{n} b_j \to c_1$ (similarly define c_i))

$\in \bigcap_{j=2}^{n} I_j \subset I_j \ \forall j$

$c_1 \equiv 1 \bmod I_1$

$c_1 \equiv 0 \bmod I_j \quad j \neq 1 \qquad c_i \equiv 1 \bmod I_i$

$c_i \equiv 0 \bmod I_j \quad j \neq 1.$

$c = \sum a_i c_i$

comm. ring with unity

$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R\}$

set of all polynomials.

$f(x)$ $g(x)$

Division Algorithm $\Rightarrow$ unique $q(x)$ and $r(x)$ s.t.

$$f(x) = g(x)\,q(x) + r(x), \text{ where } \boxed{\deg r(x) < \deg g(x)}$$

* If not working over field, assume $\boxed{g(x) \to \text{monic polynomial}}$

Ex → x^2+1 ; $2x+3$

$(x^2+1) = (2x+3)(\ \ ) + (\ \ )$

$\uparrow$ does not have inverse.

* $f(x) \in R[x]$

$a \in R$

$$f(x) = q(x)(x-a) + r(x)$$

$\deg r(x) < \deg(x-a)$

$\Rightarrow r(x) =$ constant.

$$f(a) = q(a)(a-a) + r(a)$$

$$0$$

$$\Rightarrow r(x) = f(a) \quad \forall\, x.$$

$$\Rightarrow f(x) = q(x)(x-a) + f(a)$$

$\boxed{a \text{ is a root of } f \text{ iff } f(a) = 0}$

* $\mathbb{Z}_8[x]$

$f(x) = x^3 \longrightarrow$ degree $= 3$

but no. of roots $= 4$

$\{0, 2, 4, 6\}$.

Happening

Because, $\mathbb{Z}_8$ is not an Integral Domain.

Thm — R — I.D.

Then any polynomial $f(x)$ in $R[x]$ has atmost $\deg(f)$ no. of roots.

Pf a_1 is a root

$$f(x) = g(x)(x-a_1)^{n_1} \qquad g(a_1) \neq 0$$

a_2 is another root

$$f(a_2) = 0 \Rightarrow f(a_2) = \underbrace{g(a_2)}_{q(x)(x-a_2)^{n_2}}\underbrace{(a_2-a_1)^{n_1}}_{\neq 0 \text{ (Because of ID)}}$$

and so on

Rmk — From now on, R is an ID.

Def" $a, b \in R$

We say a & b are associates if $a = ub$ (u = unit)

$a \in R$ (non-zero-non-unit) We say a is irreducible if $a = bc$ then either b or c is a unit.

$a \in R$ (non-zero, non unit) We say a is a prime in R if $a \mid bc \Rightarrow$ either $a \mid b$ or $a \mid c$.

Claim → Prime ⇒ Irreducible.

Pf → $a = bc$ (T.P. either b or c is unit.)

$a \mid bc \xrightarrow{\text{WLOG}} a \mid b \Rightarrow b = ad$

$a = adc$

$a(1-cd) = 0$

Working in Integral Domain. → $1 - cd = 0 \Rightarrow c$ is a unit

Claim → Irreducible $\not\Rightarrow$ Prime

Counterexample – $R = \mathbb{Z}[i\sqrt{3}] = \mathbb{Z}[\sqrt{-3}]$ → Commutative with unity. also ID ✓.

$= \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\}$

$2 \in R$

$2 = (a+bi\sqrt{3})(c+di\sqrt{3})$

$4 = 2 \cdot \bar{2} = (a^2+3b^2)(c^2+3d^2)$

$a = \pm 1$, $b = 0$ → (1) × 4

2 × 2 ✗ not possible as a, b ∈ ℤ

4 × (1) → $c = \pm 1$, $d = 0$

Irreducible ✓

But we have, $2 \mid (1+i\sqrt{3})(1-i\sqrt{3})$ but $2 \nmid (1+i\sqrt{3})$ and $2 \nmid (1-i\sqrt{3})$.

$a = u p_1 p_2 \dots p_k$
$a = w q_1 q_2 \dots q_r$
$\Rightarrow k = r$ and p_i & q are associates

$p = u'q$.

PAGE NO.:
DATE: / /

Defⁿ UFD (Unique Factorization Domain)

R be an ID. We say R is a UFD if every $a \in R$ can be uniquely written as →

$a = u p_1 p_2 \dots p_k$ where p_i's are irreducibles, u is a unit.

Lemma – In a UFD, irreducible $\iff$ prime.

Pf ($\Leftarrow$) Done. True for all ID's.

($\Rightarrow$) a – irreducible. $a \mid bc$

$\Rightarrow bc = ad$.

As we are working in UFD $\Rightarrow$

$u p_1 p_2 \dots p_k \, w q_1 q_2 \dots q_r = a \, v \, s_1 s_2 \dots s_t$.

WLOG

$\Rightarrow a = p_1 w'$ (associates)

$\Rightarrow a \mid b$ ∴ Prime.

\# finite ID → field ✓

→ T.P. Every nonzero element has an inverse.

$R = \{a_1, a_2, \dots, a_n\}$ → contains 1

$a_i \neq 0$

$= \{a_i^2, a_1 a_2, \dots a_i a_n\}$ $\Rightarrow a_i a_j = 1$ ✓ QED

Wedderburn's Thm →

Finite division ring ⇒ Field

Proof is quite long. A short proof online (by a tehroriest)

Defⁿ UFD → An integral domain is called a UFD if every non-zero element can be uniquely written as a pdt of irreducibles upto a unit.

$a = u\, b_1 b_2 \dots b_k$ (u: unit; b_i: irreducibles)

If $a = w c_1 c_2 \dots c_s$ then $k = s$, $b_i = w' c_j$

Gauss Thm → $R[x]$ $R[x_1, x_2, \dots x_n]$

$\mathbb{Z}[x_1 x_2 \dots x_n]$

$\mathbb{Q}[x_1 x_2 \dots x_n]$

- If a — prime, $(a) = \{ra : r \in R\}$ → prime ideal

  $xy \in (a) \Rightarrow$ either $x \mid a$ or $y \mid a$.

- R — ID

  'a' irreducible iff (a) is a maximal ideal (not necessarily unique) among the principal ideals.

  ↳ ideals generated by a single element.

Pf $(\Rightarrow)$ $(a) \subset (b) \subset R$

$a = rb$

irreducible $\rightarrow$ r = unit or b = unit

$b = r^{-1}a$ $\qquad$ $(b) = R$

$\Rightarrow b \in (a)$

$(\Leftarrow)$ $(a) \subset R$

$\hookrightarrow$ maximal.

a is not irreducible, $a = bc$ (none of them is a unit.)

$\Rightarrow (a) \subsetneq (b)$

Defⁿ Principal Ideal Domain $\rightarrow$ R-ID.

We say R is a principal ideal domain (PID) if every ideal of R is principal.

Ex- $\mathbb{Z}$ is a PID.

$F[x]$ is a PID.

Non-example $\mathbb{Z}[x]$ ideal $(2, x) \neq \langle f(x) \rangle$

(2)

then odd terms of x will not come.

$\longrightarrow$

Thm → R be an ID. Then R is a UFD iff

(1) Any ascending chain of principal ideal stabilize.

$$(a_1) \subset (a_2) \subset \dots ( ) \dots$$

$$(a_n) = (a_{n+i}) \quad \forall i$$

(2) Every irreducible is a prime.

Proof → ($\Rightarrow$)

$$(a_1) \subset (a_2) \subset \dots \subset (a_n) \subset (a_{n+1}) \dots$$

$$a_{i+1} \mid a_i \quad \forall i \qquad a_i \mid a_1$$

R is UFD $\Rightarrow a_1 = u p_1 p_2 \dots p_k$ finite

irreducibles → (Prime). (In UFD irreducible ↕ prime)

($\Leftarrow$) $a_1 \in R$

↳ irreducible ✓ (maximal ideal) among principal ideals.

If not $a_1 = a_2 b_2$ a_2, b_2 are non-units

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots (a_n)$$

$a_2 = a_3 b_3$ ↳ has to stabilise

$a = u p_1 p_2 \dots p_r$ ✓

T.P → factorisation is unique.

$a = w q_1 q_2 \dots q_r$

$p_1 \mid a_{r_1} \rightarrow a_{r_1} = p_1 r_1$

Thm → Every PID is a UFD.

Proof → $(a_1) \subset (a_2) \subset \ldots (a_n) \subset (a_{n+1}) \subset \ldots$

$I = \bigcup_{i=1}^{\infty} (a_i)$ → ideal

But we are inside a PID $\Rightarrow I = (b)$

$b \in I = \bigcup (a_i)$

$\Rightarrow b \in (a_k)$ for some k.

Thus $(b) = (a_k) = (a_{k+1}) \ldots$ (1) proved

a – irreducible

(a) – maximal ideal among principal ideals

↓

inside PID only principal ideal

↓

(a) – maximal

|

prime

a – prime (2) proved

$\therefore$ PID → UFD

Defⁿ → **Euclidean Domain (ED)** –

R is an ID. We say R is an ED if $\exists$ a function

$$\varphi : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

s.t. $a = bq + r$ $\quad a, b \in R$, $b \neq 0$

with $r = 0$ or $\varphi(r) < \varphi(b)$

Thm → Every ED is a PID. (→ Every ideal is principal ideal.)

Proof → $I \subset R$

If $I = (0)$ nothing to prove.

$I \neq (0)$ $\quad \varphi : R \longrightarrow \mathbb{Z}_{\geq 0}$

$$\varphi(I \setminus \{0\}) \subset \mathbb{Z}_{\geq 0}$$

Let $b \in I$ s.t. $\varphi(b)$ is the smallest

T.P. $I = (b)$.

$a \in I$ $\quad a = bq + r$

$r = a - bq \in I$

↓

Either $r = 0$ or $\varphi(r) < \varphi(b)$ (not possible $\varphi(b)$ is smallest.)

⇓

$a = bq$

$I = (b)$.

PAGE NO. :
DATE : / /

ED ⊆ PID ⊆ UFD ⊆ ID