교수님 email : swpark @ dau.ac.kr 1705645 성제훈.

현대대수학

todo : abelian group ? → 곱셈에대해닫혀?
associative 이야 ?

Section 18. Ring and Fields (환과체)

Def) A ring $(R, +, \cdot)$ is a nonempty set R

with two binary operations $+$ and $\cdot$ such that

1. $(R, +)$ is an abelian group. 교환법칙

2. $\cdot$ is associative on R : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. $a \cdot (b+c) = \underline{a \cdot b} + a \cdot c$ [left distributive]. $a \cdot (b+c)$
→ $a \cdot (b+c) = a \cdot c + b \cdot c$

$(a+b) \cdot c = a \cdot c + b \cdot c$ [right distributive].

b+c 연산먼저하나 분배법칙을 하나같다

for all $a, b, c \in R$

Recall) $(G, +)$ is an abelian gp.

① $+$ is an binary operation i.e. $a+b \in G$ $\forall a, b \in G$

② associate i.e. $(a+b)+c = a+(b+c)$ $\forall a, b, c \in G$

③ identity elt i.e $\exists e \in G$ s.t. $a+e = e+a = a$ $\forall a \in G$

④ inverse elt i.e, $\exists -a \in G$ s.t. $a+(-a) = (-a)+a = e$ $\forall a \in G$

⑤ $a+b = b+a$ $\forall a, b \in G$

Ex) $(\mathbb{Z}, +)$ is an abelian group.

① $2+3 = 5 \in \mathbb{Z}$

② $(2+3)+4 = 2+(3+4)$

③ $2+0 = 0+2 = 2$

④ $2+(-2) = (-2)+2 = 0$

Ex) $(\mathbb{Z}, +, \cdot)$ is a ring, $(\mathbb{Z} \neq \emptyset)$

$+, \cdot$ are binary operations. $2+3 \in \mathbb{Z}$, $2 \cdot 3 \in \mathbb{Z}$

① $(\mathbb{Z}, +)$: abelian group.

② $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in \mathbb{Z}$ $(2 \cdot 3) \cdot 4 = 2 \cdot (3 \cdot 4)$

③ $(a+b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in \mathbb{Z}$ $(2+3) \cdot 4 = 2 \cdot 4 + 3 \cdot 4$

가환환.

Def) A ring $(R, +, \cdot)$ is a commutative ring

if $a \cdot b = b \cdot a$ = $\forall a, b \in R$

Ex) $(\mathbb{Z}, +, \cdot)$ is a commutative ring.

Ex) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ → comm ring

pf) $\frac{b}{a} \in \mathbb{Q}$, $a \neq 0$ → 증명해보기.

example 18.3) Let $\mathbb{R}$: ring

define $M_n(R) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & & a_{nn} \end{pmatrix} \middle| \, a_{ij} \in R \right\}$

Ex) $\mathbb{Z}$: ring

$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z} \right\}$

→ matrix multiplication.

$(M_n(R), +, \cdot)$ is ring

① $(M_2(\mathbb{Z}), +)$ is an abelian gp.

id elt : $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$

② $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ $C = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$

$(A \cdot B) \cdot C = A \cdot (B \cdot C)$

위의 행렬에 대한 ring 을 matrix ring 이라한다.

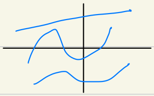
↳ 증명해보기.

identity element → id elt

Todo : cancellation property .
additive identity .

Ex 18.4) $f : \mathbb{R} \to \mathbb{R}$ function ,

Define $F = \{ f \mid f : \mathbb{R} \to \mathbb{R} \}$



→ 옆과같은함수의 집합 .

$(F, +, \cdot)$

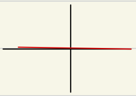
define by $(f+g)(x) = f(x) + g(x)$

$f \cdot g = f(x) \cdot g(x)$

then $(F, +, \cdot)$ is ring .

$(F, +)$: abelian g.p.

id elt : zero map . ($f(x) = 0$)



inverse of $f(x)$ is $-f(x)$

Ex 18.6) $(\mathbb{Z}_n, +, \cdot)$ is a ring (comm ring)

$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$.

$(\mathbb{Z}, +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ → 이 3개는 현대대수학에서 중요하게 사용된다

쉬운 예이므로 기억해 둘 것.

Ex) $(M_2(\mathbb{Z}_2), +, \cdot)$ $\quad \mathbb{Z}_2$

$M_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$.

$(M_2(\mathbb{Z}_2), +, \cdot)$ is a non commutative ring .

$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$

$A \cdot B \neq B \cdot A$ → non commutative ring .

Ex 18.7)

Thm 18.8) Let $(R, +, \cdot)$ be a ring

with additive identity 0 , that for any $a, b \in R$.

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

(2) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(3) $(-a) \cdot (-b) = ab$.

pf) (1) $a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0$ and

by the cancellation property of $(R, +)$, $a \cdot 0 = 0$

(2) $a \cdot (-b) + ab = a \cdot (-b+b) = a \cdot 0 = 0$ by (1)

$\therefore a \cdot (-b) = -ab$. similary $(-a) \cdot b = -ab$.

(3) $(-a) \cdot (-b) = ab$

$(-a) \cdot (-b) = -(a \cdot (-b))$ by (2) and

$-(a \cdot (-b)) = -(-(a \cdot b))$ by (2)

Then $(-a) \cdot (-b) = -(-(a \cdot b)) = a \cdot b$.

↳ add inverse of (add inverse ab)

additive identity (identity) : 0 ← 항등원 .

multiplitive identity (unity) : 1 .

Remark) Ring with unity .

모든 Ring은 identity는 항상가지지만
identity는 가지지 않을수도 있다.

$|M_2(\mathbb{Z}_2)| = 16$.

identity elt $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

unity elt $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Def) For ring R and R'

a map $\phi : R \to R'$ is a ring homomorphism

① $\phi(a+b) = \phi(a) + \phi(b)$ | group homo

② $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ | ring homo

Ex) $\phi : \mathbb{Z} \to \mathbb{Z}'$

Ex) $\phi : \mathbb{Z} \to \mathbb{Z}_5$ by $\phi(n) = r$ when $n = 5q + r$, $0 \le r < 5$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Then ϕ is a ring homomorphism . → 증명해보기 .