Ring (R0), (R1) (R2) (R3)

$+$ $\cdot$ $(R,+)$ $(R,\cdot)$ $(a+b)c = ac+bc$.

Commutative ring $ab = ba \quad \forall a,b \in R$

Unity $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

zero divisor $0 \neq a \in R$ s.t. $\exists\, b \in R$ satisfying $ab = ba = 0$.

R is an integral domain if R is commutative with unity 1 & no zero divisor

---

R is a field if $(R^*, \cdot)$ is an Abelian group

Subring: $S \subseteq R$ $(S,+,\cdot)$ is a ring.

① $(S,+)$ Abelian group ② $a,b \in S \Rightarrow ab \in S$

Ideal $A \subseteq R$ is an ideal if

① $(A,+)$ Abelian subgroup

② $a \in A, r \in R \Rightarrow ar \in A$, $ra \in A$.

1+G
aH

Theorem Let A be an ideal of a ring R.
Then $R/A = \{a+A : a \in R\}$
under the operations.

$$(a+A) + (b+A) = (a+b) + A$$
$$(a+A)(b+A) = ab + A$$

form a ring.
Called the factoring of R wrt. A.

A 是 R 的理想

Example $R: (\mathbb{Z}, +, \cdot)$
$k \in \mathbb{N}$, $k \geq 2$
$A: (k\mathbb{Z}, +, \cdot)$

$R/A = \{[0], [1], \cdots [k-1]\} \cong \mathbb{Z}_k$.

$[a]+[b]$, $[a][b]$.

(R0) ✓ (R1) R/A is an Abelian group by group theory.

Proof:

(R2) $((a+A)(b+A))(c+A)$
$= (ab+A)(c+A)$
$= ((ab)c)+A$
$= a(bc)+A = (a+A)(bc+A)$
$= (a+A)((b+A)(c+A))$ ✓

(R3) $(a+A)[(b+A)+(c+A)]$
$= (a+A)((b+c)A)$? $= a(b+c)+A$.
$= (ab+A)+(ac+A)$
$= (a+A)(b+A) + (a+A)(c+A)$

Need to show that $(a+A)(b+A) = ab+A$ is well-defined
i.e. If $a+A = c+A$, $b+A = d+A$ $\quad = (cd+A)$
Then need to show $(a+A)(b+A) = (c+A)(d+A)$

This is true because

$a+A = c+A$ means $a-c \in A$, i.e., $c = a+\alpha_1$

and $b+A = d+A$ means $b-d \in A$ i.e., $d = b+\alpha_2$, $\alpha_1, \alpha_2 \in A$

$aH = cH$ if $a^{-1}c \in H$

So

$$(c+A)(d+A) = (a+\alpha_1+A)(b+\alpha_2+A)$$

$$= (a+\alpha_1)(b+\alpha_2) + A$$

$$= (ab + a\alpha_2 + \alpha_1 b + \alpha_1\alpha_2) + A$$

$$= ab + A \quad \because a\alpha_2, \alpha_1 b, \alpha_1\alpha_2 \in A$$

Remark If A is not an ideal, then there is $\alpha \in A$, $r \in R$ s.t. $\alpha r \notin A$.

$0+A = \alpha + A$

$(0+A)(r+A) = 0\cdot r + A = A$.

but $(\alpha+A)(r+A) = \alpha r + A \neq A$.

Examples $\mathbb{Z}/4\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}[i]/\langle 2-i\rangle$, $\mathbb{R}[x]/\langle x^2+1\rangle$.

① $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$

② $R = (2\mathbb{Z}, +, \cdot)$

$A = (6\mathbb{Z}, +, \cdot)$

$R/A = \{0+6\mathbb{Z},\ 2+6\mathbb{Z},\ 4+6\mathbb{Z}\}$.

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\cong (\mathbb{Z}_3, +)$

	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

③ $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$

$A = \langle 2-i\rangle = \{(2-i)r : r \in \mathbb{Z}[i]\}$

$= \{(2-i)(a+ib) : a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]/A = \{A, 1+A, 2+A, 3+A, 4+A\}$.

$\cong (\mathbb{Z}_5, +, \cdot)$

$1 \notin A$ because $1 = (2-i)(a+ib)$

$= 2a+b+i(2b-a)$.

i.e., $\nexists$ integers a, b s.t

$\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}^{-1}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= \frac{1}{5}\begin{bmatrix} 2 \\ 1 \end{bmatrix}$

$5 = (2-i)(2+i) \in A$

$n+A =$ where $n = 5q+r$, $0 \le r < 5$

$a+bi+A = \ldots = r+A$

R is commutative.

$a \in R$

$A = \langle a\rangle = \{ar : r \in R\}$

is an ideal.

The ideal generated by $a \in R$

$ar \in A$, $s \in R$

$ars \in A$

$sar = a(sr) \in A$

$a \in M_n$

$S = \{aX : X \in M_n\}$

$aX \in S$, $Y \in M_n$??????

(4) $\mathbb{R}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{N},\ a_n \neq 0\} \cup \mathbb{R}$

$A = \langle (x^2+1) \rangle = \{(x^2+1) f(x) : f(x) \in \mathbb{R}[x]\}$

$\mathbb{R}[x]/A = \{a + bx + A : a, b \in \mathbb{R}\}$.

$\langle 2 \rangle = \mathbb{R}[x]$.

$g(x) + A = (x^2+1) q(x) + (ax+b) + A = ax + b + A$

where $g(x) = (x^2+1) q(x) + (ax+b)$

$\therefore$ Every $g(x)+A$ can be reduced to $ax+b+A$ for some $a, b \in \mathbb{R}$.

(2) Next.

If $ax+b \neq \hat{a}x+\hat{b}$.

Then $ax+b+A \neq \hat{a}x + \hat{b} + A$

because $(ax+b) - (\hat{a}x+\hat{b}) \neq (x^2+1) q(x)$

$x^2+1 \;\big|\; 3x^2+4x-1$ (3)

$3x^2+3$

$4x-4$

Note $(ax+b+A) + (cx+d+A) = (a+c)x + (b+d) + A$

$(ax+b+A)(cx+d+A) = (ax+b)(cx+d) + A$

$= acx^2 + adx + bcx + bd + A$

$= -ac(x^2+1) + acx^2 + (ad+bc)x + bd$

$= (ad+bc)x + (bd-ac) + A$.

$(ax+b+A) \xrightarrow{\phi} ai + b \in \mathbb{C}$ $\quad \phi : \mathbb{R}[x]/A \to \mathbb{C}$

$(ax+b+A) \xrightarrow{\phi} \begin{bmatrix} b & a \\ -a & b \end{bmatrix} \in \{\begin{bmatrix} x & y \\ -y & x \end{bmatrix} : x, y \in \mathbb{R}\}$

Example $\mathbb{Z}_3[x]/\langle x^2+1\rangle = \{a+bx+A : a,b\in\mathbb{Z}_3\}$

$\mathbb{Z}_3[x] \supseteq \{ax+\}$ $\quad \Phi$ $\quad A$

Check: It is a field with 9 elements.