현대대수학

1705645 성제훈

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

현대대수학

todo : abelian group ; → 곱셈에대해갈처?
associative ·에 ?

Section 18. Ring and Fields (환과체)

Q 여기서 +, · 각각 봐야!

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

$a\cdot(b+c)$ $b+c$ 연산먼저하나 분배법칙을 하나같다

$(a+b)\cdot c = a\cdot c + b\cdot c$ [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 ie, $\exists -a\in G$ 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. $2+3\in\mathbb{Z}$, $2\cdot3\in\mathbb{Z}$

① $(\mathbb{Z},+)$: abelian group.

② $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ $\forall a,b,c\in\mathbb{Z}$ $(2\cdot3)\cdot4 = 2\cdot(3\cdot4)$

③ $(a+b)\cdot c = a\cdot c+b\cdot c$ $\forall a,b,c\in\mathbb{Z}$ $(2+3)\cdot4 = 2\cdot4+3\cdot4$

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) $\frac{b}{a}\in\mathbb{Q}$, $a\neq0$ → 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 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $B=\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ $C=\begin{pmatrix} i & j \\ k & l \end{pmatrix}$

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

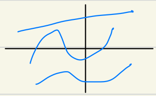
위의 행렬에 대한 ring 을 matrix ring 이라한다.

↳ 작성해보기.

identity element → id elt

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

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



→ 옆과같은함수의 집합.

$(F, +, \cdot)$

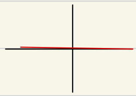
define by $(f+g)(x) = f(x) + g(x)$

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

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 둘것.

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)

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)

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

(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 않을수로 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.

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

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

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

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〉 try!

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

by $\phi(n) = r$, when $a = 4q + r$ by.

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 $\phi_a(f \cdot g) = \phi_a(f) \cdot \phi_a(g)$.

①, ② 증명해보기.

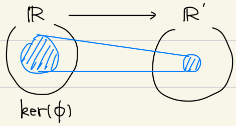
pf) ① $\phi_a(f+g) = (f+g)(a)$

$\phi_a(f)$ .. (a) $\qquad \phi_a(g) = g(a)$

$\mathbb{Z}_n$ n으로나누었을 때 나머지의 집합.

Note : kernel of ϕ, dnoted. $\phi(a)=0$ 인 a의 집합.

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



Ex) $\phi : \mathbb{Z} \to \mathbb{Z}_5$ $\quad$ $\phi : \mathbb{Z} \to \mathbb{Z}_n$

$\ker(\phi) = 5\mathbb{Z}$ $\quad$ $\ker(\phi) = 5n$.

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

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

Def 18.2) A ring homomorphism $\phi : R \to R'$ 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) $\mathrm{Im}(\mathbb{Z}, +, \cdot)$

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

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

Q 어떠한 집합이 field 임을보이는 과정?

모든원소에대해 0은 역원을가지지 않는다. $(\frac{1}{0} \times)$

~~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) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. unity. $\quad 2 \cdot \square = 1$? $\to \mathbb{Z}_4$ is not field.

$1 = 2$
$2 = 0$
$3 = 2$

※ A ring $(F, +, \cdot)$ field $(F - \{0\}, \cdot)$ abelian group.

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

Ex) $(\mathbb{Z}_p, +, \cdot)$ (p : prime) field (finite)

Ex) $(\mathbb{Z}_p, +, \cdot)$ is field.
ring

show $(\mathbb{Z}_p - \{0\}, \cdot)$ is an abelian g.p.

① $\cdot$ is a binary operation $a \cdot b \in \mathbb{Z}_p$ for $a, b \in \mathbb{Z}_p$.

② $\cdot$ is an associative

③ identity elt.

④ inverse elt

⑤ $a \cdot b = b \cdot a$.

※ ①,②,③,⑤는 자명하므로 ④만 증명하면 된다.

Todo : GCD 세로식 구하는 거 다시공부.

Recall from the number theory.

Thm) $(a,b)=1$ (GCD (a,b)), then $\exists\ s,t \in \mathbb{Z}$ $\ni$

$as+bt=1$

Ex) $(4,7)=1$ $\exists\ s,t$ $\ni$ $4s+7t=1$

Let $m \leftarrow \mathbb{Z}_p - \{0\}$ (p : prime.) then

$(m,p)=1$ $\exists$ (by the thm)

$\exists\ s,t$ $\ni$ $ms+pt \equiv 1 \pmod p$.
$pt \bmod p = 0$.

Then $ms \equiv 1$ then $m^{-1} \equiv s$

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

$\mathbb{Z}_{13} = \{0,1,2,3,\dots,12\}$.

Find 5^{-1} ? (multi inverse of 5 in $\mathbb{Z}_{13}$).

sol) $(13,5)=1$ want to find s,t $\ni$

$13s+5t \equiv 1 \pmod{13}$
$(\equiv 0)$

to find $(13,5)_{GCD}$.

$(13,5) \to (3,5) \to (3,2) \to (1,2) \to (1,0)=1$

2	13	5	1
	10	3	
1	3	2	2
	2	2	
	1	0	

to find s,t.

	2	1	1	2	
s	1	0	1	−1	2
t	0	1	−2	3	−5

$13 \cdot 2 + 5(-5) = 1$

$\therefore\ 5^{-1} = -5 \equiv 8 \pmod{13}$.

Ex2) find 8^{-1}

sol) $(13,8)=1$

$13s+8t \equiv 1$

① 1	13	8	1 ②
	8	5	
③ 1	5	3	1 ④
	3	2	
⑤ 2	2	1	
	2		
	0		

$\Rightarrow$

	①	②	③	④	⑤	
a_i	1	1	1	1	2	
s_i	1	0	1	−1	2	−3 : s
t_i	0	1	−1	2	−3	5 : t

여기는 항상 고정.

$13(-3) + 8(5) = 1$

$\therefore\ 8^{-1} = 5 \pmod{13}$.

유클리드 호제법 세로표 작성법.

1	13	8	1
	8	5	
1	5	3	1
	3	2	
2	2	1	
	2		
	0		

$\Rightarrow$

a_i	1	1	1	1	2.
s_i	1	0	$1-1\times 0$		
t_i	0	1			

연습: $\mathbb{Z}_{17}$ 에서 5^{-1}는?

3	17	5	2
	15	4	
2	2	1	
	2		
	0		

a_i	3	2	2		
s_i	1	0	1	−2	: s
t_i	0	1	−3	7	: t

$(17,5)=1$

$17 \cdot (-2) + 5 \cdot (7) = 1$
mod 17 = 0

$\therefore\ 5^{-1} = 7$.

Todo: 19.3 pf 다시해보기.

p ⇒ q 일때 　　Q $m\frac{n}{d} = \frac{m}{d}n = 0$ → 왜?

* 간접증명 ~q ⇒ ~p 를 증명.

직접증명 p ⇒ q 를 바로 증명.

Ex) $\mathbb{Z}_{19}$, $5^{-1} = ?$

$(19, 5) = ?$

3	19	5	1
	15	4	
4	4	1	
	4		
	0		

a	3	1	4	
s	1	0	1	-1
t	0	1	-3	4

$\underbrace{19\cdot(-1)}_{\text{mod } 19 = 0} + 5\cdot 4 = 1$.

$5^{-1} = 4$.

Ex) $\mathbb{Z}_{23}$　$9^{-1} = ?$

2	23	9	1
	18	5	
1	5	4	4
	4	4	
	1	0	

a	2	1	1	4	
s	1	0	1	-1	2
t	0	1	-2	3	-5

$\underbrace{23\cdot 2}_{\text{mod } 23 = 0} + 9\cdot(-5) = 1$

$\therefore 9^{-1} = -5 = 17$.

Section 19. Integral Domains.

Def 19.2) If a and b are two non zero elts of a ring R such that $a\cdot b = 0$, then a and b are zero divisors (or divisions of zero).

영인자에 대한 정의.

($a, b \neq 0$　$a\cdot b = 0$ 일때 a, b를 zero divisions 라한다.)

Ex) In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$　$(\mathbb{Z}, +, \cdot)$ ring.

위의 정의에따라 $\mathbb{Z}_6 - \{0\}$ 에서 생각한다.

$\{1, 2, 3, 4, 5\}$.

zero divicions. → $2\cdot 3 = 0$, $3\cdot 4 = 0$

5는　$5\cdot 1 \neq 0$, $5\cdot 2 \neq 0$　$5\cdot 3 \neq 0$　$5\cdot 4 \neq 0$

1은　$1\cdot 1 \neq 0$　$1\cdot 2 \neq 0$ ···

$\therefore$ 1과 5는　non zero divisor

Thm 19.3) In the ring $\mathbb{Z}_n$,

m is a zero divisor iff $(m, n) \neq 1$

(⟺) if and ony if : 필요충분조건.

ex) $(1, 6) = 1$, $(5, 6) = 1$, $(2, 6) \neq 1$, $(3, 6) \neq 1$.

pf) (⇐) Let $m \in \mathbb{Z}_n$, $m \neq 0$ and $(m, n) \neq 1$, and

$(m, n) = d > 1$　then　$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n = 0$

이 증명의 핵심.

(ex: $(4, 6) = 2$).　so $m\left(\frac{n}{d}\right) = 0$ and $\frac{n}{d} \neq 0$

Thus m is a zero divisor.

「 Not a zero divisor ; $a\cdot b = 0 \Rightarrow a = 0$ or $b = 0$ 」

(⇒) Suppose $(m, n) = 1$　If $s \in \mathbb{Z}_n$

간접증명* ~q ⇒ ~p

$m\cdot s = 0$, then　$n \mid ms$ (n devides ms).

ms가 n의 배수이다.

Since $(m, n) = 1$,　$n \mid s$

So that $s = 0$ in $\mathbb{Z}_n$

참고! Recall) From the number theory,

Thm) $n \mid ms$ and $(m, s) = 1 \Rightarrow n \mid s$

ex) $4 \mid 3\cdot 8$　$(4, 3) = 1 \Rightarrow 4 \mid 8$.

In $\mathbb{Z}_n$　$(m, n) \neq 1 \iff m$ is a zero divisor.

$(m, n) = 1$　　m is a unit.

Ex) $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

unit : $\{1, 5, 7, 11\}$

곱셈에 대한역원.

zero-divisors : $\{2, 3, 4, 6, 8, 9, 10\}$

Ex) $\mathbb{Z}_{24} = \{0, 1, 2, 3, 4 \cdots, 22, 23\}$.

unit : $\{1, 5, 7, 11, 13, 17, 19, 23\}$.

zero-divisor : $\{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22\}$

Corollary) If p is a prime, then

$\mathbb{Z}_p$ has no zero divisors.

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

Note) The cancellation laws hold in $\mathbb{R}$ (property).

if $a \cdot b = a \cdot c$ with $a \neq 0$ → $\cancel{a}b = \cancel{a}c$
$b = c$.

implies $b = c$ and $b \cdot a = c \cdot a$

with $a \neq 0$ implies $b = c$

In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

$2 \cdot 3 = 4 \cdot 3 \Rightarrow 2 = 4$.

In general. Ring 에서는 cancellation laws 가 성립 X.
(곱셈에대한).

Recall from the group theory,

In a group $(G, *)$ cancellations laws always hold.
Group 에서는 c.l이 항상성립.
→ group 의 elt 는 모두 역원이 존재하므로 성립.

ring 에서는 역원이 존재할수도 안할수도 있으므로 일반적으로 성립 X,