현대대수학

1705645 성제훈 .

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

현대대수학

todo : abelian group ; → 곱셈에대해닫혀?
associative ⋅ on ?

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

   $a\cdot(b+c)$
   b+c 연산 먼저 하나
   분배법칙을 하나 같다

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

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

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

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

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

$(M_n(R), +, \cdot)$ is ring → matrix multiplication.

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

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

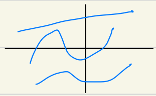
위의 행렬에 대한 ring 을 matrix ring 이라한다.

↳ 작성해보기.

identity element → id elt

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

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



→ 위와같은 함수의 집합.

$(F, +, \cdot)$

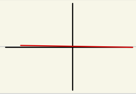
define by $(f+g)(x) = f(x) + g(x)$

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

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

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

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

Todo : cancellation property.

additive identity : 덧셈에 대한 항등원.

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 Ring는 identity는 항상 가지지만 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 $n = 5q + r$, $0 \le r < 5$

$\{0, 1, 2, 3, 4\}$

Then ϕ is a ring homomorphism. → 증명해보기.

Q : ϕ ?

Ex) $\phi : \mathbb{Z} \xrightarrow{\text{ring}} \mathbb{Z}$

$\phi(a) = r$ where $a = nq + r$ $\quad 0 \le r < n$

is a ring homomorphism

$\phi : \mathbb{Z} \to \mathbb{Z}$

$\phi(a) = 5q + r$ $\quad 0 \le r < 5$ $\quad \begin{pmatrix} 5 \mapsto 0 \\ 6 \mapsto 1 \\ 8 \to 3 \ \cdots \end{pmatrix}$.

sol) $a, b \in \mathbb{Z}$ and let

$a = bq_1 + r_1$, $b = nq_2 + r_2$

when $0 \le r_1 < n$, $0 \le r_2 < n$

① $\phi(a+b) = \phi(nq_1 + r_1 + aq_2 + r_2)$

$= \phi(n(q_1 + q_2) + r_1 + r_2) = r_1 + r_2$

$\phi(a) = \phi(nq_1 + r_1) = r_1$

$\phi(b) = \phi(nq_2 + r_2) = r_2$

$\therefore \phi(a+b) = \phi(a) + \phi(b)$

② $a \cdot b = (nq_1 + r_1)(nq_2 + r_2)$

$= n^2 q_1 q_2 + n(q_1 r_2 + q_2 r_1) + r_1^2$

$\phi(a \cdot b) = \phi(n(q_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2)$

$= r_1 \cdot r_2$

$\phi(a) \cdot \phi(b) = \phi(nq_1 + r_1)\, \phi(nq_2 + r_2)$

$= r_1 \cdot r_2$

$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

초기조건이 중요!

☆ Let $a, b \in \mathbb{Z}$ and $a = nq_1 + r_1$, $b = nq_2 + r_2$

when $0 \le r_1 < n$, $0 \le r_2 < n$

〈시험예제〉

$\phi : \mathbb{Z} \to \mathbb{Z}_4$

by $\phi(n) = r$, when $a = 4q + r$ $\quad$ why?

with $0 \le r < 4$

Ex) let $F = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$

Then for each a the evaluation map. $\phi_a : F \to \mathbb{R}$

$\phi_a(f) = f(a)$ for $f \in F$ is a ring homo

called an evaluation homomorphism.

For example

$\phi_{\sqrt{2}} : F \to \mathbb{R}$ by $\phi_{\sqrt{2}}(f) = f(\sqrt{2})$

$f(x) = x + 1$ then

$\phi_{\sqrt{2}}(f) = \underbrace{\sqrt{2} + 1}_{\in \mathbb{R}}$

$\phi_2(f) = 2 + 1 = 3$

① $\phi_a(f+g) = \phi_a(f) + \phi_a(g)$

② $\phi_a(f \cdot g) = \phi_a(f) \cdot \phi_b(f)$

①, ② 증명해보기.

$\mathbb{Z}_n$ n으로나누었을 때 나머지의 집합.

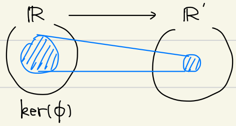
Q 어떠한 집합이 field 임을보이는 과정?

Note: kernel of ϕ, dnoted

$\phi(a)=0$ 인 a의 집합.

$\ker(\phi) = \{a \in \mathbb{R} \mid \phi(a) = 0\}$

additive identity.



Ex) $\phi : \mathbb{Z} \to \mathbb{Z}_5$ $\ker(\phi) = 5\mathbb{Z}$

$\phi : \mathbb{Z} \to \mathbb{Z}_n$ $\ker(\phi) = 5n$.

Ex) $\phi_a : F \to \mathbb{R}$

$\ker(\phi_a) = \{f \mid f(a) = 0\}$.

Def 18.2) A ring homomorphism $\phi : \mathbb{R} \to \mathbb{R}'$ is called an isormorphism dinoted by $R \cong R'$ if ϕ is 1-1 and onto.

곱셈에대한 역원.

Def) A multiplicative Inverse of an element a in a ring R with unity 1 is an elt a^{-1} such that

$aa^{-1} = a^{-1}a = 1$

Def) Let R be a ring with unity 1

An elt $u \in R$ is a unit if it has a multi Inverse in R

Ex) $(\mathbb{Q}, +, \cdot)$

unit; $2^{-1} = \frac{1}{2} \to 2 \cdot \frac{1}{2} = \frac{1}{2} \cdot 2 = 1$

Ex) $Im(\mathbb{Z}, +, \cdot)$

units of $\mathbb{Z} = \{1, -1\}$ || dinote

$\mathbb{Z}^{\times} = \{1, -1\}$.

모든원소에대해 0은 역원을가지지 않는다. ($\frac{0}{0}$ X)

Def 18.6) A ring $(R, +, \cdot)$ is a division ring if $(R - \{0\}, \cdot)$ is a group

실수집합 중 0을제외한 집합.

If $(R - \{0\}, \cdot)$ is an abelian group.

R is called a field (체).

Ex) $(\mathbb{Q}, +, \cdot)$ is a infinite field.

$(\mathbb{Q} - \{0\}, \cdot)$ is an abelian group.

1 is unity.

$a \neq 0$ inverse of a is $\frac{1}{a}$

($\frac{b}{a} \neq 0$ inverse of a is $\frac{a}{b}$ ($b \neq 0$))

Ex) $(\mathbb{Z}_p, +, \cdot)$ is a field (finite)

(p: prime)

$\mathbb{Z}_p : \{0, 1, 2, \cdots p-1\}$.

Note: $(\mathbb{Z}_n, +, \cdot)$ is not a field in general

for example (counting ex) $(\mathbb{Z}_4, +, \cdot)$ is not a field.

sol) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. $2 \cdot \square = 1$?

unity.

$1 = 2$

$2 = 0$

$3 = 2$

$\to \mathbb{Z}_4$ is not field.