6/3/2025

Rings and Fields

lec. 4

* A ring R has no zero divisors ($Div(R)=\emptyset$) $\Leftrightarrow$ R satisfies cancellation laws

$\rightarrow$ Proof: "$\Rightarrow$" let $Div(R)=\emptyset$, let $a, b, c \in R$, $a \neq 0$, $ab=ac$

$\rightarrow ab-ac=0 \rightarrow a(b-c)=0$ and $a \neq 0 \Rightarrow b-c=0 \Rightarrow b=c$

"$\Leftarrow$" let $a, b \in R$, $a\neq 0$, $ab=0 \Rightarrow ab=a0 \Rightarrow b=0 \Rightarrow Div(R)=\emptyset$

* $I \trianglelefteq R \wedge J \trianglelefteq R \Rightarrow I \cap J \trianglelefteq R$

$\rightarrow$ $I \cup J$ may not be ideal (ex.: $2\mathbb{Z}, 3\mathbb{Z} \trianglelefteq \mathbb{Z}$ but $2\mathbb{Z} \cup 3\mathbb{Z} \ntrianglelefteq \mathbb{Z}$)

$\rightarrow \{0\} \trianglelefteq R$, $R \trianglelefteq R$ (any ideal other than $\{0\}, R$ is called proper)

$\rightarrow$ If $I \trianglelefteq R$, $1 \in I \Rightarrow I = R$ (any ideal containing 1 is R itself)

Proof: $I \trianglelefteq R \Rightarrow I \subseteq R$

let $a \in R$, We have $I \trianglelefteq R \Rightarrow \forall i \in I, ai \in I \wedge ia \in I$

for $i=1$, $a1 \in I \wedge 1a \in I \Rightarrow a \in I \Rightarrow R \subseteq I \Rightarrow I = R$

$\rightarrow$ Any field F has no proper ideal

Proof: Suppose $I \trianglelefteq F$, $I \neq \{0\}$, $I \neq F$

$\Rightarrow \exists a \in I, a \neq 0$, let $r \in F$

$I \trianglelefteq F \Rightarrow ar \in I \wedge ra \in I$

for $r = a^{-1} \Rightarrow aa^{-1} \in I \Rightarrow 1 \in I \Rightarrow I = F$ $\Rightarrow$ F has no proper ideal

* let $f: R_1 \to R_2$ be homo. $\Rightarrow ker(f) \trianglelefteq R_1$

→ Proof: $f(0) = 0 \Rightarrow 0 \in ker(f) \Rightarrow ker(f) \neq \emptyset$

let $a, b \in ker(f)$, $f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b)$
$= 0 - 0 = 0 \Rightarrow a - b \in ker(f)$

$f(ab) = f(a)f(b) = 0 \cdot 0 = 0 \Rightarrow ab \in ker(f) \Rightarrow ker(f) \leq R_1$

let $r \in R$, $a \in ker(f)$, $f(ra) = f(r)f(a) = f(r)0 = 0 \Rightarrow ra \in ker(f)$

$f(ar) = f(a)f(r) = 0f(r) = 0 \Rightarrow ar \in ker(f) \Rightarrow ker(f) \trianglelefteq R_1$

→ $Im(f) \trianglelefteq R_2$ may not be true

ex.: define $f: \mathbb{Z} \to \mathbb{Q}$, $Im(f) = \mathbb{Z}$
$n \mapsto n$

, We have $\mathbb{Z} \ntrianglelefteq \mathbb{Q}$ (bec. $2 \cdot \frac{1}{3} \notin \mathbb{Z}$)

→ If f is epimorphism, then $Im(f) \trianglelefteq R_2$

* let $I \trianglelefteq R$, then $R/I = \frac{R}{I} = \{r + I : r \in R\}$ which is the set of all cosets of I in R is a ring called the quotient/residue ring of I in R where $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ and $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$

→ If $I = \{a_1, a_2, ---\}$, $r + I = \{r + a_1, r + a_2, ---\}$

ex.: $\frac{\mathbb{Z}}{6\mathbb{Z}} = \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$

↳ We stopped at $5 + 6\mathbb{Z}$ because $6 + 6\mathbb{Z} = 0 + 6\mathbb{Z}$

* Properties of quotient rings

① R is commutative $\Longrightarrow \frac{R}{I}$ is commutative

② R has $1 \Longrightarrow \frac{R}{I}$ has $1 = 1_R + I$

③ R is finite $\Longrightarrow \frac{R}{I}$ is finite

$\longrightarrow$ R is infinite $\Longrightarrow \frac{R}{I}$ may not be infinite (ex.: $\frac{\mathbb{Z}}{6\mathbb{Z}}$)

④ $Div(R) = \emptyset \Longrightarrow Div(\frac{R}{I})$ may not be equal to $\emptyset$ (ex.: $\frac{\mathbb{Z}}{6\mathbb{Z}}$)

⑤ Elements of $\frac{R}{I}$ have same properties of cosets in group theory (with addition)

⑥ $\exists f: R \longrightarrow \frac{R}{I}$ (epimorphism)
$r \longmapsto r + I$

⑦ If $f: R_1 \longrightarrow R_2$ is homo. $\Longrightarrow \frac{R_1}{\ker(f)} \cong Im(f)$ (I^{st} isomorphism theorem)

$\longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$ (ex.: $\frac{\mathbb{Z}}{7\mathbb{Z}} \cong \mathbb{Z}_7$)

$\longrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}}$ is always a field, p is prime (ex.: $\frac{\mathbb{Z}}{7\mathbb{Z}}$ is a field)

$\longrightarrow n\mathbb{Z} \equiv \langle n \rangle$

→ For the next part, we will assume all rings to be commutative with 1

* Types of ideals

1) An ideal $P \trianglelefteq R$ is said to be a <u>prime</u> ideal iff ① $P \neq R$
② $\forall ab \in P,\ a \in P \vee b \in P$

ex.: $\langle 0 \rangle$ is prime in $\mathbb{Z}$

→ Proof: We have $\langle 0 \rangle \neq \mathbb{Z}$, let $ab \in \langle 0 \rangle \Rightarrow ab = 0$

$\mathrm{Div}(\mathbb{Z}) = \phi$ and $\langle 0 \rangle \leqslant \mathbb{Z} \Rightarrow a = 0 \vee b = 0$

$\Rightarrow a \in \langle 0 \rangle \vee b \in \langle 0 \rangle \Rightarrow \langle 0 \rangle$ is prime in $\mathbb{Z}$

ex.: $\langle 5 \rangle$ is prime in $\mathbb{Z}$

ex.: $\langle 6 \rangle$ is not prime in $\mathbb{Z}$ (bec. $6 \in \langle 6 \rangle$, $6 = 2 \times 3$ but $2 \notin \langle 6 \rangle$
$\wedge\ 3 \notin \langle 6 \rangle$)

→ Any ideal generated by a prime number is prime

* An ideal $P \triangleleft R$ is prime $\Longleftrightarrow \frac{R}{P}$ is an integral domain

$\to$ Proof: "$\Longrightarrow$" let $P \triangleleft R$ be prime, we have $\frac{R}{P}$ is commutative

and $\frac{R}{P}$ has $1+P$

let $r_1+P,\ r_2+P \in \frac{R}{P}$, $r_1+P \neq P$, $(r_1+P)(r_2+P)=P$

$\Rightarrow r_1r_2+P=P \Rightarrow r_1r_2 \in P$ and P is prime $\Rightarrow r_1 \in P \vee r_2 \in P$

but if $r_1 \in P \Rightarrow r_1+P=P$ $\Rightarrow r_2 \in P \Rightarrow r_2+P=P \Rightarrow Div(\frac{R}{P})=\emptyset$

$\Rightarrow \frac{R}{P}$ is an integral domain

"$\Longleftarrow$" let $\frac{R}{P}$ be an integral domain, we have $P \triangleleft R$

and $P \neq R$ (bec. if $P=R \Rightarrow \frac{R}{P}=\frac{R}{R}=\{r+R : r \in R\}=R$)

let $ab \in P \Rightarrow ab+P=P \Rightarrow (a+P)(b+P)=P$

and $\frac{R}{P}$ is an integral domain $\Rightarrow Div(\frac{R}{P})=\emptyset \Rightarrow a+P=P \vee b+P=P$

$\Rightarrow a \in P \vee b \in P \Rightarrow P$ is prime

2 An ideal $I \trianglelefteq R$ is said to be a principal ideal iff $\exists a \in I : I = \langle a \rangle$, where $\langle a \rangle := \{ar : r \in R\}$

ex.: $\langle 2 \rangle$ is principal in $\mathbb{Z}$, $6\mathbb{Z}$

$\longrightarrow$ Any ring R is principal (bec. $\exists 1 \in R : R = \{1r \in R\} = \langle 1 \rangle$)

* A ring R is said to be a principal ideal ring iff $\forall I \trianglelefteq R$, I is principal

* $\mathbb{Z}$ is a principal ideal ring

$\longrightarrow$ Proof: let $A \trianglelefteq \mathbb{Z}$

Case 1: $A = \{0\} \Rightarrow A = \langle 0 \rangle \Rightarrow A$ is principal

Case 2: $A = \mathbb{Z} \Rightarrow A = \langle 1 \rangle \Rightarrow A$ is principal

Case 3: $A \neq \mathbb{Z}, A \neq \{0\}$, let $a \in A$, where a is the smallest positive integer in A

let $n \in A \Rightarrow \exists q, r \in \mathbb{Z} : n = qa + r$, $0 \leq r < a$ (division algorithm)

$\longrightarrow r = n - qa \in A$ ~~and~~ but a is the smallest positive integer in A

$\Rightarrow r = 0 \Rightarrow n - qa = 0 \longrightarrow n = qa \Rightarrow A = \langle a \rangle \Rightarrow A$ is principal

$\Rightarrow \mathbb{Z}$ is a principal ideal ring

$\longrightarrow$ Any field is ~~gene~~ a principal ideal ring (bec. a field contains only two ideals: $\{0\}$, F, ~~both one~~ each is generated by one element: $0, 1$)